Ministerstwo Cyfryzacji

**NARODOWY STANDARD CYBERBEZPIECZEŃSTWA**
**NSC 800-53A wer. 2.0**

**Część 2**

30 października 2023

# Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych oraz organizacjach

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

# PREAMBUŁA

***Szanowni Państwo,***

oddajemy w Państwa ręce zestaw publikacji - Narodowe Standardy Cyberbezpieczeństwa, o których mowa w interwencji 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń. Standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST) i posiadają mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, na których oparte jest zarządzanie bezpieczeństwem informacji w podmiotach krajowego systemu cyberbezpieczeństwa.

Standardy stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w tym zakresie w administracji federalnej USA.

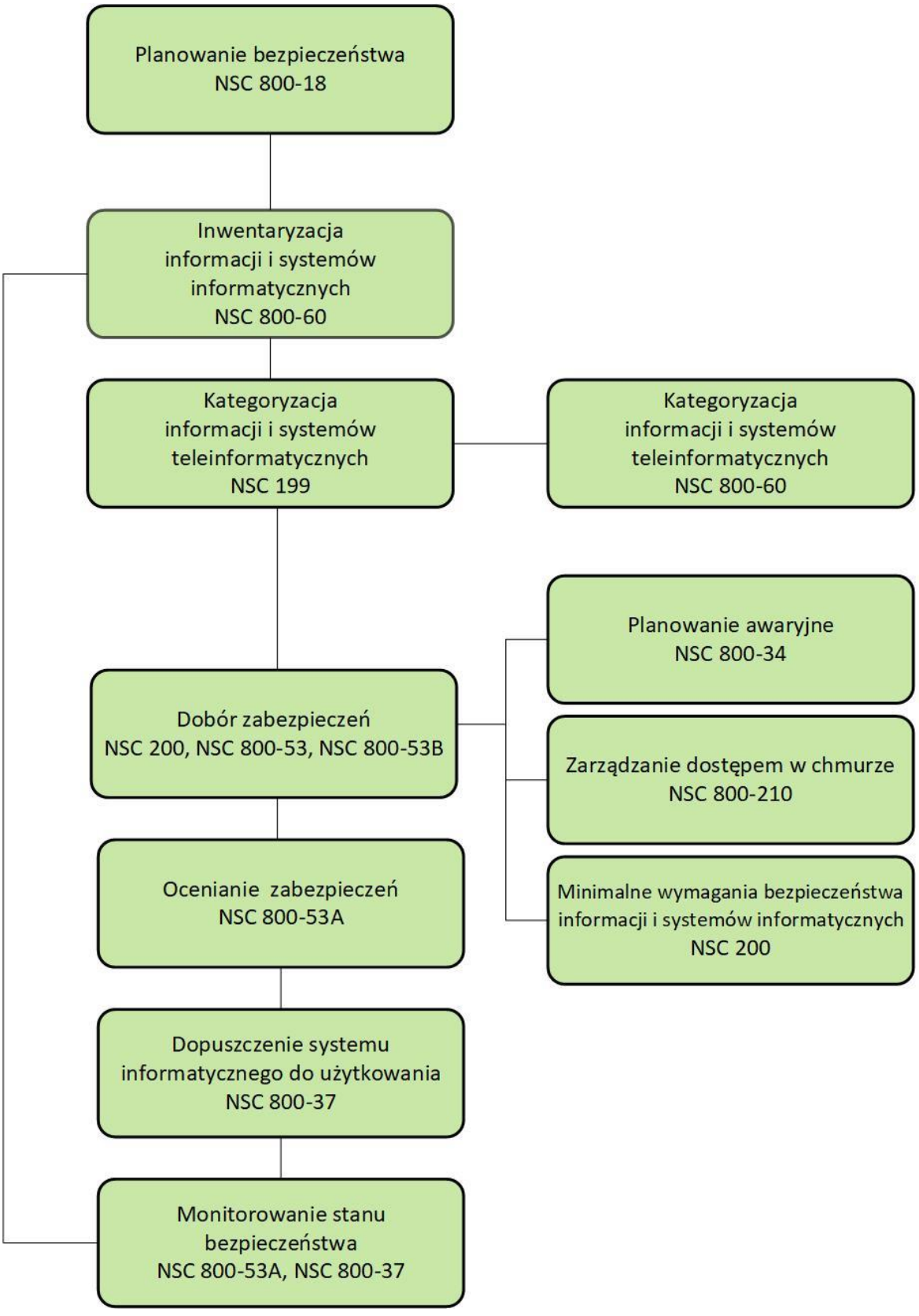
Zestaw publikacji specjalnych obejmuje następujące pozycje:

- NSC 199, *Standardy kategoryzacji bezpieczeństwa* – na podstawie FIPS 199.
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych* – na podstawie FIPS 200.
- NSC 800-18, *Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych* – na podstawie NIST SP 800-18.
- NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne* – na podstawie NIST SP 800-30.
- NSC 800-34, *Poradnik planowania awaryjnego* – na podstawie NIST SP 800-34.
- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* – na podstawie NIST SP 800-37.
- NSC 800-39, *Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego* – na podstawie NIST SP 800-39.

- NSC 800-53, *Zabezpieczenia i ochrona prywatności w systemach informacyjnych oraz organizacjach* – na podstawie NIST SP 800-53.
- NSC 800-53 MAP, *Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013*, na podstawie NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001.
- NSC 800-53B, *Zabezpieczenia bazowe systemów informacyjnych oraz organizacji* – na podstawie NIST SP 800-53B.
- NSC 800-60, *Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego* – na podstawie NIST SP 800-60.
- NSC 800-61, *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* – na podstawie NIST SP 800-61.
- NSC 800-210, *Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej* – na podstawie NIST SP 800-210.

W oparciu o te publikacje można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem informacji bazujący na publikacjach NIST wykorzystuje następujące dokumenty:




## Cykl zarządzania bezpieczeństwem informacji

# WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował szereg standardów i wytycznych w celu zapewnienia jednolitego podejścia do problematyki bezpieczeństwa informacji i systemów informacyjnych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji i systemów informacyjnych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością działalności i majątku organizacji, osób fizycznych i państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych. Dzięki jednolitemu podejściu do zarządzania ryzykiem ułatwia także wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznym i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (m. in. ISO[1]), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów.

Publikacje NIST co do zasady nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dopuszczone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejściem do zagadnień związanych z bezpieczeństwem informacji i systemów informacyjnych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST, jako godne zaufania i rekomendują stosowanie ich przez polskie

[1] International Organization for Standardization (ISO) - Międzynarodowa Organizacja Normalizacyjna– organizacja pozarządowa zrzeszająca krajowe organizacje normalizacyjne.

podmioty przy opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie.

W niniejszej publikacji mogą znajdować się odniesienia do innych opracowywanych przez nas publikacji. Informacje tu zawarte, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji powinny obowiązywać dotychczasowe wymagania, wytyczne i procedury, jeśli takie istnieją. W ramach planowanych przez Państwa prac zalecamy śledzenie naszych prac publikacyjnych.

Aktualne informacje o prowadzonych przez nas pracach dostępne są pod adresem:

 Narodowe Standardy Cyberbezpieczeństwa

Jesteśmy również otwarci na wszelkie Państwa sugestie, które pomogą nam w dalszych pracach nad standardami cyberbezpieczeństwa i zachęcamy do kontaktu.

 +48222455922

 sekretariat.dc@cyfra.gov.pl

Niniejsza publikacja, ***Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych oraz organizacjach***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NSC 800-53A, Rev. 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*.

Przytaczane i cytowane w publikacji przepisy, okólniki, rozporządzenia wykonawcze, dyrektywy, normy, standardy, polityki, memoranda itp. odnoszą się, o ile nie zaznaczono inaczej, do prawodawstwa i rynku amerykańskiego. Jeżeli cytowany fragment ma przełożenie lub odpowiednik w polskim porządku prawnym lub normalizacyjnym, wówczas informacje te wskazane są bezpośrednio w tekście lub w przypisach.

W publikacji posłużono się pojęciami zdefiniowanymi w poradniku źródłowym, na podstawie którego powstały niniejsze zalecenia. W przypadku, gdy tożsame pojęcie zostało zdefiniowane również w powszechnie obowiązujących aktach prawnych lub normatywnych, a ich definicja różni się od tej zamieszczonej w niniejszej publikacji, wówczas należy stosować sformułowania zawarte w tych aktach/w obiegu prawnym.

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa***.

Podmioty, urządzenia lub materiały o charakterze komercyjnym prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie.

Występujące w publikacji odwołania do materiałów wyszczególnianych w nawiasach kwadratowych [… ] odnoszą się do polskojęzycznych standardów NSC (np. [NSC 800-53], [NSC 800-37]) oraz ogólnodostępnych dokumentów anglojęzycznych (np. [SP 800-47], [CNSSI 1253]). Dokumenty te stanowią uzupełnienie i rozszerzenie wiedzy na temat szerokorozumianego cyberbezpieczeństwa.

# Spis treści

# ROZDZIAŁ CZWARTY

## PROCEDURY OCENY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

### CELE, METODY I PRZEDMIOT OCENY ŚRODKÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Niniejszy rozdział zawiera katalog procedur oceny środków bezpieczeństwa i ochrony prywatności oraz rozszerzeń tych zabezpieczeń zawartych w [NSC 800-53].[2] Oceniający wybierają procedury oceny z katalogu zgodnie z wytycznymi podanymi w punkcie 3.2. Treść planu bezpieczeństwa i prywatności stanowi podstawę do opracowania planów oceny bezpieczeństwa i prywatności oraz samych ocen. Jednocześnie oceniający najpewniej nie wykorzystają niektórych procedur zawartych w katalogu w przypadku gdy związane z tymi procedurami zabezpieczenia, środki ochrony prywatności lub mechanizmy rozszerzające nie są uwzględnione w planie bezpieczeństwa i prywatności dla danego systemu[3] lub jeśli takich mechanizmów nie ocenia się w danym czasie.

**SP 800-53A wer.2, Schemat procedury oceny**

Rozdział 2.4 zawiera przegląd procedur oceny, w tym konwencję nazewnictwa i numeracji, cele oceny, stwierdzenia określające funkcje, a także potencjalne metody i przedmioty oceny.

Załącznik C zawiera definicje metod oceny, odpowiednich obiektów oraz dodatkowe informacje o atrybutach oceny, tj. o głębokości i zakresie.

[2] Dokument [NSC 800-53] ma charakter rozstrzygający w odniesieniu do środków bezpieczeństwa lub ich rozszerzeń w przypadku różnic pomiędzy celami określonymi dla oceny środków bezpieczeństwa i ochrony prywatności a podstawowymi założeniami dla takich środków, zdefiniowanymi w najnowszej wersji NSC 800-53.

[3] Wdrożenie ram zarządzania ryzykiem (*ang.: Risk Management Framework — RMF*) obejmuje wybór wstępnego zestawu środków bezpieczeństwa i ochrony prywatności stosowanego w ramach systemu organizacyjnego lub przez niego odziedziczonych, po którym następuje proces dostosowywania tychże środków. Proces ten często skutkuje zmianą zestawu środków bezpieczeństwa i ochrony prywatności zawartego w ostatecznym planie bezpieczeństwa i planie programu ochrony prywatności. Dlatego też wybór procedur oceny z katalogu opiera się wyłącznie na treści planu lub planów w formie funkcjonującej po zakończeniu działań dostosowawczych.

Indywidualne przedmioty oceny mogą występować na wielu listach w ramach różnych procedur oceny. Takie przedmioty mogą być również stosowane w wielu kontekstach, aby uzyskać potrzebne informacje lub dowody dla danego aspektu oceny. Oceniający korzystają z ogólnych odniesień w celu uzyskania informacji niezbędnych do dokonania określonych ustaleń wymaganych przez cel oceny. Przykładowo w procedurach oceny dla kategorii AC-02 i AC-07 pojawia się odniesienie do polityki kontroli dostępu. W przypadku procedury oceny AC-02 oceniający korzystają z polityki kontroli dostępu, aby znaleźć informacje o tej części polityki, która dotyczy zarządzania kontami w systemie. W przypadku procedury oceny AC-07 oceniający korzystają z polityki kontroli dostępu, aby znaleźć informacje o tej części polityki, która dotyczy nieudanych prób logowania do systemu.

Oceniający zobowiązani są łączyć i konsolidować procedury oceny, ilekroć jest to możliwe lub praktyczne. Optymalizacja procedur pozwala zaoszczędzić czas oraz zmniejszyć koszty oceny i zmaksymalizować użyteczność jej wyników. Oceniający muszą optymalizować procedury oceny poprzez określenie ich możliwie najlepszej kolejności.

Dokonanie oceny niektórych środków bezpieczeństwa i ochrony prywatności przed innymi może dostarczyć informacji, które ułatwią zrozumienie i ocenę innych zabezpieczeń.[4]

Procedury oceny publikowane są w wielu formatach danych, w tym w pliku wartości rozdzielonych przecinkami (CSV), zwykłym pliku tekstowym oraz Open Security Controls Assessment (OSCAL).

Dostępne formaty danych można znaleźć na stronie dot. publikacji NIST SP 800-53A wer. 5 pod adresem:

https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final.

Repozytorium GitHub dotyczące OSCAL dostępne jest pod adresem: https://github.com/usnistgov/oscal-content.

[4] Dodatkowe informacje na temat optymalizacji procedur oceny znajdują się w rozdziale 3.2.5.

**UWAGA**

W poniższym katalogu procedur oceny zawarto **zestaw potencjalnych metod oceny**, przy czym nie są to metody obowiązkowe, ani też nie są jedynymi, które mają zastosowanie. W zależności od szczególnych okoliczności ocenianego systemu lub organizacji, konkretne metody mogą być obowiązkowe, a także może wystąpić konieczność zastosowania innych.

Zestaw **potencjalnych przedmiotów oceny** wymienionych w katalogu również nie jest obowiązkowy. Ma on raczej stanowić zbiór, z którego można wybrać niezbędny, wystarczający zestaw przedmiotów dla danej oceny, aby dokonać odpowiednich ustaleń. Głównymi czynnikami decydującymi o wyborze odpowiednich metod i przedmiotów oceny są organizacyjne wymogi bezpieczeństwa i inne czynniki związane z zarządzaniem ryzykiem (np. kategoryzacja systemu czy poziom tolerancji ryzyka organizacji).

**PORADY DOTYCZĄCE REALIZACJI**

**PORADA 1:** Do oceny należy włączyć tylko te procedury z rozdziału 4, które odpowiadają zabezpieczeniom i rozszerzonym zabezpieczeniom w zatwierdzonym planie bezpieczeństwa systemu i planie ochrony prywatności.

**PORADA 2:** Wybrane z rozdziału 4 procedury oceny są procedurami przykładowymi, które służą jako punkt wyjścia dla organizacji przygotowujących się do oceny. Procedury te są w razie potrzeby dostosowywane przez oceniających zgodnie ze wskazówkami zawartymi w rozdziale 3.2.3 w celu dostosowania do konkretnych wymagań organizacyjnych i środowisk operacyjnych.

**PORADA 3:** W odniesieniu do procedur oceny zawartych w rozdziale 4 oceniający muszą stosować tylko te procedury, metody i obiekty, które są niezbędne do podjęcia ostatecznej decyzji o tym, że dany wymóg dot. środków bezpieczeństwa jest „spełniony” lub „niespełniony” (patrz punkt 3.3).

**PORADA 4:** Do każdej metody oceny oceniający stosują wartości „głębokości" i „zasięgu" (opisane w Załączniku C), które są współmierne do charakterystyki systemu (w tym wymagań dotyczących zapewnienia bezpieczeństwa) i konkretnej czynności w zakresie oceny, która wspiera proces weryfikacji skuteczności poddawanych przeglądowi zabezpieczeń. Wartości wybrane dla atrybutów głębokości i zasięgu wskazują na względny wysiłek wymagany przy stosowaniu metody oceny do przedmiotu oceny (tj. rygor i zakres działań związanych z oceną). Atrybuty głębokości i zasięgu nie występują we wszystkich procedurach oceny w niniejszym dokumencie. Można je przedstawić w następujący sposób:

**Wywiad:** [wybór wartości atrybutów: <głębokość>, <zasięg>].

[WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sporządzanie i wdrażanie planu awaryjnego].

**PORADA 5:** Oceniający mogą znaleźć przydatne informacje związane z oceną w sekcji „Uwagi i zabezpieczenia powiązane" przy każdym zabezpieczeniu opisanym w [NSC 800-53]. Informacje zawarte w tej sekcji można wykorzystać do przeprowadzenia bardziej efektywnej weryfikacji w zakresie stosowania procedur oceny i ponownego wykorzystania artefaktów oceny.

**PORADA 6:** W przypadku zabezpieczeń z ODP[5], wartości ODP są definiowane podczas etapu *Wybór* procedury RMF i aktualizowane w razie potrzeby podczas etapów *Wdrażanie* i *Monitorowanie* tego procesu. Jeżeli wartości ODP nie są zdefiniowane i wdrożone, skuteczność środka nie może być zweryfikowana, co skutkuje oceną „niespełnione".

**PORADA 7:** Organizacje mogą wykorzystać niniejszą publikację lub formaty danych pochodnych, aby łatwo zidentyfikować wszelkie parametry zabezpieczeń, których wartości należy zdefiniować. Definicje ODP są wyróżnione na liście procedur oceny i mogą być filtrowane przy użyciu słowa kluczowego *„_ODP"* lub *„XX-nn_ODP"* (gdzie *XX to* dwucyfrowe oznaczenie kategorii zabezpieczeń, a *nn to* numer zabezpieczenia).

[5] Parametr zdefiniowany przez organizację (*ang. organization-defined parameter - ODP*)

**Uwaga:** Oceniając zgodność organizacji z rekomendacjami NSC biegli rewidenci, lub inni oceniający biorą pod uwagę fundamentalne założenia koncepcji i zasad bezpieczeństwa i prywatności zawartych w poszczególnych wytycznych oraz sposób, w jaki organizacja zastosowała te wytyczne w kontekście swoich szczególnych zadań, środowisk operacyjnych i unikalnych warunków organizacyjnych.

## 4.1. KATEGORIA AC - KONTROLA DOSTĘPU

| | | |
|---|---|---|
| **AC-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-01_ODP[01]** | ***określono personel lub role, do których ma zostać przekazana informacja o zasadach polityki kontroli dostępu;*** |
| | **AC-01_ODP[02]** | ***określono personel lub role, którym należy przekazać procedury kontroli dostępu;*** |
| | **AC-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **AC-01_ODP[04]** | ***określono pracownika funkcyjnego odpowiedzialnego za zarządzanie polityką i procedurami kontroli dostępu;*** |
| | **AC-01_ODP[05]** | ***określono częstotliwość, z jaką polityka kontroli dostępu jest przeglądana i aktualizowana;*** |
| | **AC-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji obowiązującej polityki kontroli dostępu;*** |
| | **AC-01_ODP[07]** | ***określono częstotliwość, z jaką aktualne procedury kontroli dostępu są przeglądane i aktualizowane;*** |
| | **AC-01_ODP[08]** | ***określono zdarzenia skutkujące koniecznością przeprowadzenia przeglądu i aktualizacji procedur;*** |
| | **AC-01a.[01]** | opracowano i udokumentowano politykę kontroli dostępu; |
| | **AC-01a.[02]** | informacje o polityce kontroli przekazano ***<personelowi lub roli AC-01_ODP[01]>***; |
| | **AC-01a.[03]** | opracowano i udokumentowano procedury kontroli dostępu ułatwiające wdrożenie politykę kontroli dostępu i związane z nią środki; |

| AC-01 | POLITYKA I PROCEDURY | |
|---|---|---|
| | **AC-01a.[04]** | informacje o polityce kontroli przekazano ***<personelowi lub roli AC-01_ODP[02]>***; |
| | **AC-01a.01(a)[01]** | polityka kontroli dostępu ***<WYBRANA WARTOŚĆ PARAMETRU AC-01_ODP[03]>*** odnosi się do celu; |
| | **AC-01a.01(a)[02]** | Polityka kontroli dostępu ***<WYBRANA WARTOŚĆ PARAMETRU AC-01_ODP[03]>*** odnosi się do zakresu; |
| | **AC-01a.01(a)[03]** | Polityka kontroli dostępu ***<WYBRANA WARTOŚĆ PARAMETRU AC-01_ODP[03]>*** odnosi się do ról; |
| | **AC-01a.01(a)[04]** | polityka kontroli dostępu ***<WYBRANA WARTOŚĆ PARAMETRU AC-01_ODP[03]>*** odnosi się do obowiązków; |
| | **AC-01a.01(a)[05]** | polityka kontroli dostępu ***<WYBRANA WARTOŚĆ PARAMETRU AC-01_ODP[03]>*** odnosi się do zobowiązań kierownictwa; |
| | **AC-01a.01(a)[06]** | polityka kontroli dostępu ***<WYBRANA WARTOŚĆ PARAMETRU AC-01_ODP[03]>*** odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **AC-01a.01(a)[07]** | polityka kontroli dostępu ***<WYBRANA WARTOŚĆ PARAMETRU AC-01_ODP[03]>*** odnosi się do zgodności; |
| | **AC-01a.01(b)** | polityka kontroli dostępu ***<WYBRANA WARTOŚĆ PARAMETRU AC-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **AC-01b.** | ***<urzędnik AC-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur kontroli dostępu; |
| | **AC-01c.01[01]** | aktualna polityka kontroli dostępu jest przeglądana i aktualizowana z ***<częstotliwością AC-01_ODP[05] >***; |

| | | |
|---|---|---|
| **AC-01** | **POLITYKA I PROCEDURY** | |
| | **AC-01c.01[02]** | aktualna polityka kontroli dostępu jest przeglądana i aktualizowana po ***<zdarzeniach AC-01_ODP[06]>***; |
| | **AC-01c.02[01]** | aktualne procedury kontroli dostępu są przeglądane i aktualizowane z ***<częstotliwością AC-01_ODP[07]>***; |
| | **AC-01c.02[02]** | aktualne procedury kontroli dostępu są przeglądane i aktualizowane po ***<zdarzeniach AC-01_ODP[08]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury kontroli dostępu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **AC-02** | **ZARZĄDZANIE KONTAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02_ODP[01]** | ***określono warunki wstępne i kryteria przynależności do grup i ról;*** |
| | **AC-02_ODP[02]** | ***określono atrybuty (w zależności od potrzeb) dla każdego konta;*** |
| | **AC-02_ODP[03]** | ***określono personel lub role wymagane do zatwierdzania wniosków o utworzenie konta;*** |
| | **AC-02_ODP[04]** | ***określono politykę, procedury, warunki wstępne i kryteria tworzenia, włączania, modyfikacji, wyłączania i usuwania kont;*** |
| | **AC-02_ODP[05]** | ***określono personel lub role, które mają być notyfikowane;*** |

| AC-02 | ZARZĄDZANIE KONTAMI | |
|---|---|---|
| | **AC-02_ODP[06]** | ***określono okres, w którym należy powiadomić administratora konta, gdy konto nie jest już potrzebne;*** |
| | **AC-02_ODP[07]** | ***określono okres, w którym należy powiadomić administratora konta o zakończeniu stosunku pracy/przeniesieniu użytkownika;*** |
| | **AC-02_ODP[08]** | ***określono okres, w którym należy powiadomić administratora konta o zmianach w zakresie użytkowania systemu lub wiedzy koniecznej dotyczących danej osoby.*** |
| | **AC-02_ODP[09]** | ***określono atrybuty wymagane do autoryzacji dostępu do systemu (w zależności od potrzeb);*** |
| | **AC-02_ODP[10]** | ***określono częstotliwość przeglądów kont;*** |
| | **AC-02a.[01]** | określono i udokumentowano typy kont dopuszczonych do użytku w systemie; |
| | **AC-02a.[02]** | określono i udokumentowano typy kont, których użytkowanie w systemie jest zabronione; |
| | **AC-02b.** | wyznaczono zarządzających kontami; |
| | **AC-02c.** | ustalono ***<warunki wstępne i kryteria AC-02_ODP[01] >*** dla przypisania do roli lub grupy; |
| | **AC-02d.01** | określono autoryzowanych użytkowników systemu; |
| | **AC-02d.02** | określono przynależność do grupy i roli; |
| | **AC-02d.03[01]** | dla każdego konta określono uprawnienia dostępu; |
| | **AC-02d.03[02]** | ***określono <atrybuty AC-02_ODP[02]>(w zależności od potrzeb)*** *dla każdego konta;* |
| | **AC-02e.** | ***<AC-02_ODP[03] personel lub role>*** muszą uzyskać zatwierdzenie dla wniosku o utworzenie konta; |

| **AC-02** | **ZARZĄDZANIE KONTAMI** | |
|---|---|---|
| | **AC-02f.[01]** | konta są tworzone zgodnie z ***<AC-02_ODP[04] polityką, procedurami, warunkami* wstępnymi *i kryteriami>;*** |
| | **AC-02f.[02]** | konta są aktywowane zgodnie z ***<AC-02_ODP[04] polityką, procedurami, warunkami* wstępnymi *i kryteriami>;*** |
| | **AC-02f.[03]** | konta są modyfikowane zgodnie z ***<AC-02_ODP[04] polityką, procedurami, warunkami* wstępnymi *i kryteriami>;*** |
| | **AC-02f.[04]** | konta są wyłączane zgodnie z ***<AC-02_ODP[04] polityką, procedurami, warunkami* wstępnymi *i kryteriami>;*** |
| | **AC-02f.[05]** | konta są usuwane zgodnie z ***<AC-02_ODP[04] polityką, procedurami, warunkami* wstępnymi *i kryteriami>;*** |
| | **AC-02g.** | wykorzystanie kont jest monitorowane; |
| | **AC-02h.01** | zarządzający kontami i ***<AC-02_ODP[05] osoba lub rola>*** otrzymują powiadomienia w ciągu ***<okresu AC-02_ODP[06]>***, gdy konta nie są już potrzebne; |
| | **AC-02h.02** | zarządzający kontami i ***<AC-02_ODP[05] osoba lub rola>*** otrzymują powiadomienia w ciągu ***<okresu AC-02_ODP[07]> od*** momentu zakończenia stosunku pracy/przeniesienia użytkownika; |
| | **AC-02h.03** | zarządzający kontami i ***<AC-02_ODP[05] osoba lub rola>*** otrzymują powiadomienia w ciągu ***<okresu AC-02_ODP[08]> o*** zmianach w zakresie użytkowania systemu lub wiedzy koniecznej dotyczących danej osoby; |
| | **AC-02i.01** | dostęp do systemu jest weryfikowany poprzez podanie ważnej autoryzacji dostępu; |
| | **AC-02i.02** | dostęp do systemu jest weryfikowany poprzez potwierdzenie, że jest on użytkowany zgodnie z przeznaczeniem; |
| | **AC-02i.03** | dostęp do systemu jest weryfikowany na podstawie ***<atrybutów AC-02_ODP[09] (w zależności od potrzeb)>***; |

| **AC-02** | **ZARZĄDZANIE KONTAMI** | |
|---|---|---|
| | **AC-02j.** | konta są sprawdzane pod kątem zgodności z wymogami zarządzania kontami z ***<częstotliwością AC-02_ODP[10]>***; |
| | **AC-02k.[01]** | ustanowiono proces zmiany metod uwierzytelniania kont współdzielonych lub grupowych (jeśli zostały wdrożone) w przypadku usunięcia osób z grupy; |
| | **AC-02k.[02]** | wdrożono proces zmiany metod uwierzytelniania kont współdzielonych lub grupowych (jeśli zostały wdrożone) w przypadku usunięcia osób z grupy; |
| | **AC-02l.[01]** | procesy zarządzania kontami są dostosowane do procesu zakończenia stosunku pracy z pracownikami; |

| **AC-02(01)** | **ZARZĄDZANIE KONTAMI \| AUTOMATYCZNE ZARZĄDZANIE KONTEM SYSTEMU** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02(01)_ODP** | ***określono automatyczne mechanizmy wspomagające zarządzanie kontami systemowymi;*** |
| | **AC-02(01)** | zarządzanie kontami systemowymi jest wspierane za pomocą ***<mechanizmów automatycznych AC-02(01)_ODP >***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-02(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-02(01)** | **ZARZĄDZANIE KONTAMI \| AUTOMATYCZNE ZARZĄDZANIE KONTEM SYSTEMU** | |
| | **AC-02(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-02(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające funkcje zarządzania kontami]. |

| | | |
|---|---|---|
| **AC-02(02)** | **ZARZĄDZANIE KONTAMI \| AUTOMATYCZNE ZARZĄDZANIE KONTEM CZASOWYM \| AWARYJNYM** | |
| | **CEL OCENY:**<br>**Ustalenie, czy:** | |
| | **AC-02(02)_ODP[01]** | **wybrano jedną z następujących WARTOŚCI PARAMETRÓW: {usuń; wyłącz};** |
| | **AC-02(02)_ODP[02]** | ***określono okres, po którym konta tymczasowe lub awaryjne zostaną automatycznie usunięte;*** |
| | **AC-02(02)** | konta tymczasowe i awaryjne są automatycznie ***<WYBRANA WARTOŚĆ PARAMETRU AC-02(02)_ODP[01]> po <okresie AC-02(02)_ODP[02] >***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista usuniętych lub wyłączonych kont tymczasowych; wygenerowana przez system lista usuniętych lub wyłączonych kont awaryjnych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-02(02)** | **ZARZĄDZANIE KONTAMI \| AUTOMATYCZNE ZARZĄDZANIE KONTEM CZASOWYM \| AWARYJNYM** | |
| | **AC-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-02(02)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające funkcje zarządzania kontami]. |

| | | |
|---|---|---|
| **AC-02(03)** | **ZARZĄDZANIE KONTAMI \| WYŁĄCZANIE KONT** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02(03)_ODP[01]** | ***określono okres, w którym należy wyłączyć konta;*** |
| | **AC-02(03)_ODP[02]** | ***określono czas bezczynności konta przed jego wyłączeniem;*** |
| | **AC-02(03)(a)** | konta są wyłączane w ciągu ***<okres AC-02(03)_ODP[01]> po ich*** wygaśnięciu; |
| | **AC-02(03)(b)** | konta są wyłączane w ciągu ***<okres AC-02(03)_ODP[01]>***, gdy nie są już powiązane z użytkownikiem lub osobą; |
| | **AC-02(03)(c)** | konta są wyłączane w ciągu ***<okres AC-02(03)_ODP[01]>***, jeśli łamią zasady polityki organizacji; |
| | **AC-02(03)(d)** | konta są wyłączane w ciągu ***<okres AC-02(03)_ODP[01]>***, jeśli pozostawały nieaktywne przez ***<okres AC-02(03)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **AC-02(03)** | **ZARZĄDZANIE KONTAMI \| WYŁĄCZANIE KONT** | |
|---|---|---|
| | **AC-02(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zarządzania kontami; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista usuniętych lub wyłączonych kont tymczasowych; wygenerowana przez system lista usuniętych lub wyłączonych kont awaryjnych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-02(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-02(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje zarządzania kontami]. |

| **AC-02(04)** | **ZARZĄDZANIE KONTAMI \| AUTOMATYCZNE DZIAŁANIA AUDYTOWE** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02(04)[01]** | proces tworzenia kont podlega automatycznemu audytowi; |
| | **AC-02(04)[02]** | proces modyfikacji kont podlega automatycznemu audytowi; |
| | **AC-02(04)[03]** | proces aktywacji kont podlega automatycznemu audytowi; |
| | **AC-02(04)[04]** | proces wyłączania kont podlega automatycznemu audytowi; |
| | **AC-02(04)[05]** | proces usuwania kont podlega automatycznemu audytowi; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-02(04)** | **ZARZĄDZANIE KONTAMI \| AUTOMATYCZNE DZIAŁANIA AUDYTOWE** | |
| | **AC-02(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; powiadomienia/alarmy o utworzeniu, modyfikacji, aktywowaniu, wyłączeniu lub usunięciu konta; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-02(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-02(04)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające funkcje zarządzania kontami]. |

| | | |
|---|---|---|
| **AC-02(05)** | **ZARZĄDZANIE KONTAMI \| WYLOGOWANIE PRZEZ UŻYTKOWNIKA PO OKREŚLONYM OKRESIE NIEAKTYWNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02(05)_ODP** | ***określono okres bezczynności przed wylogowaniem lub zapewniono instrukcje co do tego, kiedy należy się wylogować;*** |
| | **AC-02(05)** | użytkownicy są wylogowywani, gdy ***<okres bezczynności lub opis, kiedy należy się wylogować AC-02(05)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-02(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; raporty o naruszeniu bezpieczeństwa; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-02(05)** | **ZARZĄDZANIE KONTAMI \| WYLOGOWANIE PRZEZ UŻYTKOWNIKA PO OKREŚLONYM OKRESIE NIEAKTYWNOŚCI** | |
| | **AC-02(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; użytkownicy zobowiązani stosować się do polityki wylogowywania z powodu bezczynności]. |

| | | |
|---|---|---|
| **AC-02(06)** | **ZARZĄDZANIE KONTAMI \| DYNAMICZNE ZARZĄDZANIE UPRAWNIENIAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02(06)_ODP** | ***ustanowiono zdolności do dynamicznego zarządzania uprawnieniami;*** |
| | **AC-02(06)** | wdrożono***<zdolności do dynamicznego zarządzania uprawnieniami AC-02(06)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-02(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista możliwości dynamicznego zarządzania uprawnieniami; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-02(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-02(06)-Test** | [WYBÓR SPOŚRÓD: system lub mechanizmy wdrażające zdolności dynamicznego zarządzania uprawnieniami]. |

| | | |
|---|---|---|
| **AC-02(07)** | **ZARZĄDZANIE KONTAMI \| UPRZYWILEJOWANE KONTA UŻYTKOWNIKÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02(07)_ODP** | ***wybrano jedną z następujących WARTOŚCI PARAMETRÓW: {schemat dostępu oparty na rolach; schemat dostępu oparty na atrybutach};*** |
| | **AC-02(07)(a)** | konta użytkowników uprzywilejowanych są tworzone i zarządzane zgodnie z<br>***<WYBRANA WARTOŚĆ PARAMETRU AC-02(07)_ODP >***; |
| | **AC-02(07)(b)** | monitoruje się przypisane uprzywilejowane role i atrybuty; |
| | **AC-02(07)(c)** | monitoruje się zmiany w zakresie ról i atrybutów; |
| | **AC-02(07)(d)** | dostęp jest blokowany, gdy przypisane uprzywilejowane role i atrybuty nie są już właściwe. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-02(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowany przez system lista kont użytkowników uprzywilejowanych i związanych z nimi ról; zapisy działań podejmowanych, gdy przypisane uprzywilejowane role nie są już właściwe; zapisy z audytu systemu; raporty ze śledzenia i monitorowania audytu; zapisy z monitorowania systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-02(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-02(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje zarządzania kontami; mechanizmy monitorujące nadawanie ról uprzywilejowanych]. |

| | | |
|---|---|---|
| **AC-02(08)** | **ZARZĄDZANIE KONTAMI \| DYNAMICZNE ZARZĄDZANIE KONTAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02(08)_ODP** | ***określono konta systemowe tworzone, aktywowane, zarządzane i wyłączane w sposób dynamiczny;*** |
| | **AC-02(08)[01]** | ***<konta systemowe AC-02(08)_ODP>*** są tworzone dynamicznie; |
| | **AC-02(08)[02]** | ***<konta systemowe AC-02(08)_ODP>*** są aktywowane dynamicznie; |
| | **AC-02(08)[03]** | ***<konta systemowe AC-02(08)_ODP>*** są zarządzane dynamicznie; |
| | **AC-02(08)[04]** | ***<konta systemowe AC-02(08)_ODP>*** są wyłączane dynamicznie; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-02(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista kont systemowych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-02(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-02(08)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające funkcje zarządzania kontami]. |

| | | |
|---|---|---|
| **AC-02(09)** | **ZARZĄDZANIE KONTAMI \| OGRANICZENIA W KORZYSTANIU Z KONT WSPÓLNYCH I GRUPOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02(09)_ODP** | ***określono warunki tworzenia kont wspólnych i grupowych;*** |
| | **AC-02(09)** | użycie kont współdzielonych i grupowych jest dozwolone tylko wtedy, gdy spełnione są ***<warunki AC-02(09)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-02(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista kont wspólnych/grupowych i związanych z nimi ról; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-02(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-02(09)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje zarządzania kontami wspólnymi/grupowymi]. |

| | |
|---|---|
| **AC-02(10)** | **ZARZĄDZANIE KONTAMI \| ZMIANA POŚWIADCZANIA UPRAWNIEŃ KONTA WSPÓLNEGO I GRUPOWEGO** |
| | [WYCOFANE: Włączone do AC-2k]. |

| | | |
|---|---|---|
| **AC-02(11)** | **ZARZĄDZANIE KONTAMI \| WARUNKI UŻYTKOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02(11)_ODP[01]** | ***określono okoliczności lub warunki użytkowania, które mają być egzekwowane w odniesieniu do kont systemowych;*** |
| | **AC-02(11)_ODP[02]** | ***określono konta systemowe podlegające egzekwowaniu okoliczności lub warunków użytkowania;*** |
| | **AC-02(11)** | egzekwowane są ***<okoliczności lub warunki użytkowania AC-02(11)_ODP[01] > w*** odniesieniu do ***<kont systemowych AC-02(11)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-02(11)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista kont systemowych i związane z nimi okoliczności lub warunki użytkowania; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-02(11)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-02(11)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające funkcje zarządzania kontami]. |

| | | |
|---|---|---|
| **AC-02(12)** | **ZARZĄDZANIE KONTAMI \| MONITOROWANIE KONT POD WZGLĘDEM NIETYPOWYCH ZASTOSOWAŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02(12)_ODP[01]** | ***określono rodzaje nietypowego użytkowania, pod kątem których należy monitorować konta systemowe;*** |
| | **AC-02(12)_ODP[02]** | ***określono personel lub role odpowiedzialne za zgłaszanie nietypowego użytkowania;*** |
| | **AC-02(12)(a)** | konta systemowe są monitorowane pod kątem ***<nietypowego użytkowania AC-02(12)_ODP[01]>***; |
| | **AC-02(12)(b)** | nietypowe użytkowanie kont systemowych jest zgłaszane do ***<personelu lub roli AC-02(12)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-02(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z monitorowania systemu; zapisy z audytu systemu; raporty ze śledzenia i monitorowania audytu; ocena wpływu na prywatność; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-02(12)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-02(12)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające funkcje zarządzania kontami]. |

| | | |
|---|---|---|
| **AC-02(13)** | **ZARZĄDZANIE KONTAMI \| WYŁĄCZANIE KONT DOSTĘPOWYCH UŻYTKOWNIKOM WYSOKIEGO RYZYKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-02(13)_ODP[01]** | ***określono okres, w którym należy wyłączyć konta osób uznanych za osoby wysokiego ryzyka;*** |
| | **AC-02(13)_ODP[02]** | ***określono istotne ryzyka, których wystąpienie skutkuje wyłączeniem konta;*** |
| | **AC-02(13)** | konta osób wyłączane są w ciągu ***<okresu AC-02(13)_ODP[01]>*** ***od*** odkrycia ***<znaczącego ryzyka AC-02(13)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-02(13)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury adresujące zarządzanie kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista wyłączonych kont; lista działań użytkownika stwarzających znaczące ryzyko dla organizacji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy] |
| | **AC-02(13)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-02(13)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające funkcje zarządzania kontami]. |

| | | |
|---|---|---|
| **AC-03** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03** | zatwierdzone uprawnienia do logicznego dostępu do informacji i zasobów systemu są egzekwowane zgodnie z obowiązującymi zasadami kontroli dostępu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista zatwierdzonych uprawnień użytkowników; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-03-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu]. |

| | |
|---|---|
| **AC-03(01)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| OGRANICZONY DOSTĘP DO FUNKCJI UPRZYWILEJOWANYCH** |
| | [WYCOFANE: Włączone do AC-06]. |

| **AC-03(02)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| PODWÓJNA AUTORYZACJA** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(02)_ODP** | ***określono polecenia uprzywilejowane lub inne działania wymagające podwójnej autoryzacji;*** |
| | **AC-03(02)** | w przypadku ***<AC-03(02)_ODP poleceń uprzywilejowanych lub innych działań>*** wymagana jest podwójna autoryzacja; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania dostępu i podwójnej autoryzacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista uprzywilejowanych poleceń wymagających podwójnej autoryzacji; lista działań wymagających podwójnej autoryzacji; lista zatwierdzonych uprawnień użytkowników<br>plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy] |
| | **AC-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-03(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy podwójnej autoryzacji wdrażające politykę kontroli dostępu]. |

| **AC-03(03)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| OBOWIĄZKOWA KONTROLA DOSTĘPU** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(03)_ODP[01]** | ***określono politykę obowiązkowej kontroli dostępu, egzekwowaną w odniesieniu do objętych nią podmiotów;*** |

| AC-03(03) | EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| OBOWIĄZKOWA KONTROLA DOSTĘPU | |
|---|---|---|
| | **AC-03(03)_ODP[02]** | ***określono politykę obowiązkowej kontroli dostępu, egzekwowaną w odniesieniu do objętych nią obiektów;*** |
| | **AC-03(03)_ODP[03]** | ***określono podmioty, którym bezwzględnie należy nadać uprawnienia;*** |
| | **AC-03(03)_ODP[04]** | ***określono uprawnienia, które bezwzględnie należy nadać podmiotom;*** |
| | **AC-03(03)[01]** | ***<AC-03(03)_ODP[01] polityka obowiązkowej kontroli dostępu>*** egzekwowana jest w odniesieniu do zbioru objętych nią podmiotów, określonych w jej treści; |
| | **AC-03(03)[02]** | ***<AC-03(03)_ODP[02] polityka uznaniowej kontroli dostępu>*** jest stosowana w odniesieniu do zbioru objętych nią obiektów, określonych w jej treści; |
| | **AC-03(03)(a)[01]** | ***<AC-03(03)_ODP[01] polityka obowiązkowej kontroli dostępu>*** egzekwowana jest w odniesieniu do zbioru objętych nią podmiotów, określonych w jej treści; |
| | **AC-03(03)(a)[02]** | ***<AC-03(03)_ODP[02] polityka obowiązkowej kontroli dostępu>*** egzekwowana jest jednolicie w odniesieniu do objętych nią podmiotów w systemie; |
| | **AC-03(03)(b)(01)** | ***<polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[01]> oraz <polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[02] >*** określające, że na podmiot, któremu przyznano dostęp do informacji, nakłada się ograniczenia co do przekazywania takich informacji nieuprawnionym podmiotom lub obiektom, są egzekwowane; |
| | **AC-03(03)(b)(02)** | ***<polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[01]> oraz <polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[02] >*** określające, że na podmiot, któremu przyznano dostęp do informacji, nakłada się ograniczenia co do przyznania jego uprawnień innym podmiotom, są egzekwowane. |

| AC-03(03) | EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| OBOWIĄZKOWA KONTROLA DOSTĘPU | |
|---|---|---|
| | **AC-03(03)(b)(03)** | ***<polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[01]> i <polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[02]>*** określające, że na podmiot, któremu przyznano dostęp do informacji, nakłada się ograniczenia co do zmiany jednego lub więcej atrybutów bezpieczeństwa i ich wartości (określonych przez politykę) w podmiotach, obiektach, systemie lub komponentach systemu, są egzekwowane; |
| | **AC-03(03)(b)(04)** | ***<polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[01]> i <polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[02]>*** określające, że na podmiot, któremu przyznano dostęp do informacji, nakłada się ograniczenia co do wyboru atrybutów bezpieczeństwa i wartości atrybutów (określonych przez politykę) powiązanych z nowo tworzonymi lub modyfikowanymi obiektami, są egzekwowane; |
| | **AC-03(03)(b)(05)** | ***<polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[01]> oraz <polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[02] >*** określające, że na podmiot, któremu przyznano dostęp do informacji, nakłada się ograniczenia co do zmiany zasad kontroli dostępu, są egzekwowane; |
| | **AC-03(03)(c)** | ***<polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[01]>*** oraz ***<polityka obowiązkowej kontroli dostępu AC-03(03)_ODP[02] >*** określające, że ***<podmiotom AC-03(03)_ODP[03]>*** można jednoznacznie nadać takie***<uprawnienia AC-03(03)_ODP[04]>***,które nie są one ograniczone żadnym z ww. podzbiorów ograniczeń (lub przez wszystkie z nich), są egzekwowane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| AC-03(03) | EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| OBOWIĄZKOWA KONTROLA DOSTĘPU | |
|---|---|---|
| | **AC-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka obowiązkowej kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista podmiotów i obiektów (tj. użytkowników i zasobów) wymagających egzekwowania polityki obowiązkowej kontroli dostępu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-03(03)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające obowiązkową kontrolę dostępu]. |

| AC-03(04) | EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| UZNANIOWA KONTROLA DOSTĘPU | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(04)_ODP[01]** | ***określono zasady uznaniowej kontroli dostępu do zbioru objętych nią podmiotów;*** |
| | **AC-03(04)_ODP[02]** | ***określono zasady uznaniowej kontroli dostępu do zbioru objętych nią podmiotów;*** |
| | **AC-03(04)[01]** | ***<AC-03(04)_ODP[01] polityka uznaniowej kontroli dostępu>*** jest stosowana w odniesieniu do zbioru objętych nią podmiotów określonych w polityce; |
| | **AC-03(04)[02]** | ***<AC-03(04)_ODP[02] polityka uznaniowej kontroli dostępu>*** jest stosowana w odniesieniu do zbioru objętych nią podmiotów określonych w polityce; |

| AC-03(04) | EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| UZNANIOWA KONTROLA DOSTĘPU | |
|---|---|---|
| | **AC-03(04)(a)** | ***<AC-03(04)_ODP[01] polityka uznaniowej kontroli dostępu> i <AC-03(04)_ODP[02] polityka uznaniowej kontroli dostępu>*** jest stosowana, gdy polityka określa, że<br>podmiot, który uzyskał dostęp do informacji, może przekazać takie informacje innym podmiotom lub obiektom; |
| | **AC-03(04)(b)** | ***<AC-03(04)_ODP[01] polityka uznaniowej kontroli dostępu> i <AC-03(04)_ODP[02] polityka uznaniowej kontroli dostępu>*** są stosowane w przypadku gdy polityka określa, że podmiot, który otrzymał dostęp do informacji, może przekazywać swoje uprawnienia innym podmiotom; |
| | **AC-03(04)(c)** | ***<AC-03(04)_ODP[01] polityka uznaniowej kontroli dostępu> i <AC-03(04)_ODP[02] polityka uznaniowej kontroli dostępu>*** są stosowane w przypadku gdy polityka określa, że podmiot, który uzyskał dostęp do informacji, może zmienić zabezpieczenia atrybutów w podmiotach, obiektach, systemie lub komponentach systemu; |
| | **AC-03(04)(d)** | ***<AC-03(04)_ODP[01] polityka uznaniowej kontroli dostępu> i <AC-03(04)_ODP[02] polityka uznaniowej kontroli dostępu>*** jest stosowana, gdy polityka określa, że<br>podmiot, który uzyskał dostęp do informacji, może wybrać zabezpieczenia atrybutów, które będą powiązane z nowo utworzonymi lub zmienionymi obiektami; |
| | **AC-03(04)(e)** | ***<AC-03(04)_ODP[01] polityka uznaniowej kontroli dostępu> i <AC-03(04)_ODP[02] polityka uznaniowej kontroli dostępu>*** są stosowane w przypadku gdy polityka określa, że podmiot, który uzyskał dostęp do informacji, może zmienić zasady kontroli dostępu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| AC-03(04) | EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| UZNANIOWA KONTROLA DOSTĘPU | |
|---|---|---|
| | **AC-03(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka uznaniowej kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista podmiotów i obiektów (tj. użytkowników i zasobów) wymagających egzekwowania polityki uznaniowej kontroli dostępu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-03(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-03(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę uznaniowej kontroli dostępu]. |

| AC-03(05) | EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| INFORMACJE DOTYCZĄCE BEZPIECZEŃSTWA | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(05)_ODP** | ***określono istotne z punktu widzenia bezpieczeństwa informacje, do których dostęp został uniemożliwiony w każdym przypadku, z wyjątkiem bezpiecznych sytuacji, gdy system nie jest użytkowany;*** |
| | **AC-03(05)** | Dostęp do ***<informacji związanych z bezpieczeństwem AC-03(05)_ODP>*** został uniemożliwiony, z wyjątkiem bezpiecznych sytuacji, gdy system nie jest użytkowany. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-03(05)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| INFORMACJE DOTYCZĄCE BEZPIECZEŃSTWA** | |
| | **AC-03(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-03(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-03(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy uniemożliwiające dostęp do informacji istotnych dla bezpieczeństwa w systemie]. |

| | | |
|---|---|---|
| **AC-03(06)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| OCHRONA INFORMACJI UŻYTKOWNIKA I SYSTEMU** | |
| | [WYCOFANE: Włączone do MP-04, SC-28]. | |

| | | |
|---|---|---|
| **AC-03(07)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| KONTROLA DOSTĘPU OPARTA NA ROLI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(07)_ODP[01]** | ***określono role, na których może opierać się kontrola dostępu;*** |
| | **AC-03(07)_ODP[02]** | ***określono użytkowników upoważnionych do objęcia ról (zdefiniowanych w AC-03(07)_ODP[01]);*** |
| | **AC-03(07)[01]** | polityka kontroli dostępu opartej na rolach jest egzekwowana w odniesieniu do zdefiniowanych podmiotów; |

| | | |
|---|---|---|
| **AC-03(07)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| KONTROLA DOSTĘPU OPARTA NA ROLI** | |
| | **AC-03(07)[02]** | polityka kontroli dostępu opartej na rolach jest egzekwowana w odniesieniu do zdefiniowanych obiektów; |
| | **AC-03(07)[03]** | kontrola dostępu jest realizowana na podstawie ***<ról AC-03(07)_ODP[01]>*** oraz***<użytkowników upoważnionych do objęcia takich ról AC-03(07)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-03(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli dostępu oparta na rolach; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista ról, użytkowników i związanych z nimi uprawnień wymaganych do kontroli dostępu do systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-03(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-03(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu opartą na rolach]. |

| | | |
|---|---|---|
| **AC-03(08)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| COFNIĘCIE ZEZWOLEŃ NA DOSTĘP** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(08)_ODP** | ***określono zasady wyznaczające termin cofnięcia uprawnień dostępu;*** |

| | | |
|---|---|---|
| **AC-03(08)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| COFNIĘCIE ZEZWOLEŃ NA DOSTĘP** | |
| | **AC-03(08)[01]** | egzekwuje się cofanie uprawnień dostępu, wynikające ze zmian atrybutów bezpieczeństwa podmiotów na podstawie ***<zasad AC-03(08)_ODP>***; |
| | **AC-03(08)[02]** | egzekwuje się cofanie uprawnień dostępu, wynikające ze zmian atrybutów bezpieczeństwa obiektów na podstawie ***<zasad AC-03(08)_ODP>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-03(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zasady regulujące cofanie uprawnień dostępu, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-03(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-03(08)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania uprawnień dostępu]. |

| | | |
|---|---|---|
| **AC-03(09)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| KONTROLOWANE UDOSTĘPNIENIE INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(09)_ODP[01]** | ***określono system zewnętrzny lub komponent systemu, któremu należy udostępnić informację;*** |

| | | |
|---|---|---|
| **AC-03(09)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| KONTROLOWANE UDOSTĘPNIENIE INFORMACJI** | |
| | **AC-03(09)_ODP[02]** | ***określono środki, które mają być zapewnione przez system zewnętrzny lub komponent systemu (zdefiniowane w AC-03(09)_ODP[01]);*** |
| | **AC-03(09)_ODP[03]** | ***określono środki stosowane w celu weryfikacji, czy informacja przeznaczona do udostępnienia jest odpowiednia;*** |
| | **AC-03(09)(a)** | informacja jest udostępniana poza systemem tylko wtedy, gdy otrzymujący ją ***<system lub element systemu AC-03(09)_ODP[01]>*** zapewnia odpowiednie ***<zabezpieczenia AC-03(09)_ODP[02]>***; |
| | **AC-03(09)(b)** | informacja jest udostępniana poza systemem tylko wtedy, gdy***<zabezpieczenia AC-03(09)_ODP[03]>*** są używane w celu potwierdzenia, że informacje przeznaczone do przekazania są odpowiednie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-03(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista środków bezpieczeństwa i ochrony prywatności zapewnianych przez system odbiorczy lub komponenty systemu; lista środków bezpieczeństwa i ochrony prywatności potwierdzających stosowność informacji przeznaczonych do udostępnienia; zapisy z audytu systemu; wyniki ocen okresowych (inspekcji/testów) systemu zewnętrznego; umowy o udostępnianiu informacji; protokoły ustaleń; przejęcia/umowy; plan bezpieczeństwa systemu; plan ochrony prywatności; inne stosowne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-03(09)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| KONTROLOWANE UDOSTĘPNIENIE INFORMACJI** | |
| | **AC-03(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; personel organizacyjny odpowiedzialny za przejęcia/umowy; radca prawny; programiści systemu]. |
| | **AC-03(09)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania uprawnień dostępu]. |

| | | |
|---|---|---|
| **AC-03(10)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| NADZOROWANE OBEJŚCIE MECHANIZMÓW KONTROLI DOSTĘPU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(10)_ODP[01]** | ***określono warunki, w których należy zastosować kontrolowane obejście automatycznych mechanizmów kontroli dostępu;*** |
| | **AC-03(10)_ODP[02]** | ***określono role upoważnione do obejścia automatycznych mechanizmów kontroli dostępu;*** |
| | **AC-03(10)** | kontrolowane obejście mechanizmów automatycznej kontroli dostępu stosowane jest w ***<warunkachAC-03(10)_ODP[01]>*** przez ***<role AC-03(10)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-03(10)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| NADZOROWANE OBEJŚCIE MECHANIZMÓW KONTROLI DOSTĘPU** | |
| | **AC-03(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; warunki stosowania kontrolowanego obejścia mechanizmów automatycznej kontroli dostępu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-03(10)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **AC-03(10)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania uprawnień dostępu]. |

| | | |
|---|---|---|
| **AC-03(11)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| OGRANICZENIE DOSTĘPU DO OKREŚLONYCH RODZAJÓW INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(11)_ODP** | ***określono typy informacji wymagające ograniczonego dostępu do repozytoriów danych;*** |
| | **AC-03(11)** | dostęp do repozytoriów danych zawierających ***<typy informacji AC-03(11)_ODP>*** jest ograniczony. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-03(11)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| OGRANICZENIE DOSTĘPU DO OKREŚLONYCH RODZAJÓW INFORMACJI** | |
| | **AC-03(11)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-03(11)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; personel organizacyjny odpowiedzialny za repozytoria danych; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-03(11)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania uprawnień dostępu]. |

| | | |
|---|---|---|
| **AC-03(12)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| ZAPEWNIENIE I EGZEKWOWANIE DOSTĘPU DO APLIKACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(12)_ODP** | ***określono aplikacje systemowe i funkcje wymagające zapewnienia dostępu;*** |
| | **AC-03(12)(a)** | w ramach procesu instalacji aplikacje muszą zapewnić dostęp do następujących aplikacji i funkcji systemu: ***<aplikacje i funkcje systemu AC-03(12)_ ODP>***; |
| | **AC-03(12)(b)** | zapewniono mechanizm zapobiegający nieuprawnionemu dostępowi; |
| | **AC-03(12)(c)** | zmiany w zakresie dostępu po wstępnej instalacji aplikacji podlegają zatwierdzeniu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-03(12)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| ZAPEWNIENIE I EGZEKWOWANIE DOSTĘPU DO APLIKACJI** | |
| | **AC-03(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-03(12)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **AC-03(12)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania uprawnień dostępu]. |

| | | |
|---|---|---|
| **AC-03(13)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| KONTROLA DOSTĘPU NA PODSTAWIE ATRYBUTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(13)_ODP** | ***określono atrybuty do przyjmowania uprawnień dostępu;*** |
| | **AC-03(13)[01]** | polityka kontroli dostępu opartej na atrybutach jest egzekwowana w odniesieniu do zdefiniowanych podmiotów; |
| | **AC-03(13)[02]** | polityka kontroli dostępu opartej na atrybutach jest egzekwowana w odniesieniu do zdefiniowanych obiektów; |
| | **AC-03(13)[03]** | dostęp jest kontrolowany na podstawie ***<atrybutów AC-03(13)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-03(13)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista podmiotów i obiektów (tj. użytkowników i zasobów) wymagających egzekwowania polityki kontroli dostępu opartej na atrybutach; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-03(13)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **AC-03(13)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania uprawnień dostępu]. |

| | | |
|---|---|---|
| **AC-03(14)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| DOSTĘP INDYWIDUALNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(14)_ODP[01]** | ***określono mechanizmy umożliwiające osobom fizycznym dostęp do elementów ich danych identyfikacyjnych;*** |
| | **AC-03(14)_ODP[02]** | ***określono elementy danych identyfikacyjnych, do których osoby fizyczne mają dostęp;*** |
| | **AC-03(14)** | zapewniono ***<mechanizmy AC-03(14)_ODP[01]>***, aby umożliwić osobom fizycznym dostęp do ***<elementów AC-03(14)_ODP[02]> ich*** danych identyfikacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-03(14)-Badanie** | [WYBÓR SPOŚRÓD: Mechanizmy dostępu (np. formularze wniosków i interfejsy aplikacji); polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dotycząca dostępu do informacji danych identyfikacyjnych osób fizycznych; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; ustalenia lub sprawozdania z oceny prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-03(14)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; radca prawny]. |
| | **AC-03(14)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania uprawnień dostępu; mechanizmy umożliwiające indywidualny dostęp do danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **AC-03(15)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| UZNANIOWA I OBOWIĄZKOWA KONTROLA DOSTĘPU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-03(15)_ODP[01]** | ***zdefiniowano obowiązkową politykę kontroli dostępu, egzekwowaną w odniesieniu do zbioru objętych nią podmiotów określonych w polityce;*** |
| | **AC-03(15)_ODP[02]** | ***zdefiniowano obowiązkową politykę kontroli dostępu, egzekwowaną w odniesieniu do zbioru objętych nią obiektów określonych w polityce;*** |
| | **AC-03(15)_ODP[03]** | ***zdefiniowano politykę uznaniowej kontroli dostępu, egzekwowaną w odniesieniu do zbioru objętych nią podmiotów określonych w polityce;*** |
| | **AC-03(15)_ODP[04]** | ***zdefiniowano politykę uznaniowej kontroli dostępu, egzekwowaną w odniesieniu do zbioru objętych nią obiektów określonych w polityce;*** |
| | **AC-03(15)(a)[01]** | ***<polityka obowiązkowej kontroli dostępu AC-03(15)_ODP[01]>*** jest egzekwowana w odniesieniu do objętych nią podmiotów określonych w polityce; |
| | **AC-03(15)(a)[02]** | ***<obowiązkowa polityka kontroli dostępu AC-03(15)_ODP[02]>*** jest egzekwowana w odniesieniu do zbioru objętych nią obiektów określonych w polityce; |
| | **AC-03(15)(b)[01]** | ***<polityka uznaniowej kontroli dostępu AC-03(15)_ODP[03] >*** jest egzekwowana w odniesieniu do objętych nią podmiotów określonych w polityce; |
| | **AC-03(15)(b)[02]** | ***<polityka uznaniowej kontroli dostępu AC-03(15)_ODP[04]>*** jest egzekwowana w odniesieniu do zbioru objętych nią obiektów określonych w polityce. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-03(15)** | **EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU \| UZNANIOWA I OBOWIĄZKOWA KONTROLA DOSTĘPU** | |
| | **AC-03(15)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista podmiotów i obiektów (tj. użytkowników i zasobów) wymagających egzekwowania polityki obowiązkowej kontroli dostępu; lista podmiotów i obiektów (tj. użytkowników i zasobów) wymagających egzekwowania polityki uznaniowej kontroli dostępu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-03(15)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-03(15)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę obowiązkowej i uznaniowej kontroli dostępu]. |

| | | |
|---|---|---|
| **AC-04** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04_ODP** | ***określono politykę kontroli przepływu informacji w obrębie systemu i pomiędzy połączonymi systemami;*** |
| | **AC-04** | egzekwowane są zatwierdzone uprawnienia w zakresie kontroli przepływu informacji w systemie i pomiędzy połączonymi systemami w oparciu o ***<polityka kontroli przepływu informacji AC-04_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **AC-04** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI** | |
|---|---|---|
| | **AC-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja architektury bezpieczeństwa; dokumentacja architektury prywatności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; bazowa konfiguracja systemu; lista uprawnień w zakresie przepływu informacji; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-04-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za rozwój architektury bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-04-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji]. |

| **AC-04(01)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| BEZPIECZEŃSTWO OBIEKTÓW I ATRYBUTY PRYWATNOŚCI** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(01)_ODP[01]** | ***określono atrybuty bezpieczeństwa, które mają być związane z obiektami informacyjnymi, źródłowymi i docelowymi;*** |
| | **AC-04(01)_ODP[02]** | ***określono atrybuty prywatności, które mają być związane z obiektami informacyjnymi, źródłowymi i docelowymi;*** |
| | **AC-04(01)_ODP[03]** | ***określono obiekty informacyjne, które mają być powiązane z atrybutami bezpieczeństwa informacji;*** |

| | | |
|---|---|---|
| **AC-04(01)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| BEZPIECZEŃSTWO OBIEKTÓW I ATRYBUTY PRYWATNOŚCI** | |
| | **AC-04(01)_ODP[04]** | ***określono obiekty informacyjne, które mają być powiązane z atrybutami prywatności informacji;*** |
| | **AC-04(01)_ODP[05]** | ***określono obiekty źródłowe, które mają być powiązane z atrybutami bezpieczeństwa informacji;*** |
| | **AC-04(01)_ODP[06]** | ***określono obiekty źródłowe, które mają być powiązane z atrybutami prywatności informacji;*** |
| | **AC-04(01)_ODP[07]** | ***określono obiekty docelowe, które mają być powiązane z atrybutami bezpieczeństwa informacji;*** |
| | **AC-04(01)_ODP[08]** | ***określono obiekty docelowe, które mają być powiązane z atrybutami prywatności informacji;*** |
| | **AC-04(01)_ODP[09]** | ***określono politykę kontroli przepływu informacji, stanowiącą podstawę do egzekwowania decyzji ws. zasad przepływu informacji;*** |
| | **AC-04(01)[01]** | ***<atrybuty bezpieczeństwa AC-04(01)_ODP[01]>*** związane z ***<obiektami informacyjnymi AC-04(01)_ODP[03] >***, ***<obiektami źródłowymi AC-04(01)_ODP[05]>*** oraz<br>***<obiektami docelowymi AC-04(01)_ODP[07]>*** są stosowane do egzekwowania<br>***<polityki kontroli przepływu informacji AC-04(01)_ODP[09]>*** jako podstawa do decyzji ws. kontroli przepływu; |
| | **AC-04(01)[02]** | ***<atrybuty prywatności AC-04(01)_ODP[02]>*** związane z ***<obiektami informacyjnymi AC-04(01)_ODP[04] >***, ***<obiektami źródłowymi AC-04(01)_ODP[06]>*** oraz<br>***<obiektami docelowymi AC-04(01)_ODP[08]>*** są stosowane do egzekwowania<br>***<polityki kontroli przepływu informacji AC-04(01)_ODP[09]>*** jako podstawa do decyzji ws. kontroli przepływu. |

| | | |
|---|---|---|
| **AC-04(01)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| BEZPIECZEŃSTWO OBIEKTÓW I ATRYBUTY PRYWATNOŚCI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista atrybutów bezpieczeństwa i prywatności oraz związanych z nimi obiektów źródłowych i docelowych; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za prywatność; programiści systemu]. |
| | **AC-04(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(02)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| PRZETWARZANIE DOMEN** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(02)_ODP** | ***określono mechanizmy kontroli przepływu informacji, których zaszyfrowane informacje nie mogą ominąć;*** |
| | **AC-04(02)** | chronione domeny przetwarzania są wykorzystywane do egzekwowania ***<polityki kontroli przepływu informacji AC-04(02)_ODP>*** jako podstawy do decyzji ws. kontroli przepływu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| AC-04(02) | EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| PRZETWARZANIE DOMEN | |
|---|---|---|
| | **AC-04(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji]. |

| AC-04(03) | EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| DYNAMICZNA KONTROLA PRZEPŁYWU INFORMACJI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(03)_ODP** | ***określono politykę kontroli przepływu informacji, która ma być egzekwowana;*** |
| | **AC-04(03)** | ***<polityka kontroli przepływu informacji AC-04(03)_ODP >*** jest egzekwowana. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-04(03)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| DYNAMICZNA KONTROLA PRZEPŁYWU INFORMACJI** | |
| | **AC-04(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-04(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(04)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| KONTROLA PRZEPŁYWU ZASZYFROWANYCH INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(04)_ODP[01]** | ***określono mechanizmy kontroli przepływu informacji, których zaszyfrowane informacje nie mogą ominąć;*** |
| | **AC-04(04)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {odszyfrowanie informacji; zablokowanie przepływu zaszyfrowanej informacji; zakończenie sesji komunikacyjnych próbujących przekazać zaszyfrowaną informację;***<br>***<procedura lub metoda określona przez organizację AC-04(04)_ODP[03]>};*** |

| | | |
|---|---|---|
| **AC-04(04)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| KONTROLA PRZEPŁYWU ZASZYFROWANYCH INFORMACJI** | |
| | **AC-04(04)_ODP[03]** | ***określono zdefiniowaną przez organizację procedurę lub metodę zapobiegającą omijaniu mechanizmów kontroli przepływu informacji przez zaszyfrowane informacje (jeśli wybrano);*** |
| | **AC-04(04)** | Zaszyfrowane informacje są zabezpieczone przed ominięciem ***<mechanizmów kontroli przepływu informacji AC-04(04)_ODP[01]>*** przez ***<WYBRANA WARTOŚĆ PARAMETRU AC-04(04)_ODP[02]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-04(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(05)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WBUDOWANE RODZAJE DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(05)_ODP** | ***określono ograniczenia dotyczące osadzania typów danych wewnątrz innych typów danych;*** |

| | | |
|---|---|---|
| **AC-04(05)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WBUDOWANE RODZAJE DANYCH** | |
| | **AC-04(05)** | przy osadzaniu typów danych w innych typach danych egzekwowane są ***<ograniczenia AC-04(05)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista ograniczeń, które mają być egzekwowane w odniesieniu do osadzania typów danych w innych typach danych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(05)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-04(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(06)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| METADANE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(06)_ODP** | ***określono metadane, na których można oprzeć egzekwowanie kontroli przepływu informacji;*** |
| | **AC-04(06)** | egzekwowanie kontroli przepływu informacji oparte jest na***<metadanych AC-04(06)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-04(06)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| METADANE** | |
| | **AC-04(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; rodzaje metadanych wykorzystywanych do egzekwowania decyzji dotyczących kontroli przepływu informacji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(06)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-04(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(07)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| MECHANIZMY PRZEPŁYWU JEDNOKIERUNKOWEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(07)** | sprzętowe mechanizmy kontroli przepływu wymuszają jednokierunkowy przepływ informacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-04(07)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| MECHANIZMY PRZEPŁYWU JEDNOKIERUNKOWEGO** | |
| | **AC-04(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania przepływu informacji; dokumentacja projektowa systemu;<br>ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; mechanizmy sprzętowe systemu i związane z nimi konfiguracje; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(07)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-04(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy sprzętowe wdrażające politykę egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(08)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| FILTRY POLITYKI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(08)_ODP[01]** | ***określono filtry polityki bezpieczeństwa, które mają być podstawą do egzekwowania kontroli przepływu informacji;*** |
| | **AC-04(08)_ODP[02]** | ***określono filtry polityki prywatności, które mają być podstawą do egzekwowania kontroli przepływu informacji;*** |
| | **AC-04(08)_ODP[03]** | ***określono przepływy informacji, w przypadku których egzekwowanie kontroli przepływu realizowane jest za pomocą filtrów bezpieczeństwa;*** |
| | **AC-04(08)_ODP[04]** | ***określono przepływy informacji, w przypadku których egzekwowanie kontroli przepływu realizowane jest za pomocą filtrów prywatności;*** |

| | | |
|---|---|---|
| **AC-04(08)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| FILTRY POLITYKI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **AC-04(08)_ODP[05]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {zablokuj; usuń; zmodyfikuj; przenieś do kwarantanny};*** |
| | **AC-04(08)_ODP[06]** | ***określono politykę bezpieczeństwa identyfikującą działania podejmowane po wystąpieniu awarii filtra przetwarzania;*** |
| | **AC-04(08)_ODP[07]** | ***określono politykę prywatności identyfikującą działania podejmowane po wystąpieniu awarii filtra przetwarzania;*** |
| | **AC-04(08)(a)[01]** | Kontrola przepływu jest realizowana przy użyciu ***<filtra polityki bezpieczeństwa AC-04(08)_ODP[01]>*** jako podstawy do decyzji ws. kontroli przepływu w zakresie ***<przepływów informacji AC-04(08)_ODP[03]>***; |
| | **AC-04(08)(a)[02]** | Kontrola przepływu jest realizowana przy użyciu ***<filtra polityki prywatności AC-04(08)_ODP[02]>*** jako podstawy do decyzji ws. kontroli przepływu w zakresie ***<przepływów informacji AC-04(08)_ODP[04]>***; |
| | **AC-04(08)(b)** | dane ***<AC-04(08)_ODP[05] WYBRANA WARTOŚĆ PARAMETRU>*** ***po*** wystąpieniu awarii przetwarzania w filtrze zgodnie z ***<polityką bezpieczeństwa AC-04(08)_ODP[06]>***;<br>dane ***<AC-04(08)_ODP[05] WYBRANA WARTOŚĆ PARAMETRU>*** ***po*** wystąpieniu awarii przetwarzania w filtrze zgodnie z ***<polityką prywatności> AC-04(08)_ODP[07]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-04(08)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| FILTRY POLITYKI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **AC-04(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista filtrów polityki bezpieczeństwa regulujących decyzje ws. kontroli przepływu; lista filtrów polityki prywatności regulujących decyzje ws. kontroli przepływu; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-04(08)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; programiści systemu]. |
| | **AC-04(08)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji; filtry polityki bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **AC-04(09)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| OCENA PRZEZ UPRAWNIONĄ OSOBĘ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(09)_ODP[01]** | ***określono przepływy informacji wymagające nadzoru człowieka;*** |
| | **AC-04(09)_ODP[02]** | ***określono warunki, na podstawie których ma być egzekwowany nadzór człowieka nad przepływami informacji;*** |
| | **AC-04(09)** | Nadzór człowieka stosuje się w przypadku ***<przepływów informacji AC-04(09)_ODP[01]> w*** razie wystąpienia ***<warunków AC-04(09)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-04(09)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| OCENA PRZEZ UPRAWNIONĄ OSOBĘ** | |
| | **AC-04(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące nadzoru człowieka nad przepływem informacji; lista przepływów informacji wymagających nadzoru człowieka; lista warunków wymagających nadzoru człowieka w odniesieniu do przepływów informacji; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-04(09)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; programiści systemu]. |
| | **AC-04(09)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wymuszające stosowanie nadzoru człowieka]. |

| | | |
|---|---|---|
| **AC-04(10)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WŁĄCZANIE I WYŁĄCZANIE FILTRÓW BEZPIECZEŃSTWA LUB POLITYKI PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(10)_ODP[01]** | ***określono filtry polityki bezpieczeństwa, które uprzywilejowani administratorzy mogą włączać i wyłączać;*** |
| | **AC-04(10)_ODP[02]** | ***określono filtry polityki prywatności, które uprzywilejowani administratorzy mogą włączać i wyłączać;*** |
| | **AC-04(10)_ODP[03]** | ***określono warunki, w których uprzywilejowani administratorzy mają możliwość włączania i wyłączania filtrów polityki bezpieczeństwa;*** |

| | | |
|---|---|---|
| **AC-04(10)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WŁĄCZANIE I WYŁĄCZANIE FILTRÓW BEZPIECZEŃSTWA LUB POLITYKI PRYWATNOŚCI** | |
| | **AC-04(10)_ODP[04]** | ***określono warunki, w których uprzywilejowani administratorzy mają możliwość włączania i wyłączania filtrów polityki prywatności;*** |
| | **AC-04(10)[01]** | Uprawnieni administratorzy mają możliwość włączania i wyłączania ***<filtrów bezpieczeństwa AC-04(10)_ODP[01]> w*** warunkach***<AC-04(10)_ODP[03]>***; |
| | **AC-04(10)[02]** | Uprawnieni administratorzy mają możliwość włączania i wyłączania ***<filtrów prywatności AC-04(10)_ODP[02]> w <warunkach AC-04(10)_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista filtrów polityki bezpieczeństwa włączonych/wyłączonych przez uprzywilejowanych administratorów;<br>lista filtrów polityki prywatności włączonych/wyłączonych przez uprzywilejowanych administratorów; lista zatwierdzonych typów danych, które mogą włączać/wyłączać uprzywilejowani administratorzy; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-04(10)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za włączanie/wyłączanie filtrów polityki bezpieczeństwa i prywatności; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |

| | | |
|---|---|---|
| **AC-04(10)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WŁĄCZANIE I WYŁĄCZANIE FILTRÓW BEZPIECZEŃSTWA LUB POLITYKI PRYWATNOŚCI** | |
| | **AC-04(10)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji; filtry polityki bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **AC-04(11)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| KONFIGURACJA FILTRÓW BEZPIECZEŃSTWA LUB POLITYKI PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(11)_ODP[01]** | ***określono filtry polityki bezpieczeństwa, które uprzywilejowani administratorzy mogą skonfigurować w celu obsługi różnych polityk bezpieczeństwa i prywatności;*** |
| | **AC-04(11)_ODP[02]** | ***określono filtry polityki prywatności, które uprzywilejowani administratorzy mogą skonfigurować w celu obsługi różnych polityk bezpieczeństwa i prywatności;*** |
| | **AC-04(11)[01]** | Uprawnieni administratorzy mają możliwość skonfigurowania ***<filtrów polityki bezpieczeństwa AC-04(11)_ODP[01]> do*** obsługi różnych polityk bezpieczeństwa lub prywatności; |
| | **AC-04(11)[02]** | Uprawnieni administratorzy mają możliwość skonfigurowania ***<filtrów polityki prywatności AC-04(11)_ODP[02]> do*** obsługi różnych polityk bezpieczeństwa lub prywatności; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-04(11)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| KONFIGURACJA FILTRÓW BEZPIECZEŃSTWA LUB POLITYKI PRYWATNOŚCI** | |
| | **AC-04(11)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista filtrów polityki bezpieczeństwa; lista filtrów polityki prywatności; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-04(11)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za konfigurowanie filtrów polityki bezpieczeństwa i prywatności; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-04(11)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji; filtry polityki bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **AC-04(12)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| IDENTYFIKATORY TYPÓW DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(12)_ODP** | ***określono identyfikatory typów danych, które mają być stosowane do walidacji danych niezbędnych do podejmowania decyzji w zakresie przepływu informacji;*** |
| | **AC-04(12)** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa<br>***<identyfikatory typów danych AC-04(12)_ODP>*** są stosowane do zatwierdzania danych istotnych dla decyzji ws. przepływu informacji. |

| | | |
|---|---|---|
| **AC-04(12)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| IDENTYFIKATORY TYPÓW DANYCH** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista identyfikatorów typów danych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(12)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-04(12)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(13)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| DEKOMPOZYCJA INFORMACJI NA ODPOWIEDNIE PODSKŁADNIKI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(13)_ODP** | ***określono elementy składowe dotyczące polityki, na które można rozłożyć informacje w celu przekazania do mechanizmów egzekwowania polityki;*** |
| | **AC-04(13)** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa, informacje rozkładane są na ***<elementy składowe dotyczące polityki AC-04(13)_ODP> w*** celu przekazania do mechanizmów egzekwowania polityki. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-04(13)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| DEKOMPOZYCJA INFORMACJI NA ODPOWIEDNIE PODSKŁADNIKI** | |
| | **AC-04(13)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(13)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-04(13)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(14)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| POLITYKA STOSOWANIA FILTRÓW BEZPIECZEŃSTWA LUB OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(14)_ODP[01]** | ***określono filtry polityki bezpieczeństwa, które wymagają w pełni wyliczanych formatów ograniczających strukturę i zawartość danych;*** |
| | **AC-04(14)_ODP[02]** | ***określono filtry polityki prywatności, które wymagają w pełni wyliczanych formatów ograniczających strukturę i zawartość danych;*** |
| | **AC-04(14)[01]** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa, wdrożone<br>***<filtry polityki bezpieczeństwa AC-04(14)_ODP[01]>*** wymagają w pełni wyliczanych formatów ograniczających strukturę i zawartość danych; |

| | | |
|---|---|---|
| **AC-04(14)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| POLITYKA STOSOWANIA FILTRÓW BEZPIECZEŃSTWA LUB OCHRONY PRYWATNOŚCI** | |
| | **AC-04(14)[02]** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa, wdrożone<br>***<filtry polityki prywatności AC-04(14)_ODP[02]>*** wymagają w pełni wyliczanych formatów ograniczających strukturę i zawartość danych; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(14)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista filtrów polityki bezpieczeństwa i prywatności; lista filtrów polityki struktury danych; lista filtrów polityki zawartości danych; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-04(14)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; programiści systemu]. |
| | **AC-04(14)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji; filtry polityki bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **AC-04(15)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WYKRYWANIE INFORMACJI NIEAKCEPTOWANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(15)_ODP[01]** | ***określono niezatwierdzone informacje, które muszą być wykrywane;*** |

| | | |
|---|---|---|
| **AC-04(15)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WYKRYWANIE INFORMACJI NIEAKCEPTOWANYCH** | |
| | **AC-04(15)_ODP[02]** | ***określono politykę bezpieczeństwa, która wymaga, aby transfer niezatwierdzonych informacji pomiędzy różnymi domenami bezpieczeństwa był zabroniony (jeśli wybrano);*** |
| | **AC-04(15)_ODP[03]** | ***określono politykę prywatności, która wymaga zakazu przekazywania informacji niezatwierdzonych przez organizację pomiędzy różnymi domenami bezpieczeństwa (jeśli wybrano);*** |
| | **AC-04(15)[01]** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa, informacje są sprawdzane pod kątem obecności ***<niezatwierdzonych informacji AC-04(15)_ODP[01]>***; |
| | **AC-04(15)[02]** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa, transfer ***<niezatwierdzonych informacji AC-04(15)_ODP[01]>*** jest zabroniony zgodnie z ***<polityką bezpieczeństwa AC-04(15)_ODP[02]>***; |
| | **AC-04(15)[03]** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa, transfer ***<niezatwierdzonych informacji AC-04(15)_ODP[01]>*** jest zabroniony zgodnie z ***<polityką prywatności AC-04(15)_ODP[02]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(15)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista typów niezatwierdzonych informacji i związane z nimi informacje; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-04(15)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za prywatność; programiści systemu]. |

| | | |
|---|---|---|
| **AC-04(15)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WYKRYWANIE INFORMACJI NIEAKCEPTOWANYCH** | |
| | **AC-04(15)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(16)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| PRZEKAZYWANIE INFORMACJI POMIĘDZY SYSTEMAMI** | |
| | [WYCOFANE: Włączone do AC-04]. | |

| | | |
|---|---|---|
| **AC-04(17)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| UWIERZYTELNIANIE DOMEN** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(17)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {organizacja, system, aplikacja, usługa, osoba fizyczna};*** |
| | **AC-04(17)** | w przypadku transferu informacji punkty źródłowe i docelowe są jednoznacznie identyfikowane i uwierzytelniane przez ***<WYBRANA WARTOŚĆ PARAMETRU AC-04(17)_ODP >***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(17)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu;<br>procedury dotyczące identyfikacji i uwierzytelniania domeny źródłowej i docelowej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; lista etykiet systemowych; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-04(17)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| UWIERZYTELNIANIE DOMEN** | |
| | **AC-04(17)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; programiści systemu]. |
| | **AC-04(17)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji]. |

| | |
|---|---|
| **AC-04(18)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| POWIAZANIE ATRYBUTÓW BEZPIECZEŃSTWA** |
| | [WYCOFANE: Włączone do AC-16]. |

| | | |
|---|---|---|
| **AC-04(19)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| UWIERZYTELNIANIE METADANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(19)_ODP[01]** | ***określono filtry polityki bezpieczeństwa, które mają być stosowane w odniesieniu do metadanych (jeśli wybrano);*** |
| | **AC-04(19)_ODP[02]** | ***określono filtry polityki prywatności, które mają być stosowane w odniesieniu do metadanych (jeśli wybrano);*** |
| | **AC-04(19)[01]** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa, ***<filtry polityki bezpieczeństwa AC-04(19)_ODP[01]>*** są stosowane w odniesieniu do metadanych; |
| | **AC-04(19)[02]** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa, ***<filtry polityki prywatności AC-04(19)_ODP[02]>*** są stosowane w odniesieniu do metadanych; |

| | | |
|---|---|---|
| **AC-04(19)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| UWIERZYTELNIANIE METADANYCH** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(19)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; polityka kontroli informacji; procedury dotyczące egzekwowania zasad dotyczących przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista kryteriów filtrowania polityki bezpieczeństwa stosowanych do metadanych i ładunków danych; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-04(19)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za prywatność; programiści systemu]. |
| | **AC-04(19)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad przepływu informacji; filtry bezpieczeństwa i polityki]. |

| | | |
|---|---|---|
| **AC-04(20)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| ZATWIERDZONE ROZWIĄZANIA BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(20)_ODP[01]** | ***określono rozwiązania w zatwierdzonych konfiguracjach do kontroli przepływu informacji przez domeny bezpieczeństwa;*** |
| | **AC-04(20)_ODP[02]** | ***określono informacje, które mają być kontrolowane podczas ich przepływu przez domeny bezpieczeństwa;*** |

| | | |
|---|---|---|
| **AC-04(20)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| ZATWIERDZONE ROZWIĄZANIA BEZPIECZEŃSTWA** | |
| | **AC-04(20)** | określono ***<rozwiązania w zatwierdzonych konfiguracjach AC-04(20)_ODP[01]> do*** kontroli przepływu ***<informacji AC-04(20)_ODP[02]>*** przez domeny bezpieczeństwa; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(20)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista rozwiązań w zatwierdzonych konfiguracjach; zatwierdzone konfiguracje bazowe; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(20)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(20)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(21)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| FIZYCZNA LUB LOGICZNA SEPARACJA PRZEPŁYWÓW INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(21)_ODP[01]** | ***określono mechanizmy lub techniki stosowane do logicznej separacji przepływów informacji (jeśli wybrano);*** |
| | **AC-04(21)_ODP[02]** | ***określono mechanizmy lub techniki stosowane do fizycznej separacji przepływów informacji (jeśli wybrano);*** |

| | | |
|---|---|---|
| **AC-04(21)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| FIZYCZNA LUB LOGICZNA SEPARACJA PRZEPŁYWÓW INFORMACJI** | |
| | **AC-04(21)_ODP[03]** | ***określono wymagane techniki separacji w podziale na typy informacji;*** |
| | **AC-04(21)[01]** | przepływy informacji są rozdzielone logicznie przy użyciu ***<mechanizmów lub technik AC-04(21)_ODP[01]>*** w celu osiągnięcia ***<wymaganej separacji AC-04(21)_ODP[03]>***; |
| | **AC-04(21)[02]** | przepływy informacji są rozdzielone fizycznie przy użyciu ***<mechanizmów lub technik AC-04(21)_ODP[02]>*** w celu osiągnięcia ***<wymaganej separacji AC-04(21)_ODP[03]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(21)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista wymaganych typów separacji przepływów informacji;<br>lista mechanizmów lub technik stosowanych do logicznego lub fizycznego oddzielenia przepływu informacji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(21)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-04(21)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(22)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| TYLKO DOSTĘP** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(22)** | zapewnia się dostęp z jednego urządzenia do platform komputerowych, aplikacji lub danych, które znajdują się w wielu różnych domenach bezpieczeństwa, przy jednoczesnym zapobieganiu przepływowi informacji pomiędzy domenami bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(22)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(22)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(22)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(23)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| MODYFIKACJA INFORMACJI, KTÓRYCH NIE MOŻNA UDOSTĘPNIAĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(23)_ODP** | ***określono czynności modyfikacyjne, którym mają zostać poddane informacje niepodlegające ujawnieniu;*** |

| | | |
|---|---|---|
| **AC-04(23)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| MODYFIKACJA INFORMACJI, KTÓRYCH NIE MOŻNA UDOSTĘPNIAĆ** | |
| | **AC-04(23)** | przy przenoszeniu informacji między domenami bezpieczeństwa informacja niepodlegająca ujawnieniu jest zmieniana przez zastosowanie ***<modyfikacji AC-04(23)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(23)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(23)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(23)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(24)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WEWNĘTRZNY ZNORMALIZOWANY FORMAT** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(24)[01]** | Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa dane przychodzące są przetwarzane na wewnętrzny, znormalizowany format; |

| | | |
|---|---|---|
| **AC-04(24)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WEWNĘTRZNY ZNORMALIZOWANY FORMAT** | |
| | **AC-04(24)[02]** | Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa dane są ponownie generowane tak, by były zgodne z określoną specyfikacją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(24)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(24)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(24)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(25)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| SANITYZACJA DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(25)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {dostarczenie złośliwych treści, zarządzanie złośliwym kodem, ulepszenie złośliwego kodu i dane zakodowane steganograficznie; wyciek wrażliwych informacji};*** |

| | | |
|---|---|---|
| **AC-04(25)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| SANITYZACJA DANYCH** | |
| | **AC-04(25)_ODP[02]** | ***określono politykę sanityzacji danych;*** |
| | **AC-04(25)** | podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa dane zostają poddane sanityzacji w celu zminimalizowania ***<WYBRANA WARTOŚĆ PARAMETRU AC-04(25)_ODP[01]>*** zgodnie z ***<polityką AC-04(25)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(25)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(25)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(25)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(26)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| AUDYT DZIAŁAŃ FILTRUJĄCYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(26)[01]** | przy przenoszeniu informacji między różnymi domenami bezpieczeństwa czynności w zakresie filtrowania treści są rejestrowane i kontrolowane; |
| | **AC-04(26)[02]** | przy przenoszeniu informacji między różnymi domenami bezpieczeństwa wyniki dotyczące filtrowanej informacji są rejestrowane i kontrolowane; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(26)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(26)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(26)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad przepływu informacji; mechanizmy wdrażające filtrowanie treści; mechanizmy rejestrowania i kontroli filtrowania treści]. |

| | | |
|---|---|---|
| **AC-04(27)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| REDUNDANTNE/NIEZALEŻNE MECHANIZMY FILTRACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(27)** | przy przekazywaniu informacji pomiędzy domenami bezpieczeństwa zaimplementowane rozwiązania w zakresie filtrowania treści zapewniają nadmiarowe i niezależne mechanizmy filtrowania dla każdego typu danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(27)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(27)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(27)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(28)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| KASKADOWY FILTR TREŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(28)** | podczas przesyłania informacji między domenami bezpieczeństwa stosowany jest liniowy proces filtrowania, egzekwowany za pomocą uznaniowych i obowiązkowych mechanizmów kontroli dostępu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(28)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(28)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(28)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad przepływu informacji; mechanizmy wdrażające liniowe filtrowanie treści]. |

| | | |
|---|---|---|
| **AC-04(29)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| SILNIKI ARANŻACJI FILTROWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(29)_ODP** | ***polityka filtrowania treści;*** |

| | | |
|---|---|---|
| **AC-04(29)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| SILNIKI ARANŻACJI FILTROWANIA** | |
| | **AC-04(29)(a)** | podczas przesyłania informacji między domenami bezpieczeństwa stosuje się silniki aranżacji filtrów treści, aby zapewnić, że mechanizmy filtrowania treści pomyślnie zakończą działanie bez wystąpienia błędów; |
| | **AC-04(29)(b)[01]** | podczas przesyłania informacji między domenami bezpieczeństwa stosuje się silniki aranżacji filtrów treści, aby zapewnić, że filtrowanie treści będzie odbywało się w odpowiedniej kolejności; |
| | **AC-04(29)(b)[02]** | podczas przesyłania informacji między domenami bezpieczeństwa, stosuje się silniki aranżacji filtrów treści, aby zapewnić, że filtrowanie treści odbywa się zgodnie z ***<polityką AC-04(29)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(29)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(29)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(29)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji; mechanizmy wdrażające silniki aranżacji filtrów treści]. |

| | | |
|---|---|---|
| **AC-04(30)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| MECHANIZMY FILTRUJĄCE WYKORZYSTUJĄCE PROCESY WIELEKROTNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(30)** | podczas przesyłania informacji między domenami bezpieczeństwa stosuje się mechanizmy filtrowania treści z użyciem wielu procesów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(30)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(30)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(30)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji; mechanizmy wdrażające filtrowanie treści]. |

| | | |
|---|---|---|
| **AC-04(31)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| ZAPOBIEGANIE PRZENOSZENIU NIEWŁAŚCIWYCH TREŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(31)** | przy przekazywaniu informacji pomiędzy różnymi domenami bezpieczeństwa zapobiega się przekazywaniu niefiltrowanych treści do domeny otrzymującej. |

| | | |
|---|---|---|
| **AC-04(31)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| ZAPOBIEGANIE PRZENOSZENIU NIEWŁAŚCIWYCH TREŚCI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(31)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(31)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(31)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad przepływu informacji]. |

| | | |
|---|---|---|
| **AC-04(32)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WYMOGI DOTYCZĄCE PROCESU PRZEKAZYWANIA INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-04(32)(a)** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa proces, który przekazuje informacje między potokami filtrów, nie filtruje treści wiadomości; |
| | **AC-04(32)(b)** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa proces, który przekazuje informacje między potokami filtrów, weryfikuje metadane filtrowania; |
| | **AC-04(32)(c)** | przy przekazywaniu informacji między różnymi domenami |

| | | |
|---|---|---|
| **AC-04(32)** | **EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI \| WYMOGI DOTYCZĄCE PROCESU PRZEKAZYWANIA INFORMACJI** | |
| | | bezpieczeństwa proces, który przekazuje informacje między potokami filtrów, zapewnia, że zawartość z metadanymi filtrowania pomyślnie przeszła filtrację; |
| | **AC-04(32)(d)** | przy przekazywaniu informacji między różnymi domenami bezpieczeństwa proces, który przekazuje informacje między potokami filtrów, przekazuje zawartość do potoku filtra docelowego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-04(32)-Badanie** | [WYBÓR SPOŚRÓD: Polityka egzekwowania zasad przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; architektura bezpieczeństwa systemu i związana z nią dokumentacja; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja, zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-04(32)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad przepływu informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-04(32)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę egzekwowania zasad przepływu informacji; mechanizmy wdrażające filtrowanie treści]. |

| | | |
|---|---|---|
| **AC-05** | **ROZDZIAŁ OBOWIĄZKÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-05_ODP** | ***określono obowiązki osób, w zakresie których należy zastosować rozdział obowiązków;*** |

| | | |
|---|---|---|
| **AC-05** | **ROZDZIAŁ OBOWIĄZKÓW** | |
| | **AC-05a.** | ***<obowiązki osób AC-05_ODP >*** są określone i udokumentowane; |
| | **AC-05b.** | określono uprawnienia dostępu do systemu wspierające rozdział obowiązków. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zakresu odpowiedzialności i rozdziału obowiązków; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista zakresów odpowiedzialności i rozdziału obowiązków; upoważnienia do dostępu do systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za definiowanie odpowiednich zakresów odpowiedzialności i rozdział obowiązków; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **AC-05-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę rozdziału obowiązków]. |

| | | |
|---|---|---|
| **AC-06** | **ZASADA WIEDZY KONIECZNEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-06** | stosuje się zasadę wiedzy koniecznej, zezwalając użytkownikom (lub procesom działającym w ich imieniu) tylko na taki dostęp, który jest niezbędny do wykonania przydzielonych zadań w ramach organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-06** | **ZASADA WIEDZY KONIECZNEJ** | |
| | **AC-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; lista przypisanych uprawnień dostępu (przywileje użytkowników); ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za realizację zasady wiedzy koniecznej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **AC-06-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje związane z zasadą wiedzy koniecznej]. |

| | | |
|---|---|---|
| **AC-06(01)** | **ZASADA WIEDZY KONIECZNEJ \| UPOWAŻNIONY DOSTĘP DO FUNKCJI BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-06(01)_ODP[01]** | ***określono osoby i role z autoryzowanym dostępem do zabezpieczeń i informacji istotnych z punktu widzenia bezpieczeństwa;*** |
| | **AC-06(01)_ODP[02]** | ***określono zabezpieczenia w zakresie autoryzowanego dostępu (w sprzęcie);*** |
| | **AC-06(01)_ODP[03]** | ***określono zabezpieczenia w zakresie autoryzowanego dostępu (w oprogramowaniu);*** |
| | **AC-06(01)_ODP[04]** | ***określono zabezpieczenia w zakresie autoryzowanego dostępu (w oprogramowaniu sprzętowym);*** |
| | **AC-06(01)_ODP[05]** | ***określono istotne z punktu widzenia bezpieczeństwa informacje dot. autoryzowanego dostępu;*** |

| | | |
|---|---|---|
| **AC-06(01)** | **ZASADA WIEDZY KONIECZNEJ \| UPOWAŻNIONY DOSTĘP DO FUNKCJI BEZPIECZEŃSTWA** | |
| | **AC-06(01)(a)[01]** | ***<AC-06(01)_ODP[01] osoby i rola>*** mają dostęp do ***<AC-06(01)_ODP[02] funkcje bezpieczeństwa (sprzętowe)***>; |
| | **AC-06(01)(a)[02]** | ***<AC-06(01)_ODP[01] osoby i rola>*** mają dostęp do ***<AC-06(01)_ODP[03] funkcje bezpieczeństwa (w oprogramowaniu)***>; |
| | **AC-06(01)(a)[03]** | ***<AC-06(01)_ODP[01] osoby i rola>*** mają dostęp do ***<AC-06(01)_ODP[04] funkcje bezpieczeństwa (w oprogramowaniu sprzętowym)***>; |
| | **AC-06(01)(b)** | ***<AC-06(01)_ODP[01] osoby i rola>*** mają dostęp do ***<AC-06(01)_ODP[05] informacje dotyczące bezpieczeństwa***>. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-06(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; lista funkcji bezpieczeństwa (w sprzęcie, oprogramowaniu i oprogramowaniu sprzętowym) oraz informacji istotnych dla bezpieczeństwa, do których dostęp musi wymagać wyraźnego upoważnienia;<br>ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-06(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za realizację zasady wiedzy koniecznej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **AC-06(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje związane z zasadą wiedzy koniecznej]. |

| | | |
|---|---|---|
| **AC-06(02)** | **ZASADA WIEDZY KONIECZNEJ \| NIEUPRZYWILEJOWANY DOSTĘP DO FUNKCJI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-06(02)_ODP** | ***określono funkcje bezpieczeństwa lub informacje dotyczące bezpieczeństwa, do których dostęp wymaga od użytkowników korzystania z kont nieuprzywilejowanych w celu uzyskania dostępu do funkcji niezwiązanych z bezpieczeństwem;*** |
| | **AC-06(02)** | Podczas korzystania z funkcji niezwiązanych z bezpieczeństwem użytkownicy kont systemowych (lub role) z dostępem do ***<funkcji bezpieczeństwa lub informacji dotyczących bezpieczeństwa AC-06(02)_ODP>*** są zobowiązani do korzystania z kont lub ról nieuprzywilejowanych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-06(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; lista wygenerowanych przez system funkcji bezpieczeństwa lub informacji istotnych dla bezpieczeństwa przypisanych do kont lub ról systemowych;<br>ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-06(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za realizację zasady wiedzy koniecznej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **AC-06(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje związane z zasadą wiedzy koniecznej]. |

| | | |
|---|---|---|
| **AC-06(03)** | **ZASADA WIEDZY KONIECZNEJ \| DOSTĘP SIECIOWY DO UPRZYWILEJOWANYCH POLECEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-06(03)_ODP[01]** | ***określono uprzywilejowane polecenia, do których dostęp poprzez sieć jest dozwolony tylko w przypadku uzasadnionej potrzeby operacyjnej;*** |
| | **AC-06(03)_ODP[02]** | ***określono uzasadnione potrzeby operacyjne, w przypadku których dostęp do uprzywilejowanych poleceń poprzez sieć jest dozwolony;*** |
| | **AC-06(03)[01]** | dostęp sieciowy do ***<poleceń uprzywilejowanych AC-06(03)_ODP[01]>*** jest dozwolony tylko w przypadku***<uzasadnionych potrzeb operacyjnych AC-06(03)_ODP[02]>***; |
| | **AC-06(03)[02]** | uzasadnienie zezwolenia na dostęp sieciowy do uprzywilejowanych poleceń jest udokumentowane w planie bezpieczeństwa systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-06(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; lista potrzeb operacyjnych uzasadniających dostęp sieciowy do uprzywilejowanych poleceń; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-06(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za realizację zasady wiedzy koniecznej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **AC-06(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje związane z zasadą wiedzy koniecznej]. |

| AC-06(04) | ZASADA WIEDZY KONIECZNEJ \| ODDZIELNE DOMENY PRZETWARZANIA | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-06(04)** | zapewnione są oddzielne domeny przetwarzania, aby umożliwić bardziej szczegółowy przydział uprawnień dla użytkowników. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-06(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-06(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za realizację zasady wiedzy koniecznej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-06(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje związane z zasadą wiedzy koniecznej]. |

| AC-06(05) | ZASADA WIEDZY KONIECZNEJ \| UPRZYWILEJOWANE KONTA | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-06(05)_ODP** | ***określono personel lub role upoważnione do korzystania z kont uprzywilejowanych w systemie;*** |
| | **AC-06(05)** | z kont uprzywilejowanych w systemie mogą korzystać***<personel lub role AC-06(05)_ODP >***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-06(05)** | **ZASADA WIEDZY KONIECZNEJ \| UPRZYWILEJOWANE KONTA** | |
| | **AC-06(05)-Badanie** | [WYBÓR SPOŚRÓD: polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; lista wygenerowanych przez system kont uprzywilejowanych; lista pracowników odpowiedzialnych za administrowanie systemem;<br>ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-06(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za realizację zasady wiedzy koniecznej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **AC-06(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje związane z zasadą wiedzy koniecznej]. |

| | | |
|---|---|---|
| **AC-06(06)** | **ZASADA WIEDZY KONIECZNEJ \| UPRZYWILEJOWANY DOSTĘP PRZEZ UŻYTKOWNIKÓW NIEORGANIZACYJNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-06(06)** | uprzywilejowany dostęp do systemu zabroniony jest dla użytkowników spoza organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-06(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; lista wygenerowanych przez system kont uprzywilejowanych; lista użytkowników spoza organizacji; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-06(06)** | **ZASADA WIEDZY KONIECZNEJ \| UPRZYWILEJOWANY DOSTĘP PRZEZ UŻYTKOWNIKÓW NIEORGANIZACYJNYCH** | |
| | **AC-06(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za realizację zasady wiedzy koniecznej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **AC-06(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zakazujące uprzywilejowanego dostępu do systemu]. |

| | | |
|---|---|---|
| **AC-06(07)** | **ZASADA WIEDZY KONIECZNEJ \| PRZEGLĄD UPRAWNIEŃ UŻYTKOWNIKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-06(07)_ODP[01]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu uprawnień przypisanych do ról lub klas użytkowników;*** |
| | **AC-06(07)_ODP[02]** | ***określono role lub klasy użytkowników, do których przypisane są uprawnienia;*** |
| | **AC-06(07)(a)** | uprawnienia przypisane do ***<ról i klas AC-06(07)_ODP[02]>*** są sprawdzane<br>z ***<częstotliwością AC-06(07)_ODP[01]>***, aby potwierdzić konieczność ich posiadania; |
| | **AC-06(07)(b)** | w razie potrzeby uprawnienia są ponownie przydzielane lub odbierane w celu prawidłowej realizacji misji organizacji oraz potrzeb biznesowych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| AC-06(07) | ZASADA WIEDZY KONIECZNEJ \| PRZEGLĄD UPRAWNIEŃ UŻYTKOWNIKA | |
|---|---|---|
| | **AC-06(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; lista wygenerowanych przez system ról lub klas użytkowników oraz przypisanych im uprawnień; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; przeglądy weryfikujące uprawnienia przypisane rolom, klasom lub użytkownikom; zapisy dotyczące usuwania lub ponownego przypisywania uprawnień dla ról lub klas użytkowników; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-06(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę wdrożenia zasady wiedzy koniecznej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **AC-06(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające przegląd uprawnień użytkowników]. |

| AC-06(08) | ZASADA WIEDZY KONIECZNEJ \| POZIOMY UPRAWNIEŃ DO WYKONANIA KODU | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-06(08)_ODP** | ***określono oprogramowanie, któremu należy uniemożliwić przeprowadzanie wykonywania na wyższych poziomach uprawnień niż użytkownicy wykonujący takie oprogramowanie;*** |
| | **AC-06(08)** | ***<oprogramowanie AC-06(08)_ODP> nie może przeprowadzać wykonywania na wyższych poziomach uprawnień niż użytkownicy wykonujący to oprogramowanie;*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| AC-06(08) | ZASADA WIEDZY KONIECZNEJ \| POZIOMY UPRAWNIEŃ DO WYKONANIA KODU | |
|---|---|---|
| | **AC-06(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; lista oprogramowania, które nie może przeprowadzać wykonywania na wyższych poziomach uprzywilejowania niż użytkownicy wykonujący oprogramowanie; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-06(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za realizację zasady wiedzy koniecznej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AC-06(08)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje związane z zasadą wiedzy koniecznej w zakresie wykonywania oprogramowania]. |

| AC-06(09) | ZASADA WIEDZY KONIECZNEJ \| KONTROLA WYKORZYSTANIA UPRZYWILEJOWANYCH FUNKCJI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-06(09)** | wykonanie funkcji uprzywilejowanych jest rejestrowane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-06(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista uprzywilejowanych funkcji podlegających kontroli; lista kontrolowanych zdarzeń; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-06(09)** | **ZASADA WIEDZY KONIECZNEJ \| KONTROLA WYKORZYSTANIA UPRZYWILEJOWANYCH FUNKCJI** | |
| | **AC-06(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę wdrożenia zasady wiedzy koniecznej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AC-06(09)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kontrolujące realizację funkcji związanych z zasadą wiedzy koniecznej]. |

| | | |
|---|---|---|
| **AC-06(10)** | **ZASADA WIEDZY KONIECZNEJ \| ODMOWA WYKONYWANIA PRZEZ NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW UPRZYWILEJOWANYCH FUNKCJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-06(10)** | nieuprzywilejowani użytkownicy nie mogą wykonywać uprzywilejowanych funkcji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-06(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista uprzywilejowanych funkcji i przypisanych do nich kont użytkowników; dokumentacja audytu systemu; plan bezpieczeństwa systemu; odpowiednie dokumenty]. przydziały kont użytkowników;<br>zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-06(10)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za realizację zasady wiedzy koniecznej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |

| | | |
|---|---|---|
| **AC-06(10)** | **ZASADA WIEDZY KONIECZNEJ \| ODMOWA WYKONYWANIA PRZEZ NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW UPRZYWILEJOWANYCH FUNKCJI** | |
| | **AC-06(10)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje związane z zasadą wiedzy koniecznej w odniesieniu do użytkowników nieuprzywilejowanych]. |

| | | |
|---|---|---|
| **AC-07** | **NIEUDANE PRÓBY LOGOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-07_ODP[01]** | ***określono liczbę kolejnych nieudanych prób logowania dopuszczalnych dla użytkownika w okresie;*** |
| | **AC-07_ODP[02]** | ***określono okres dla kolejnych nieudanych prób logowania dopuszczalnych dla użytkownika;*** |
| | **AC-07_ODP[03]** | ***wybrano jedną lub więcej z następujących WARTOŚCI PARAMETRÓW: {zablokowanie konta lub węzła na <okres AC-07_ODP[04]>; zablokowanie konta lub węzła do czasu odblokowania przez administratora; opóźnienie następnego monitu logowania według <algorytmu opóźnienia AC-07_ODP[05]>; powiadomienie administratora systemu; podjęcie innych <działań AC-07_ODP[06]>};*** |
| | **AC-07_ODP[04]** | ***określono okres blokady konta lub węzła (jeśli wybrano);*** |
| | **AC-07_ODP[05]** | ***określono algorytm kontrolujące opóźnienie dot. następnego monitu logowania (jeśli wybrano);*** |
| | **AC-07_ODP[06]** | ***określono inne działania, które mają być podjęte po przekroczeniu maksymalnej liczby nieudanych prób logowania (jeśli wybrano);*** |
| | **AC-07a.** | egzekwowany jest limit określony przez ***<liczbę AC-07_ODP[01]>*** kolejnych nieudanych prób logowania przez użytkownika w ciągu ***<okresu AC-07_ODP[02]>;*** |

| | | |
|---|---|---|
| **AC-07** | **NIEUDANE PRÓBY LOGOWANIA** | |
| | **AC-07b.** | ***<WYBRANA WARTOŚĆ PARAMETRU AC-07_ODP[03]>*** ma zastosowanie automatycznie po przekroczeniu maksymalnej liczby nieudanych prób. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące nieudanych prób logowania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu; administratorzy systemu/sieci]. |
| | **AC-07-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu w przypadku nieudanej próby logowania]. |

| | |
|---|---|
| **AC-07(01)** | **NIEUDANE PRÓBY LOGOWANIA \| AUTOMATYCZNE ZAMKNIĘCIE KONTA** |
| | [WYCOFANE: Włączone do AC-07]. |

| | | |
|---|---|---|
| **AC-07(02)** | **NIEUDANE PRÓBY LOGOWANIA \| USUWANIE INFORMACJI Z URZĄDZEŃ PRZENOŚNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-07(02)_ODP[01]** | ***określono urządzenia przenośne, w przypadku których stosuje się kasowanie lub wymazywanie danych;*** |

| | | |
|---|---|---|
| **AC-07(02)** | **NIEUDANE PRÓBY LOGOWANIA \| USUWANIE INFORMACJI Z URZĄDZEŃ PRZENOŚNYCH** | |
| | **AC-07(02)_ODP[02]** | ***Określono wymagania dotyczące kasowania lub wymazywania danych z urządzeń przenośnych oraz techniki, które należy stosować w ramach tego procesu;*** |
| | **AC-07(02)_ODP[03]** | ***określono liczbę kolejnych, nieudanych prób logowania możliwych przed skasowaniem lub wymazaniem danych z urządzenia przenośnego;*** |
| | **AC-07(02)** | informacje są kasowane lub wymazywane z ***<urządzeń przenośnych AC-07(02)_ODP[01]>*** w oparciu o ***<wymogi lub techniki kasowania lub wymazywania danych AC-07(02)_ODP[02]>*** po ***<liczbie AC-07(02)_ODP[03]>*** nieudanych prób logowania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-07(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące nieudanych prób logowania na urządzeniach przenośnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista urządzeń przenośnych, z których mają być skasowane/wymazane dane po określonej przez organizację liczbie kolejnych, nieudanych próba logowania do urządzenia; lista wymagań lub technik dot. kasowania/wymazywania danych z urządzeń przenośnych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-07(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-07(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu w zakresie nieudanych prób logowania do urządzenia]. |

| | | |
|---|---|---|
| **AC-07(03)** | **NIEUDANE PRÓBY LOGOWANIA \| OGRANICZANIE PRÓB LOGOWANIA BIOMETRYCZNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-07(03)_ODP** | ***określono liczbę nieudanych prób logowania biometrią;*** |
| | **AC-07(03)** | nieudane próby logowania biometrią są ograniczone do ***<liczby AC-07(03)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-07(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące nieudanych prób logowania na urządzeniach biometrycznych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-07(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-07(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu w przypadku nieudanej próby logowania]. |

| | | |
|---|---|---|
| **AC-07(04)** | **NIEUDANE PRÓBY LOGOWANIA \| UŻYCIE ALTERNATYWNEGO CZYNNIKA UWIERZYTELNIANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-07(04)_ODP[01]** | ***Określono dopuszczalne składniki uwierzytelniania inne od podstawowych składników uwierzytelniania;*** |

| | | |
|---|---|---|
| **AC-07(04)** | **NIEUDANE PRÓBY LOGOWANIA \| UŻYCIE ALTERNATYWNEGO CZYNNIKA UWIERZYTELNIANIA** | |
| | **AC-07(04)_ODP[02]** | ***określono liczbę kolejnych nieudanych prób logowania z użyciem alternatywnych składników, po których na użytkownika nakłada się ograniczenie;*** |
| | **AC-07(04)_ODP[03]** | ***określono okres, w którym użytkownik może podejmować próby logowania za pomocą składników alternatywnych;*** |
| | **AC-07(04)(a)** | po przekroczeniu liczby zdefiniowanych przez organizację kolejnych nieprawidłowych prób logowania dopuszczalne jest wykorzystanie ***<składników uwierzytelnienia AC-07(04)_ODP[01]>*** innych niż składniki podstawowe; |
| | **AC-07(04)(b)** | limit ***<AC-07(04)_ODP[02] liczby>*** kolejnych nieudanych prób logowania przez użycie składników alternatywnych przez użytkownika w ***<okresie AC-07(04)_ODP[03]>*** jest egzekwowany. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-07(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące nieudanych prób logowania z użyciem podstawowych i alternatywnych składników uwierzytelniania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-07(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-07(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu w przypadku nieudanej próby logowania]. |

| | | |
|---|---|---|
| **AC-08** | **POWIADOMIENIE O ZASADACH UŻYCIA SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-08_ODP[01]** | ***określono komunikat lub baner powiadamiający o zasadach użycia systemu, który ma być wyświetlany przez system użytkownikom przed przyznaniem dostępu do systemu;*** |
| | **AC-08_ODP[02]** | ***określa się zasady użycia systemu, które mają być wyświetlane przez system przed przyznaniem dostępu;*** |
| | **AC-08a.** | przed przyznaniem dostępu do systemu użytkownikom wyświetlane jest ***<powiadomienie o zasadach użycia systemu AC-08_ODP[01]>***, które zawiera informacje dotyczące prywatności i bezpieczeństwa zgodne z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, standardami i wytycznymi; |
| | **AC-08a.01** | powiadomienie o zasadach użycia systemu określa, że użytkownicy uzyskują dostęp do systemu należącego do rządu Stanów Zjednoczonych; |
| | **AC-08a.02** | powiadomienie o zasadach użycia systemu określa, że użytkowanie systemu może być monitorowane, rejestrowane i podlegać audytowi; |
| | **AC-08a.03** | powiadomienie o zasadach użycia systemu określa, że nieuprawnione korzystanie z systemu jest zabronione i podlega odpowiedzialności karnej i cywilnej; oraz |
| | **AC-08a.04** | powiadomienie o zasadach użycia systemu określa, że korzystanie z systemu oznacza zgodę na monitorowanie i nagrywanie; |
| | **AC-08b.** | komunikat lub baner z powiadomieniem pozostaje na ekranie do momentu, aż użytkownik wyrazi zgodę na zasady korzystania z systemu i podejmie wyraźne próby logowania lub dalszego dostępu do systemu; |

| | | |
|---|---|---|
| **AC-08** | **POWIADOMIENIE O ZASADACH UŻYCIA SYSTEMU** | |
| | **AC-08c.01** | w przypadku systemów dostępnych publicznie przed umożliwieniem dostępu wyświetlane są ***<warunki AC-08_ODP[02]>*** użycia systemu**;** |
| | **AC-08c.02** | w przypadku systemów publicznie dostępnych wyświetlane są wszelkie odniesienia do monitorowania, rejestrowania lub audytu zgodnego z przepisami dotyczącymi prywatności w tego rodzaju systemach, które zwykle zabraniają takich działań; |
| | **AC-08c.03** | w przypadku systemów publicznie dostępnych dołącza się opis dozwolonych sposobów użycia systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka prywatności i bezpieczeństwa, procedury dotyczące powiadomień o zasadach użycia systemu; udokumentowane zatwierdzenie komunikatów lub banerów dotyczących zasad użycia systemu; zapisy z audytu systemu; potwierdzenia użytkowników dotyczące komunikatów lub banerów dot. zasadach użycia systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wiadomości dotyczące powiadomień o zasadach użycia systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; raport z oceny prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-08-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; radca prawny; programiści systemu]. |
| | **AC-08-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające powiadomienia o zasadach użycia systemu]. |

| **AC-09** | **POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-09** | po pomyślnym zalogowaniu się do systemu użytkownik jest powiadamiany o dacie i godzinie ostatniego logowania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące powiadomienia o poprzednim logowaniu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; powiadomienia o zasadach użycia systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-09-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-09-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu w zakresie powiadomienia o poprzednim zalogowaniu]. |

| **AC-09(01)** | **POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU \| NIEUDANE LOGOWANIE** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-09(01)** | przy udanym logowaniu użytkownik jest powiadamiany o liczbie nieudanych prób logowania od ostatniego udanego logowania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-09(01)** | **POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU \| NIEUDANE LOGOWANIE** | |
| | **AC-09(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące powiadomienia o poprzednim logowaniu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-09(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-09(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu w zakresie powiadomienia o poprzednim zalogowaniu]. |

| | | |
|---|---|---|
| **AC-09(02)** | **POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU \| UDANE I NIEUDANE LOGOWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-09(02)_ODP[01]** | ***wybrano jedną z następujących WARTOŚCI PARAMETRÓW: {pomyślne logowania; nieudane próby logowania; oba};*** |
| | **AC-09(02)_ODP[02]** | ***określany jest okres, za który użytkownik otrzymuje powiadomienie o liczbie udanych logowań, nieudanych prób logowania lub obu;*** |
| | **AC-09(02)** | po pomyślnym zalogowaniu użytkownik jest powiadamiany o liczbie ***<WYBRANA WARTOŚĆ PARAMETRU AC-09(02)_ODP[01]> w <okresie AC-09(02)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-09(02)** | **POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU \| UDANE I NIEUDANE LOGOWANIE** | |
| | **AC-09(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące powiadomienia o poprzednim logowaniu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-09(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-09(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu w zakresie powiadomienia o poprzednim zalogowaniu]. |

| | | |
|---|---|---|
| **AC-09(03)** | **POWIADOMIENIE O POPRZEDNIM LOGOWANIU \| POWIADOMIENIE O ZMIANACH W KONCIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-09(03)_ODP[01]** | ***określono zmiany cech lub parametrów konta użytkownika związanych z bezpieczeństwem, które wymagają powiadomienia;*** |
| | **AC-09(03)_ODP[02]** | ***określono okres, w którym system powiadamia użytkownika o zmianach w zakresie cech lub parametrów związanych z bezpieczeństwem konta użytkownika;*** |
| | **AC-09(03)** | po udanym zalogowaniu użytkownik jest powiadamiany o zmianach w ***<cechach lub parametrach związanych z bezpieczeństwem AC-09(03)_ODP[01]>***, jakie miały miejsce ***w <okresie AC-09(03)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-09(03)** | **POWIADOMIENIE O POPRZEDNIM LOGOWANIU \| POWIADOMIENIE O ZMIANACH W KONCIE** | |
| | **AC-09(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące powiadomienia o poprzednim logowaniu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-09(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-09(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu w zakresie powiadomienia o poprzednim zalogowaniu]. |

| | | |
|---|---|---|
| **AC-09(04)** | **POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU \| DODATKOWE INFORMACJE DOTYCZĄCE LOGOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-09(04)_ODP** | ***określono dodatkowe informacje, o których należy powiadomić użytkownika;*** |
| | **AC-09(04)** | po pomyślnym zalogowaniu użytkownik jest powiadamiany o ***<dodatkowych informacjach AC-09(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-09(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące powiadomienia o poprzednim logowaniu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-09(04)** | **POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU \| DODATKOWE INFORMACJE DOTYCZĄCE LOGOWANIA** | |
| | **AC-09(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-09(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu w zakresie powiadomienia o poprzednim zalogowaniu]. |

| | | |
|---|---|---|
| **AC-10** | **KONTROLA ILOŚCI JEDNOCZESNYCH SESJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-10_ODP[01]** | ***określono konta lub typy kont, w przypadku których należy ograniczyć liczbę równoczesnych sesji;*** |
| | **AC-10_ODP[02]** | ***dla każdego konta lub typu konta określono dopuszczalną liczbę równoczesnych sesji;*** |
| | **AC-10** | liczba jednoczesnych sesji dla każdego ***<konta lub typów kont AC-10_ODP[01]>*** jest ograniczona do ***<liczby AC-10_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące kontroli sesji równoczesnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-10-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |

| | | |
|---|---|---|
| **AC-10** | **KONTROLA ILOŚCI JEDNOCZESNYCH SESJI** | |
| | **AC-10-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu dla sesji równoczesnych]. |

| | | |
|---|---|---|
| **AC-11** | **BLOKADA URZĄDZENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-11_ODP[01]** | ***wybrano jedną lub więcej z następujących WARTOŚCI PARAMETRÓW: {blokada urządzenia po <okresie AC-11_ODP[02]> bezczynności; wymaganie od użytkownika zablokowania urządzenia przed pozostawieniem systemu bez nadzoru};*** |
| | **AC-11_ODP[02]** | ***określono okres bezczynności, po którym następuje blokada urządzenia (jeśli wybrano);*** |
| | **AC-11a.** | dalszy dostęp do systemu zostaje uniemożliwiony przez ***<WYBRANA WARTOŚĆ PARAMETRU AC-11_ODP[01]>***; |
| | **AC-11b.** | urządzenie pozostaje zablokowane do czasu ponownego uzyskania dostępu przez użytkownika przy użyciu ustalonych procedur identyfikacji i uwierzytelniania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-11-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące blokady sesji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-11-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |

| | | |
|---|---|---|
| **AC-11** | **BLOKADA URZĄDZENIA** | |
| | **AC-11-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające politykę kontroli dostępu w zakresie blokady sesji]. |

| | | |
|---|---|---|
| **AC-11(01)** | **BLOKADA URZĄDZENIA \| WYGASZACZ EKRANU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-11(01)** | blokada urządzenia skutkuje ukryciem uprzednio widocznych na ekranie informacji i zastąpienie ich obrazem przeznaczonym do publicznego wyświetlania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-11(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące blokady sesji; ekran z włączoną blokadą sesji; dokumentacja projektowa systemu;<br>ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-11(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-11(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy blokady sesji systemowej]. |

| **AC-12** | **ZAKOŃCZENIE SESJI** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-12_ODP** | ***określono warunki lub zdarzenia wyzwalające wymagające zakończenia sesji;*** |
| | **AC-12** | w przypadku wystąpienia***<warunków lub zdarzeń wyzwalających AC-12_ODP >*** sesja użytkownika ulega automatycznemu zakończeniu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-12-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zakończenia sesji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista warunków lub zdarzeń wyzwalających wymagających zakończenia sesji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-12-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-12-Test** | [WYBÓR SPOŚRÓD: Mechanizmy automatyczne służące do zakończenia sesji użytkownika]. |

| **AC-12(01)** | **ZAKOŃCZENIE SESJI \| WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-12(01)_ODP** | ***określono zasoby informacyjne, w przypadku których wymagana jest możliwość wylogowania z sesji komunikacyjnej zainicjowanej przez użytkownika;*** |

| AC-12(01) | ZAKOŃCZENIE SESJI \| WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA | |
|---|---|---|
| | **AC-12(01)** | zapewniona jest możliwość wylogowania się z sesji komunikacyjnych inicjowanych przez użytkownika w każdym przypadku, gdy w celu uzyskania dostępu do ***<zasobów informacyjnych AC-12(01)_ODP>*** stosuje się uwierzytelnianie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-12(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zakończenia sesji; komunikaty o wylogowaniu użytkownika; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-12(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-12(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zakończenia sesji systemowej; możliwość wylogowania z sesji komunikacyjnych inicjowanych przez użytkownika]. |

| AC-12(02) | ZAKOŃCZENIE SESJI \| KOMUNIKAT O ZAKOŃCZENIU SESJI (WYLOGOWANIU) | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-12(02)** | użytkownikom wyświetlany jest wyraźny komunikat o wylogowaniu, informujący o zakończeniu uwierzytelnionych sesji komunikacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-12(02)** | **ZAKOŃCZENIE SESJI \| KOMUNIKAT O ZAKOŃCZENIU SESJI (WYLOGOWANIU)** | |
| | **AC-12(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zakończenia sesji; komunikaty o wylogowaniu użytkownika; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-12(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-12(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zakończenia sesji systemowej; wyświetlanie komunikatów o wylogowaniu]. |

| | | |
|---|---|---|
| **AC-12(03)** | **ZAKOŃCZENIE SESJI \| KOMUNIKAT OSTRZEGAWCZY O PRZEKROCZENIU LIMITU CZASU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-12(03)_ODP** | ***określono czas do końca sesji, który jest wyświetlany użytkownikom;*** |
| | **AC-12(03)** | użytkownikom wyświetlany jest wyraźny komunikat wskazujący, że sesja zakończy się w ciągu<br>***<czasu AC-12(03)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-12(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zakończenia sesji;<br>komunikaty o czasie do zakończenia sesji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-12(03)** | **ZAKOŃCZENIE SESJI \| KOMUNIKAT OSTRZEGAWCZY O PRZEKROCZENIU LIMITU CZASU** | |
| | **AC-12(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-12(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zakończenia sesji systemowej; wyświetlanie komunikatów o czasie do zakończenia sesji]. |

| | | |
|---|---|---|
| **AC-13** | **NADZÓR I PRZEGLĄD KONTROLI DOSTĘPU** | |
| | [WYCOFANE: Włączone do AC-02, AU-06]. | |

| | | |
|---|---|---|
| **AC-14** | **DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-14_ODP** | ***określono działania, które użytkownik może wykonywać w systemie bez identyfikacji lub uwierzytelnienia;*** |
| | **AC-14a.** | określono ***<działania użytkownika AC-14_ODP>***, które można wykonywać w systemie bez identyfikacji lub uwierzytelnienia wymaganego zgodnie z misją organizacji i funkcjami biznesowymi; |
| | **AC-14b.[01]** | działania użytkownika niewymagające identyfikacji lub uwierzytelnienia są dokumentowane w planie bezpieczeństwa systemu; |
| | **AC-14b.[02]** | w planie bezpieczeństwa systemu przedstawiono uzasadnienie dla działań użytkownika niewymagających identyfikacji lub uwierzytelnienia. |

| | | |
|---|---|---|
| **AC-14** | **DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-14-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące działań możliwych bez identyfikacji lub uwierzytelnienia; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa; lista działań użytkownika, które mogą być wykonywane bez identyfikacji lub uwierzytelnienia; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-14-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | |
|---|---|
| **AC-14(01)** | **DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA \| NIEZBĘDNE ZASTOSOWANIA** |
| | [WYCOFANE: Włączone do AC-14]. |

| | |
|---|---|
| **AC-15** | **ZNAKOWANIE AUTOMATYCZNE** |
| | [WYCOFANE: Włączone do MP-03]. |

| | | |
|---|---|---|
| **AC-16** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-16_ODP[01]** | ***określono rodzaje atrybutów bezpieczeństwa, które mają być powiązane z wartościami atrybutów bezpieczeństwa informacji przechowywanych, przetwarzanych lub przesyłanych;*** |

| AC-16 | ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | |
|---|---|---|
| | **AC-16_ODP[02]** | ***określono rodzaje atrybutów prywatności, które mają być powiązane z wartościami atrybutów prywatności informacji przechowywanych, przetwarzanych lub przesyłanych;*** |
| | **AC-16_ODP[03]** | ***określono wartości atrybutów bezpieczeństwa dla typów atrybutów bezpieczeństwa;*** |
| | **AC-16_ODP[04]** | ***określono wartości atrybutów prywatności dla typów atrybutów prywatności;*** |
| | **AC-16_ODP[05]** | ***określono systemy, dla których mają być ustanowione dozwolone atrybuty bezpieczeństwa;*** |
| | **AC-16_ODP[06]** | ***określono systemy, dla których mają być ustanowione dozwolone atrybuty prywatności;*** |
| | **AC-16_ODP[07]** | ***określono dopuszczalne dla systemów atrybuty bezpieczeństwa, definiowane jako część AC-16a;*** |
| | **AC-16_ODP[08]** | ***określono dopuszczalne dla systemów atrybuty prywatności, definiowane jako część AC-16a;*** |
| | **AC-16_ODP[09]** | ***określono wartości atrybutów lub zakresy dla ustalonych atrybutów;*** |
| | **AC-16_ODP[10]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu atrybutów bezpieczeństwa pod kątem możliwości ich zastosowania;*** |
| | **AC-16_ODP[11]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu atrybutów prywatności pod kątem możliwości ich zastosowania;*** |
| | **AC-16a.[01]** | zapewnione są środki służące do powiązania ***<typów atrybutów bezpieczeństwa AC-16_ODP[01]>*** z ***<wartościami atrybutów bezpieczeństwa AC-16_ODP[03]> w*** odniesieniu do informacji przechowywanych, przetwarzanych lub przekazywanych; |

| **AC-16** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
|---|---|---|
| | **AC-16a.[02]** | zapewnione są środki służące do powiązania ***<typów atrybutów prywatności AC-16_ODP[02]>*** z ***<wartościami atrybutów prywatności AC-16_ODP[04]> w*** odniesieniu do informacji przechowywanych, przetwarzanych lub przekazywanych; |
| | **AC-16b.[01]** | dokonuje się powiązania atrybutów; |
| | **AC-16b.[02]** | powiązania atrybutów są zachowywane wraz z informacjami; |
| | **AC-16c.[01]** | określono następujące dozwolone atrybuty bezpieczeństwa na podstawie atrybutów zdefiniowanych w AC-16_ODP[01] dla ***<systemów AC-16_ODP[05]>***: ***<atrybuty bezpieczeństwa AC-16_ODP[07]>***; |
| | **AC-16c.[02]** | określono następujące dozwolone atrybuty prywatności na podstawie atrybutów zdefiniowanych w AC-16_ODP[02] dla ***<systemów AC-16_ODP[06]>***: ***<atrybuty prywatności AC-16_ODP[08]>***; |
| | **AC-16d.** | określono następujące dopuszczalne wartości lub zakresy atrybutów dla każdego z ustalonych atrybutów: ***<wartości lub zakresy atrybutów AC-16_ODP[09]>***; |
| | **AC-16e.** | zmiany atrybutów podlegają kontroli; |
| | **AC-16f.[01]** | ***<atrybuty bezpieczeństwa AC-16_ODP[07]>*** są sprawdzane pod kątem możliwości zastosowania z ***<częstotliwością AC-16_ODP[10]>***; |
| | **AC-16f.[02]** | ***<atrybuty prywatności AC-16_ODP[08]>*** są sprawdzane pod kątem możliwości zastosowania z ***<częstotliwością AC-16_ODP[11]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **AC-16** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
|---|---|---|
| | **AC-16-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące powiązania atrybutów bezpieczeństwa i prywatności z informacjami przechowywanymi, przetwarzanymi i przesyłanymi; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-16-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; programiści systemu]. |
| | **AC-16-Test** | [WYBÓR SPOŚRÓD: Zdolności organizacyjnej wspierające i utrzymujące powiązanie atrybutów bezpieczeństwa i prywatności z informacjami przechowywanymi, przetwarzanymi i przesyłanymi]. |

| **AC-16(01)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| DYNAMICZNE KOJARZENIE ATRYBUTÓW** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-16(01)_ODP[01]** | ***określono podmioty, z którymi atrybuty bezpieczeństwa mają być dynamicznie kojarzone w miarę tworzenia i łączenia informacji;*** |
| | **AC-16(01)_ODP[02]** | ***określono obiekty, z którymi atrybuty bezpieczeństwa mają być dynamicznie kojarzone w miarę tworzenia i łączenia informacji;*** |
| | **AC-16(01)_ODP[03]** | ***określono podmioty, z którymi atrybuty prywatności mają być dynamicznie kojarzone w miarę tworzenia i łączenia informacji;*** |
| | **AC-16(01)_ODP[04]** | ***określono obiekty, z którymi atrybuty prywatności mają być dynamicznie kojarzone w miarę tworzenia i łączenia informacji;*** |

| | | |
|---|---|---|
| **AC-16(01)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| DYNAMICZNE KOJARZENIE ATRYBUTÓW** | |
| | **AC-16(01)_ODP[05]** | ***określono polityki bezpieczeństwa wymagające dynamicznego powiązania atrybutów bezpieczeństwa z podmiotami i obiektami;*** |
| | **AC-16(01)_ODP[06]** | ***określono polityki prywatności wymagające dynamicznego powiązania atrybutów prywatności z podmiotami i obiektami;*** |
| | **AC-16(01)[01]** | atrybuty bezpieczeństwa są dynamicznie kojarzone z ***<podmiotami AC-16(01)_ODP[01]>*** zgodnie z następującymi zasadami bezpieczeństwa w miarę tworzenia i łączenia informacji: ***<polityki bezpieczeństwa AC-16(01)_ODP[05]>***; |
| | **AC-16(01)[02]** | atrybuty bezpieczeństwa są dynamicznie kojarzone z ***<obiektami AC-16(01)_ODP[02]>*** zgodnie z następującymi zasadami bezpieczeństwa w miarę tworzenia i łączenia informacji: ***<polityki bezpieczeństwa AC-16(01)_ODP[05]>***; |
| | **AC-16(01)[03]** | atrybuty prywatności są dynamicznie kojarzone z ***<podmiotami AC-16(01)_ODP[03]>*** zgodnie z następującymi zasadami bezpieczeństwa w miarę tworzenia i łączenia informacji: ***<polityki bezpieczeństwa AC-16(01)_ODP[06]>***; |
| | **AC-16(01)[04]** | atrybuty prywatności są dynamicznie kojarzone z ***<podmiotami AC-16(01)_ODP[04]>*** zgodnie z następującymi zasadami bezpieczeństwa w miarę tworzenia i łączenia informacji: ***<polityki bezpieczeństwa AC-16(01)_ODP[06]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-16(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące dynamicznego powiązania atrybutów bezpieczeństwa i prywatności z informacjami przechowywanymi, przetwarzanymi i przesyłanymi; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-16(01)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| DYNAMICZNE KOJARZENIE ATRYBUTÓW** | |
| | **AC-16(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; programiści systemu]. |
| | **AC-16(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające dynamiczne powiązanie atrybutów bezpieczeństwa i prywatności z informacjami]. |

| | | |
|---|---|---|
| **AC-16(02)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZMIANY WARTOŚCI ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-16(02)[01]** | upoważnione osoby (lub procesy działające w imieniu osób) mają możliwość definiowania lub zmiany wartości powiązanych atrybutów bezpieczeństwa; |
| | **AC-16(02)[02]** | upoważnione osoby (lub procesy działające w imieniu osób) mają możliwość definiowania lub zmiany wartości powiązanych atrybutów prywatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-16(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zmiany wartości atrybutów bezpieczeństwa i prywatności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista osób upoważnionych do zmiany wartości atrybutów bezpieczeństwa i prywatności; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-16(02)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZMIANY WARTOŚCI ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY** | |
| | **AC-16(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny upoważniony do zmiany wartości atrybutów bezpieczeństwa i prywatności; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-16(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy umożliwiające zmianę wartości atrybutów bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **AC-16(03)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| UTRZYMANIE KOJARZENIA ATRYBUTÓW PRZEZ SYSTEM INFORMATYCZNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-16(03)_ODP[01]** | ***określono atrybuty bezpieczeństwa, które wymagają powiązania i utrzymania integralności;*** |
| | **AC-16(03)_ODP[02]** | ***określono atrybuty prywatności, które wymagają powiązania i utrzymania integralności;*** |
| | **AC-16(03)_ODP[03]** | ***określono podmioty, które wymagają powiązania ze sobą atrybutów bezpieczeństwa oraz utrzymania ich integralności;*** |
| | **AC-16(03)_ODP[04]** | ***określono obiekty, które wymagają powiązania ze sobą atrybutów bezpieczeństwa oraz utrzymania ich integralności;*** |
| | **AC-16(03)_ODP[05]** | ***określono podmioty, które wymagają powiązania ze sobą atrybutów prywatności oraz utrzymania ich integralności;*** |
| | **AC-16(03)_ODP[06]** | ***określono obiekty, które wymagają powiązania ze sobą atrybutów prywatności oraz utrzymania ich integralności;*** |

| | | |
|---|---|---|
| **AC-16(03)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| UTRZYMANIE KOJARZENIA ATRYBUTÓW PRZEZ SYSTEM INFORMATYCZNY** | |
| | **AC-16(03)[01]** | powiązania oraz integralność ***<atrybutów bezpieczeństwa AC-16(03)_ODP[01]>*** względem ***<podmiotów AC-16(03)_ODP[03]>*** są zachowane; |
| | **AC-16(03)[02]** | powiązania oraz integralność ***<atrybutów bezpieczeństwa AC-16(03)_ODP[01]>*** względem ***<obiektów AC-16(03)_ODP[04]>*** są zachowane; |
| | **AC-16(03)[03]** | powiązania oraz integralność ***<atrybutów prywatności AC-16(03)_ODP[02]>*** względem ***<podmiotów AC-16(03)_ODP[05]>*** są zachowane; |
| | **AC-16(03)[04]** | powiązania oraz integralność ***<atrybutów prywatności AC-16(03)_ODP[02]>*** względem ***<obiektów AC-16(03)_ODP[06]>*** są zachowane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-16(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące dynamicznego powiązania atrybutów bezpieczeństwa i prywatności z informacjami przechowywanymi, przetwarzanymi i przesyłanymi; procedury dotyczące etykietowania lub oznaczania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-16(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; programiści systemu]. |
| | **AC-16(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy utrzymujące integralność i powiązania atrybutów bezpieczeństwa i prywatności do informacji]. |

| | | |
|---|---|---|
| **AC-16(04)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| KOJARZENIE ATRYBUTÓW PRZEZ AUTORYZOWANY PERSONEL** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-16(04)_ODP[01]** | ***określono atrybuty bezpieczeństwa, które mają być powiązane z podmiotami przez upoważnione osoby (lub procesy działające w imieniu osób);*** |
| | **AC-16(04)_ODP[02]** | ***określono atrybuty bezpieczeństwa, które mają być powiązane z obiektami przez upoważnione osoby (lub procesy działające w imieniu osób);*** |
| | **AC-16(04)_ODP[03]** | ***określono atrybuty prywatności, które mają być powiązane z podmiotami przez upoważnione osoby (lub procesy działające w imieniu osób);*** |
| | **AC-16(04)_ODP[04]** | ***określono atrybuty prywatności, które mają być powiązane z obiektami przez upoważnione osoby (lub procesy działające w imieniu osób);*** |
| | **AC-16(04)_ODP[05]** | ***określono podmioty wymagające powiązania z atrybutami bezpieczeństwa przez upoważnione osoby (lub procesy działające w imieniu osób);*** |
| | **AC-16(04)_ODP[06]** | ***określono obiekty wymagające powiązania z atrybutami bezpieczeństwa przez upoważnione osoby (lub procesy działające w imieniu osób);*** |
| | **AC-16(04)_ODP[07]** | ***określono podmioty wymagające powiązania z atrybutami prywatności przez upoważnione osoby (lub procesy działające w imieniu osób);*** |
| | **AC-16(04)_ODP[08]** | ***określono obiekty wymagające powiązania z atrybutami prywatności przez upoważnione osoby (lub procesy działające w imieniu osób);*** |
| | **AC-16(04)[01]** | upoważnione osoby (lub procesy działające w imieniu osób) mają możliwość powiązania ***<atrybutów bezpieczeństwa AC-16(04)_ODP[01]>*** z ***<podmiotami AC-16(04)_ODP[05]>***; |
| | **AC-16(04)[02]** | upoważnione osoby (lub procesy działające w imieniu osób) mają możliwość powiązania ***<atrybutów bezpieczeństwa AC-16(04)_ODP[02]>*** z ***<obiektami AC-16(04)_ODP[06]>***; |

| | | |
|---|---|---|
| **AC-16(04)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| KOJARZENIE ATRYBUTÓW PRZEZ AUTORYZOWANY PERSONEL** | |
| | **AC-16(04)[03]** | upoważnione osoby (lub procesy działające w imieniu osób) mają możliwość powiązania ***<atrybutów prywatności AC-16(04)_ODP[03]>*** z ***<podmiotami AC-16(04)_ODP[07]>***; |
| | **AC-16(04)[04]** | upoważnione osoby (lub procesy działające w imieniu osób) mają możliwość powiązania ***<atrybutów prywatności AC-16(04)_ODP[04]>*** z ***<obiektami AC-16(04)_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-16(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące powiązania atrybutów bezpieczeństwa i prywatności z informacjami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista użytkowników upoważnionych do powiązania atrybutów bezpieczeństwa i prywatności z informacjami; komunikaty systemowe dla użytkowników uprzywilejowanych dotyczące wyboru atrybutów bezpieczeństwa i prywatności, które mają być powiązane z obiektami informacji; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-16(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za powiązanie atrybutów bezpieczeństwa i prywatności z informacjami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-16(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające powiązanie atrybutów bezpieczeństwa i prywatności z informacjami przez użytkowników]. |

| | | |
|---|---|---|
| **AC-16(05)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ATRYBUTY BEZPIECZEŃSTWA PREZENTOWANE NA WYŚWIETLACZACH URZĄDZEŃ WYJŚCIOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-16(05)_ODP[01]** | ***określono specjalne instrukcje rozpowszechniania, obsługi lub dystrybucji, które mają być stosowane w odniesieniu do każdego obiektu przekazywanego przez system do urządzeń wyjściowych;*** |
| | **AC-16(05)_ODP[02]** | ***określono czytelną dla człowieka, standardową nomenklaturę dla atrybutów bezpieczeństwa i prywatności, które mają być wyświetlane w czytelnej dla człowieka formie na każdym obiekcie, który system przekazuje do urządzeń wyjściowych;*** |
| | **AC-16(05)[01]** | na każdym obiekcie przekazywanym przez system do urządzeń wyjściowych wyświetlane są atrybuty bezpieczeństwa w formie czytelnej dla człowieka w celu identyfikacji ***<instrukcji AC-16(05)_ODP[01]>*** przy użyciu ***<nomenklatury AC-16(05)_ODP[02]>***; |
| | **AC-16(05)[02]** | Na każdym obiekcie przekazywanym przez system do urządzeń wyjściowych wyświetlane są atrybuty prywatności w formie czytelnej dla człowieka w celu identyfikacji ***<instrukcji AC-16(05)_ODP[01]>*** przy użyciu ***<nomenklatury AC-16(05)_ODP[02]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-16(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące wyświetlania atrybutów bezpieczeństwa i prywatności w formie czytelnej dla człowieka; specjalne instrukcje rozpowszechniania, obsługi lub dystrybucji; rodzaje czytelnej dla człowieka, standardowej nomenklatury; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-16(05)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ATRYBUTY BEZPIECZEŃSTWA PREZENTOWANE NA WYŚWIETLACZACH URZĄDZEŃ WYJŚCIOWYCH** | |
| | **AC-16(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; programiści systemu]. |
| | **AC-16(05)-Test** | [WYBÓR SPOŚRÓD: Urządzenia wyjściowe systemu wyświetlające atrybuty bezpieczeństwa i prywatności w formie czytelnej dla człowieka na każdym obiekcie]. |

| | | |
|---|---|---|
| **AC-16(06)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZARZĄDZANIE POWIĄZANYMI ATRYBUTAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-16(06)_ODP[01]** | ***określono atrybuty bezpieczeństwa, które mają być powiązane z podmiotami;*** |
| | **AC-16(06)_ODP[02]** | ***określono atrybuty bezpieczeństwa, które mają być powiązane z obiektami;*** |
| | **AC-16(06)_ODP[03]** | ***określono atrybuty prywatności , które mają być powiązane z podmiotami;*** |
| | **AC-16(06)_ODP[04]** | ***określono atrybuty prywatności , które mają być powiązane z obiektami;*** |
| | **AC-16(06)_ODP[05]** | ***określono podmioty, które mają być powiązane z atrybutami bezpieczeństwa informacji;*** |
| | **AC-16(06)_ODP[06]** | ***określono obiekty, które mają być powiązane z atrybutami bezpieczeństwa informacji;*** |
| | **AC-16(06)_ODP[07]** | ***określono podmioty, które mają być powiązane z atrybutami prywatności;*** |

| | | |
|---|---|---|
| **AC-16(06)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZARZĄDZANIE POWIĄZANYMI ATRYBUTAMI** | |
| | **AC-16(06)_ODP[08]** | ***określono obiekty, które mają być powiązane z atrybutami prywatności;*** |
| | **AC-16(06)_ODP[09]** | ***polityki bezpieczeństwa, które wymagają od personelu powiązania i utrzymania powiązania atrybutów bezpieczeństwa i prywatności z podmiotami i obiektami;*** |
| | **AC-16(06)_ODP[10]** | ***polityki prywatności, które wymagają od personelu powiązania i utrzymania powiązania atrybutów bezpieczeństwa i prywatności z podmiotami i obiektami;*** |
| | **AC-16(06)[01]** | personel zobowiązany jest zapewnić powiązanie oraz utrzymanie powiązania ***<atrybutów bezpieczeństwa AC-16(06)_ODP[01]> z <podmiotami AC-16(06)_ODP[05] podmiotami>*** zgodnie z ***<politykami bezpieczeństwa AC-16(06)_ODP[09]>***; |
| | **AC-16(06)[02]** | personel zobowiązany jest zapewnić powiązanie oraz utrzymanie powiązania ***<atrybutów bezpieczeństwa AC-16(06)_ODP[02]> z <obiektami AC-16(06)_ODP[06]>*** zgodnie z ***<politykami bezpieczeństwa AC-16(06)_ODP[09]>***; |
| | **AC-16(06)[03]** | personel zobowiązany jest zapewnić powiązanie oraz utrzymanie powiązania ***<atrybutów prywatności AC-16(06)_ODP[03]> z <podmiotami AC-16(06)_ODP[07]>*** zgodnie z ***<politykami prywatności AC-16(06)_ODP[10]>***; |
| | **AC-16(06)[04]** | personel zobowiązany jest zapewnić powiązanie oraz utrzymanie powiązania ***<atrybutów prywatności AC-16(06)_ODP[04]> z <podmiotami AC-16(06)_ODP[08]>*** zgodnie z ***<politykami prywatności AC-16(06)_ODP[10]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-16(06)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZARZĄDZANIE POWIĄZANYMI ATRYBUTAMI** | |
| | **AC-16(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące powiązania atrybutów bezpieczeństwa i prywatności z podmiotami i obiektami; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-16(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za powiązanie i utrzymywanie powiązania atrybutów bezpieczeństwa i prywatności z podmiotami i obiektami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-16(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające działania w zakresie powiązania atrybutów bezpieczeństwa i prywatności z podmiotami i obiektami]. |

| | | |
|---|---|---|
| **AC-16(07)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| INTERPRETACJA WSPÓLNYCH ATRYBUTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-16(07)[01]** | zapewniona jest spójna interpretacja atrybutów bezpieczeństwa przekazywanych pomiędzy komponentami systemu rozproszonego; |
| | **AC-16(07)[02]** | zapewniona jest spójna interpretacja atrybutów prywatności przekazywanych pomiędzy komponentami systemu rozproszonego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-16(07)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| INTERPRETACJA WSPÓLNYCH ATRYBUTÓW** | |
| | **AC-16(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury kontroli dostępu; procedury dotyczące spójnej interpretacji atrybutów bezpieczeństwa i prywatności przekazywanych między komponentami systemu rozproszonego; procedury dotyczące egzekwowania zasad kontroli dostępu;<br>procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy audytu systemu; plan bezpieczeństwa systemu; polityka kontroli dostępu do zabezpieczeń prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-16(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zapewnienie spójnej interpretacji atrybutów bezpieczeństwa i prywatności wykorzystywanych w działaniach związanych z egzekwowaniem zasad dostępu i przepływu informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-16(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania zasad dostępu i przepływu informacji]. |

| | | |
|---|---|---|
| **AC-16(08)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| TECHNIKI I TECHNOLOGIE WIĄZANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-16(08)_ODP[01]** | ***określono techniki i technologie, które należy wdrożyć w powiązaniu atrybutów bezpieczeństwa z informacjami;*** |
| | **AC-16(08)_ODP[02]** | ***określono techniki i technologie, które należy wdrożyć w powiązaniu atrybutów prywatności z informacjami;*** |

| | | |
|---|---|---|
| **AC-16(08)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| TECHNIKI I TECHNOLOGIE WIĄZANIA** | |
| | **AC-16(08)[01]** | ***<techniki i technologie AC-16(08)_ODP[01]>*** są wdrażane w procesie powiązania atrybutów bezpieczeństwa z informacjami; |
| | **AC-16(08)[02]** | ***<techniki i technologie AC-16(08)_ODP[02]>*** są wdrażane w procesie powiązania atrybutów prywatności z informacjami; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-16(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące powiązania atrybutów bezpieczeństwa i prywatności z informacjami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-16(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za powiązanie atrybutów bezpieczeństwa i prywatności z informacjami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-16(08)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające powiązanie atrybutów bezpieczeństwa i prywatności z informacjami]. |

| | | |
|---|---|---|
| **AC-16(09)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| PONOWNY PRZYDZIAŁ ATRYBUTÓW - MECHANIZMY ZMIANY KLASYFIKACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-16(09)_ODP[01]** | ***określono techniki lub procedury stosowane do walidacji mechanizmów reklasyfikacji atrybutów bezpieczeństwa;*** |

| | | |
|---|---|---|
| **AC-16(09)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| PONOWNY PRZYDZIAŁ ATRYBUTÓW - MECHANIZMY ZMIANY KLASYFIKACJI** | |
| | **AC-16(09)_ODP[02]** | ***określono techniki lub procedury stosowane do walidacji mechanizmów reklasyfikacji atrybutów prywatności;*** |
| | **AC-16(09)[01]** | atrybuty bezpieczeństwa powiązane z informacjami są zmieniane tylko poprzez mechanizmy reklasyfikacji zatwierdzone przy użyciu ***<technik lub procedur AC-16(09)_ODP[01]>***; |
| | **AC-16(09)[02]** | atrybuty prywatności powiązane z informacjami są zmieniane tylko poprzez mechanizmy reklasyfikacji zatwierdzone przy użyciu ***<technik lub procedur AC-16(09)_ODP[02]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-16(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dot. ponownego przypisania atrybutów bezpieczeństwa do informacji; dokumentacja projektowa systemu;<br>ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne stosowne dokumenty lub zapisy]. |
| | **AC-16(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ponowne przypisanie atrybutów bezpieczeństwa i prywatności z informacjami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-16(09)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające techniki lub procedury ponownego przypisywania atrybutów bezpieczeństwa i prywatności do informacji]. |

| | | |
|---|---|---|
| **AC-16(10)** | **ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| KONFIGURACJA ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-16(10)[01]** | osoby upoważnione mają możliwość definiowania lub zmiany rodzaju i wartości atrybutów bezpieczeństwa dostępnych do skojarzenia z podmiotami i obiektami; |
| | **AC-16(10)[02]** | osoby upoważnione mają możliwość definiowania lub zmiany rodzaju i wartości atrybutów prywatności dostępnych do skojarzenia z podmiotami i obiektami. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-16(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące konfiguracji atrybutów bezpieczeństwa i prywatności przez osoby upoważnione; dokumentacja projektowa systemu;<br>ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-16(10)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za definiowanie lub zmianę atrybutów bezpieczeństwa i prywatności związanych z informacjami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-16(10)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwość definiowania lub zmiany atrybutów bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **AC-17** | **DOSTĘP ZDALNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-17a.[01]** | dla każdego rodzaju dozwolonego zdalnego dostępu ustanowione i udokumentowane są ograniczenia w użytkowaniu; |
| | **AC-17a.[02]** | dla każdego rodzaju dozwolonego zdalnego dostępu ustanowione i udokumentowane są wymagania dotyczące konfiguracji/połączeń; |
| | **AC-17a.[03]** | dla każdego rodzaju dozwolonego zdalnego dostępu ustanowiono i udokumentowano wytyczne dotyczące wdrażania; |
| | **AC-17b.** | każdy rodzaj zdalnego dostępu do systemu podlega autoryzacji przed zezwoleniem na takie połączenie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-17-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dot. wdrażania i wykorzystania zdalnego dostępu (w tym ograniczenia); plan zarządzania konfiguracją; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; uprawnienia do zdalnego dostępu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-17-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie połączeniami zdalnego dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-17-Test** | [WYBÓR SPOŚRÓD: Możliwość zarządzania zdalnym dostępem do systemu]. |

| | | |
|---|---|---|
| **AC-17(01)** | **DOSTĘP ZDALNY \| AUTOMATYCZNE MONITOROWANIE I KONTROLA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-17(01)[01]** | Do monitorowania metod zdalnego dostępu stosowane są mechanizmy automatyczne; |
| | **AC-17(01)[02]** | Do kontrolowania metod zdalnego dostępu stosowane są mechanizmy automatyczne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-17(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zdalnego dostępu do systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; zapisy z monitorowania systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-17(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-17(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy monitorowania i kontroli metod zdalnego dostępu]. |

| | | |
|---|---|---|
| **AC-17(02)** | **DOSTĘP ZDALNY \| OCHRONA POUFNOŚCI I INTEGRALNOŚCI Z WYKORZYSTANIEM SZYFROWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-17(02)** | Do ochrony poufności i integralności sesji zdalnego dostępu stosuje się mechanizmy kryptograficzne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-17(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zdalnego dostępu do systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; mechanizmy kryptograficzne i związana z nimi dokumentacja konfiguracyjna;<br>zapisy audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-17(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-17(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne chroniące poufność i integralność sesji zdalnego dostępu]. |

| | | |
|---|---|---|
| **AC-17(03)** | **DOSTĘP ZDALNY \| ZARZĄDZANE PUNKTY KONTROLI DOSTĘPU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-17(03)** | połączenia dostępu zdalnego są przekierowywane przez autoryzowane punkty kontroli dostępu do sieci. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| AC-17(03) | DOSTĘP ZDALNY \| ZARZĄDZANE PUNKTY KONTROLI DOSTĘPU | |
|---|---|---|
| | **AC-17(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zdalnego dostępu do systemu; dokumentacja projektowa systemu; lista wszystkich zarządzanych punktów kontroli dostępu do sieci; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-17(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-17(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy przekierowujące wszystkie połączenia zdalnego dostępu przez autoryzowane punkty kontroli dostępu do sieci]. |

| AC-17(04) | DOSTĘP ZDALNY \| POLECENIA UPRZYWILEJOWANE I DOSTĘP | |
|---|---|---|
| | **CEL OCENY:**<br><br>*Ustalenie, czy:* | |
| | **AC-17(04)_ODP[01]** | ***określono potrzeby wymagające wykonania uprzywilejowanych poleceń przez zdalny dostęp;*** |
| | **AC-17(04)_ODP[02]** | ***określono sytuacje wymagające dostępu do informacji istotnych dla bezpieczeństwa poprzez dostęp zdalny;*** |
| | **AC-17(04)(a)[01]** | wykonywanie uprzywilejowanych poleceń za pośrednictwem zdalnego dostępu jest dozwolone tylko w formacie umożliwiającym ocenę dowodów; |

| | | |
|---|---|---|
| **AC-17(04)** | **DOSTĘP ZDALNY \| POLECENIA UPRZYWILEJOWANE I DOSTĘP** | |
| | **AC-17(04)(a)[02]** | dostęp do informacji istotnych dla bezpieczeństwa za pośrednictwem zdalnego dostępu jest dozwolony wyłącznie w formacie zapewniającym możliwe do oceny dowody; |
| | **AC-17(04)(a)[03]** | wykonanie uprzywilejowanych poleceń poprzez dostęp zdalny jest dozwolony tylko w następujących sytuacjach: ***<sytuacje wymagające zdalnego dostępu AC-17(04)_ODP[01]>***; |
| | **AC-17(04)(a)[04]** | dostęp do informacji istotnych dla bezpieczeństwa za pośrednictwem zdalnego dostępu jest dozwolony wyłącznie w następujących sytuacjach: ***<AC-17(04)_ODP[02] potrzeby wymagające zdalnego dostępu>***; |
| | **AC-17(04)(b)** | uzasadnienie dla zdalnego dostępu jest udokumentowane w planie bezpieczeństwa dla systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-17(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zdalnego dostępu do systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa; zapisy audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-17(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **AC-17(04)** | **DOSTĘP ZDALNY \| POLECENIA UPRZYWILEJOWANE I DOSTĘP** | |
| | **AC-17(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zarządzanie zdalnym dostępem]. |

| | |
|---|---|
| **AC-17(05)** | **DOSTĘP ZDALNY \| MONITOROWANIE NIEAUTORYZOWANYCH POŁĄCZEŃ** |
| | [WYCOFANE: Włączone do SI-04]. |

| | | |
|---|---|---|
| **AC-17(06)** | **DOSTĘP ZDALNY \| OCHRONA MECHANIZMÓW DOSTĘPU ZDALNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-17(06)** | informacje o mechanizmach zdalnego dostępu są chronione przed nieuprawnionym użyciem i ujawnieniem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-17(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące zdalnego dostępu do systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-17(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za wdrożenie lub monitorowanie zdalnego dostępu do systemu; użytkownicy systemu posiadający wiedzę o mechanizmach zdalnego dostępu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | |
|---|---|
| **AC-17(07)** | **DOSTĘP ZDALNY \| DODATKOWA OCHRONA DOSTĘPU DO FUNKCJI BEZPIECZEŃSTWA** |
| | [WYCOFANE: Włączone do AC-03(10)]. |

| | |
|---|---|
| **AC-17(08)** | **DOSTĘP ZDALNY \| WYŁĄCZANIE NIEZABEZPIECZONYCH PROTOKOŁÓW SIECIOWYCH** |
| | [WYCOFANE: Włączone do CM-07]. |

| | | |
|---|---|---|
| **AC-17(09)** | **DOSTĘP ZDALNY \|ODŁĄCZENIE LUB WYŁĄCZENIE DOSTĘPU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-17(09)_ODP** | ***określono okres, po którym należy odłączyć lub zablokować dostęp zdalny do systemu;*** |
| | **AC-17(09)** | zapewniono możliwość rozłączenia lub zablokowania zdalnego dostępu do systemu w ***<okresie AC-17(09)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-17(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące odłączania lub wyłączania zdalnego dostępu do systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa, zapisy audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-17(09)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-17(09)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwość rozłączenia lub zablokowania zdalnego dostępu do systemu]. |

| | | |
|---|---|---|
| **AC-17(10)** | **DOSTĘP ZDALNY \| UWIERZYTELNIANIE ZDALNYCH POLECEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-17(10)_ODP[01]** | ***określono mechanizmy wdrożone do uwierzytelniania zdalnych poleceń;*** |
| | **AC-17(10)_ODP[02]** | ***określono zdalne polecenia, które mają być uwierzytelnione przez mechanizmy;*** |
| | **AC-17(10)** | wdrożono ***<mechanizmy AC-17(10)_ODP[01]> w*** celu uwierzytelniania ***<poleceń zdalnych AC-17(10)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-17(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące uwierzytelniania zdalnych poleceń; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-17(10)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-17(10)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające uwierzytelniania zdalnych poleceń]. |

| | | |
|---|---|---|
| **AC-18** | **DOSTĘP BEZPRZEWODOWY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-18a.[01]** | Dla każdego rodzaju dostępu bezprzewodowego ustalane są wymagania konfiguracyjne; |
| | **AC-18a.[02]** | Dla każdego rodzaju dostępu bezprzewodowego ustalane są wymagania w zakresie połączenia; |
| | **AC-18a.[03]** | Dla każdego rodzaju dostępu bezprzewodowego ustala się wytyczne dotyczące wdrażania; |
| | **AC-18b.** | Każdy rodzaj bezprzewodowego dostępu do systemu podlega autoryzacji przed zezwoleniem na takie połączenie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-18-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące wdrożenia i wykorzystania dostępu bezprzewodowego (w tym ograniczenia); plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; upoważnienia do dostępu bezprzewodowego; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-18-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie połączeniami dostępu bezprzewodowego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-18-Test** | [WYBÓR SPOŚRÓD: Możliwość zarządzania dostępem bezprzewodowym w systemie]. |

| | | |
|---|---|---|
| **AC-18(01)** | **DOSTĘP BEZPRZEWODOWY \| UWIERZYTELNIANIE ORAZ SZYFROWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-18(01)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {użytkownicy; urządzenia};*** |
| | **AC-18(01)[01]** | bezprzewodowy dostęp do systemu jest chroniony za pomocą mechanizmu uwierzytelniania z ***<WYBRANA WARTOŚĆ PARAMETRU AC-18(01)_ODP>***; |
| | **AC-18(01)[02]** | bezprzewodowy dostęp do systemu jest chroniony za pomocą szyfrowania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-18(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące wdrożenia i wykorzystania sieci bezprzewodowej (w tym ograniczenia); dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-18(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-18(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zabezpieczenia w zakresie bezprzewodowego dostępu do systemu]. |

| | |
|---|---|
| **AC-18(02)** | **DOSTĘP BEZPRZEWODOWY \| MONITOROWANIE POŁĄCZEŃ NIEAUTORYZOWANYCH** |
| | [WYCOFANE: Włączone do SI-04]. |

| | | |
|---|---|---|
| **AC-18(03)** | **DOSTĘP BEZPRZEWODOWY \| DEZAKTYWACJA SIECI BEZPRZEWODOWEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-18(03)** | funkcje sieci bezprzewodowej wbudowane w elementy systemu są wyłączane przed ich wydaniem i wdrożeniem, jeśli nie są przeznaczone do użytku. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-18(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące wdrożenia i wykorzystania sieci bezprzewodowej (w tym ograniczenia); dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-18(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-18(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy umożliwiające wyłączanie środków łączności bezprzewodowej wbudowanych w elementy systemu]. |

| | | |
|---|---|---|
| **AC-18(04)** | **DOSTĘP BEZPRZEWODOWY \| OGRANICZENIE DOKONYWANIA KONFIGURACJI PRZEZ UŻYTKOWNIKÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-18(04)[01]** | określono użytkowników, którzy mogą samodzielnie konfigurować funkcje sieci bezprzewodowej; |
| | **AC-18(04)[02]** | użytkownicy, którzy mogą samodzielnie konfigurować funkcje sieci bezprzewodowej, są do tego wyraźnie upoważnieni. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-18(04)** | **DOSTĘP BEZPRZEWODOWY \| OGRANICZENIE DOKONYWANIA KONFIGURACJI PRZEZ UŻYTKOWNIKÓW** | |
| | **AC-18(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące wdrożenia i wykorzystania sieci bezprzewodowej (w tym ograniczenia); dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-18(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-18(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy autoryzujące niezależną konfigurację użytkownika w zakresie możliwości sieci bezprzewodowych]. |

| | | |
|---|---|---|
| **AC-18(05)** | **DOSTĘP BEZPRZEWODOWY \| POZIOMY MOCY ANTEN/TRANSMISJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-18(05)[01]** | anteny radiowe są dobrane tak, aby zmniejszyć prawdopodobieństwo odbioru sygnałów z bezprzewodowych punktów dostępowych poza obszarem kontrolowanym przez organizację; |
| | **AC-18(05)[02]** | poziom mocy nadawania jest skalibrowany tak, aby zmniejszyć prawdopodobieństwo odbioru sygnałów z bezprzewodowych punktów dostępowych poza obszarem kontrolowanym przez organizację; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-18(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące wdrożenia i wykorzystania sieci bezprzewodowej (w tym ograniczenia); dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| AC-18(05) | DOSTĘP BEZPRZEWODOWY \| POZIOMY MOCY ANTEN/TRANSMISJI | |
|---|---|---|
| | **AC-18(05)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-18(05)-Test** | [WYBÓR SPOŚRÓD: Kalibracja poziomów mocy nadawania dla urządzeń dostępu bezprzewodowego; sygnały anten radiowych dla urządzeń dostępu bezprzewodowego; odbiór sygnału dostępu bezprzewodowego poza obszarem kontrolowanym przez organizację]. |

| AC-19 | KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-19a.[01]** | ustanowiono wymagania konfiguracyjne dla urządzeń przenośnych kontrolowanych przez organizację, również w przypadku, gdy urządzenia te znajdują się poza obszarem kontrolowanym; |
| | **AC-19a.[02]** | ustanowiono wymagania dotyczące połączeń dla urządzeń przenośnych kontrolowanych przez organizację, również w przypadku, gdy urządzenia te znajdują się poza obszarem kontrolowanym; |
| | **AC-19a.[03]** | ustanowiono wytyczne wdrożeniowe dla urządzeń przenośnych kontrolowanych przez organizację, w tym w przypadku, gdy takie urządzenia znajdują się poza obszarem kontrolowanym; |
| | **AC-19b.** | do podłączenia urządzeń przenośnych do systemów organizacji wymaga się uwierzytelnienia. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| AC-19 | KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH | |
|---|---|---|
| | **AC-19-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące kontroli dostępu do urządzeń przenośnych (w tym ograniczenia); plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; uwierzytelnianie połączeń urządzeń przenośnych z systemami organizacji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-19-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny wykorzystujący urządzenia przenośne do dostępu do systemów organizacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-19-Test** | [WYBÓR SPOŚRÓD: Możliwość kontroli dostępu w zakresie połączeń urządzeń przenośnych z systemami organizacji; konfiguracja urządzeń przenośnych]. |

| AC-19(01) | KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH \| KORZYSTANIE Z ZAPISYWALNYCH I PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH |
|---|---|
| | [WYCOFANE: Włączone do MP-07]. |

| AC-19(02) | KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH \| KORZYSTANIE Z OSOBISTYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH |
|---|---|
| | [WYCOFANE: Włączone do MP-07]. |

| AC-19(03) | KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH \| KORZYSTANIE Z OGÓLNODOSTĘPNYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH |
|---|---|
| | [WYCOFANE: Włączone do MP-07]. |

| | | |
|---|---|---|
| **AC-19(04)** | **KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH \| OGRANICZENIA DOTYCZĄCE INFORMACJI NIEJAWNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-19(04)_ODP[01]** | ***określono urzędników ds. bezpieczeństwa odpowiedzialnych za przegląd i kontrolę jawnych urządzeń przenośnych oraz informacji przechowywanych na tych urządzeniach;*** |
| | **AC-19(04)_ODP[02]** | ***określono polityki bezpieczeństwa ograniczające podłączanie niejawnych urządzeń przenośnych do niejawnych systemów;*** |
| | **AC-19(04)(a)** | korzystanie z nieklasyfikowanych urządzeń przenośnych w obiektach, na terenie których znajdują się systemy przetwarzające, przechowujące lub przesyłające informacje uznaje się za zabronione, chyba że jest to wyraźnie dozwolone przez upoważnioną osobę; |
| | **AC-19(04)(b)(01)** | egzekwuje się zakaz podłączania jawnych urządzeń przenośnych do systemów niejawnych w stosunku do osób, którym oficjalnie zezwolono na korzystanie z jawnych urządzeń przenośnych na terenie obiektów zawierających systemy przetwarzające, przechowujące lub przekazujące informacje niejawne; |
| | **AC-19(04)(b)(02)** | egzekwuje się wymóg posiadania zgody uprawnionej osoby na podłączenie jawnych urządzeń przenośnych do niejawnych systemów wobec osób dopuszczonych do korzystania z jawnych urządzeń przenośnych w obiektach zawierających systemy przetwarzające, przechowujące lub przekazujące informacje niejawne; |
| | **AC-19(04)(b)(03)** | egzekwuje się zakaz używania wewnętrznych lub zewnętrznych modemów lub interfejsów bezprzewodowych w jawnych urządzeniach przenośnych wobec osób, którym oficjalnie zezwolono na używanie jawnych urządzeń przenośnych w obiektach zawierających systemy przetwarzające, przechowujące lub przekazujące informacje niejawne; |

| | | |
|---|---|---|
| **AC-19(04)** | **KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH \| OGRANICZENIA DOTYCZĄCE INFORMACJI NIEJAWNYCH** | |
| | **AC-19(04)(b)[01]** | stosuje się wyrywkowy przegląd i kontrolę jawnych urządzeń przenośnych oraz informacji przechowywanych na tych urządzeniach przez ***<urzędników ds. bezpieczeństwa AC-19(04)_ODP[01]>***; |
| | **AC-19(04)(b)[02]** | stosuje się zapisy polityki obsługi incydentów w przypadku odkrycia informacji niejawnych podczas wyrywkowego przeglądu i kontroli jawnych urządzeń przenośnych; |
| | **AC-19(04)(c)** | podłączanie niejawnych urządzeń przenośnych do jawnych systemów jest ograniczone zgodnie z ***<polityką bezpieczeństwa AC-19(04)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-19(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; polityka obsługi incydentów; procedury dotyczące kontroli dostępu do urządzeń przenośnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dowodowa dotycząca wyrywkowych inspekcji i przeglądów urządzeń przenośnych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-19(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za wyrywkowe przeglądy/kontrole urządzeń przenośnych; personel organizacyjny korzystający z urządzeń przenośnych w obiektach zawierających systemy przetwarzające, przechowujące lub przekazujące informacje niejawne; personel organizacyjny odpowiedzialny za reagowanie na incydenty; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji].<br><br>administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **AC-19(04)** | **KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH \| OGRANICZENIA DOTYCZĄCE INFORMACJI NIEJAWNYCH** | |
| | **AC-19(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zakazujące stosowania wewnętrznych lub zewnętrznych modemów lub interfejsów bezprzewodowych z urządzeniami przenośnymi]. |

| | | |
|---|---|---|
| **AC-19(05)** | **KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH \| SZYFROWANIE ZAWARTOŚCI CAŁEGO URZĄDZENIA/WYBRANYCH ZASOBÓW URZĄDZENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-19(05)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {szyfrowanie całego urządzenia; szyfrowanie oparte na kontenerze};*** |
| | **AC-19(05)_ODP[02]** | ***określono urządzenia przenośne, w których można zastosować tymczasowe szyfrowanie;*** |
| | **AC-19(05)** | ***<WYBRANA WARTOŚĆ PARAMETRU AC-19(05)_ODP[01]>*** jest stosowana w celu ochrony poufności i integralności informacji na ***<urządzeniach mobilnych AC-19(05)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-19(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące kontroli dostępu do urządzeń przenośnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; mechanizmy szyfrowania i związana z nimi dokumentacja konfiguracyjna; zapisy audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-19(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu do urządzeń przenośnych; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **AC-19(05)** | **KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH \| SZYFROWANIE ZAWARTOŚCI CAŁEGO URZĄDZENIA/WYBRANYCH ZASOBÓW URZĄDZENIA** | |
| | **AC-19(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy szyfrowania chroniące poufność i integralność informacji w urządzeniach mobilnych]. |

| | | |
|---|---|---|
| **AC-20** | **WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-20_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {ustalenie.***<br>***<warunków AC-20_ODP[02] >; określenie <ustanowienia kontroli AC-20_ODP[03]>};*** |
| | **AC-20_ODP[02]** | ***określono warunki zgodne z relacjami zaufania nawiązanymi z innymi organizacjami posiadającymi, obsługującymi lub utrzymującymi systemy zewnętrzne (jeśli wybrano);*** |
| | **AC-20_ODP[03]** | ***określono zabezpieczenia, które mają być wdrożone w systemach zewnętrznych zgodnie z relacjami zaufania nawiązanymi z innymi organizacjami posiadającymi, obsługującymi lub utrzymującymi systemy zewnętrzne;*** |
| | **AC-20_ODP[04]** | ***określono rodzaje systemów zewnętrznych, których używanie jest zabronione;*** |
| | **AC-20a.1** | ***<WYBRANA WARTOŚĆ PARAMETRU AC-20_ODP[01]>*** jest/są zgodna(-e) z relacjami zaufania nawiązanymi z innymi organizacjami posiadającymi, obsługującymi lub utrzymującymi systemy zewnętrzne, umożliwiając uprawnionym osobom dostęp do systemu z systemów zewnętrznych (jeśli dotyczy); |

| | | |
|---|---|---|
| **AC-20** | **WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH** | |
| | **AC-20a.2** | ***<WYBRANA WARTOŚĆ PARAMETRU AC-20_ODP[01]>*** jest/są zgodna(-e) z relacjami zaufania nawiązanymi z innymi organizacjami posiadającymi, obsługującymi lub utrzymującymi systemy zewnętrzne, umożliwiając upoważnionym osobom przetwarzanie, przechowywanie lub przekazywanie informacji kontrolowanych przez organizację przy użyciu systemów zewnętrznych (jeśli dotyczy); |
| | **AC-20b.** | zabronione jest stosowanie ***<zabronionych rodzajów systemów zewnętrznych AC-20_ODP[04]>*** (jeżeli dotyczy). |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-20-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące korzystania z systemów zewnętrznych; warunki korzystania z systemów zewnętrznych; lista rodzajów aplikacji dostępnych z systemów zewnętrznych; maksymalna kategoria bezpieczeństwa dla informacji przetwarzanych, przechowywanych lub przekazywanych w systemach zewnętrznych; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-20-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za definiowanie warunków korzystania z systemów zewnętrznych w celu uzyskania dostępu do systemów organizacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-20-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające warunki w zakresie korzystania z systemów zewnętrznych]. |

| | | |
|---|---|---|
| **AC-20(01)** | **WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH \| OGRANICZENIA AUTORYZOWANEGO DOSTĘPU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-20(01)(a)** | osoby upoważnione mogą korzystać z systemu zewnętrznego w celu uzyskania dostępu do systemu lub w celu przetwarzania, przechowywania lub przekazywania informacji kontrolowanych przez organizację wyłącznie po zweryfikowaniu wdrożenia zabezpieczeń w systemie zewnętrznym zgodnie z polityką bezpieczeństwa i prywatności organizacji oraz planami bezpieczeństwa i prywatności (jeśli dotyczy) |
| | **AC-20(01)(b)** | osoby upoważnione mogą korzystać z systemu zewnętrznego w celu uzyskania dostępu do systemu lub w celu przetwarzania, przechowywania lub przekazywania informacji kontrolowanych przez organizację tylko po zawarciu zatwierdzonych umów dotyczących połączenia z systemem lub przetwarzania z jednostką organizacyjną hostującą system zewnętrzny (jeśli dotyczy). |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-20(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące korzystania z systemów zewnętrznych; umowy dotyczące podłączenia do systemu lub przetwarzania danych; dokumenty dotyczące zarządzania kontem; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-20(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-20(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające ograniczenia w użytkowaniu systemów zewnętrznych]. |

| | | |
|---|---|---|
| **AC-20(02)** | **KORZYSTANIE Z SYSTEMÓW ZEWNĘTRZNYCH \| PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE - OGRANICZONE ZASTOSOWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-20(02)_ODP** | ***określono ograniczenia dotyczące korzystania przez uprawnione osoby z kontrolowanych przez organizację przenośnych urządzeń pamięci masowej w systemach zewnętrznych;*** |
| | **AC-20(02)** | korzystanie z kontrolowanych przez organizację przenośnych urządzeń pamięci masowej przez osoby upoważnione jest ograniczone w systemach zewnętrznych przy użyciu ***<ograniczeń AC-20(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-20(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące korzystania z systemów zewnętrznych; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; umowy dotyczące podłączenia do systemu lub przetwarzania danych; dokumenty dotyczące zarządzania kontem; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-20(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ograniczenie lub zakaz używania kontrolowanych przez organizację urządzeń pamięci masowej w systemach zewnętrznych; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-20(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające ograniczenia w korzystaniu z przenośnych urządzeń pamięci masowej]. |

| | | |
|---|---|---|
| **AC-20(03)** | **KORZYSTANIE Z SYSTEMÓW ZEWNĘTRZNYCH \| SYSTEMY NIENALEŻĄCE DO ORGANIZACJI - OGRANICZONE ZASTOSOWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-20(03)_ODP** | ***określono ograniczenia dotyczące wykorzystania systemów lub komponentów systemów niebędących własnością organizacji do przetwarzania, przechowywania lub przekazywania informacji organizacyjnych;*** |
| | **AC-20(03)** | wykorzystanie systemów lub komponentów systemów niebędących własnością organizacji do przetwarzania, przechowywania lub przekazywania informacji organizacyjnych podlega ***<ograniczeniom AC-20(03)_ODP>*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-20(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące korzystania z systemów zewnętrznych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; umowy dotyczące podłączenia do systemu lub przetwarzania danych; dokumenty dotyczące zarządzania kontami; zapisy z audytu systemu, inne istotne dokumenty lub zapisy]. |
| | **AC-20(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ograniczenie lub zakaz korzystania z systemów, komponentów systemu lub urządzeń niebędących własnością organizacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-20(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy realizujące ograniczenia w korzystaniu z systemów, komponentów lub urządzeń niebędących własnością organizacji]. |

| | | |
|---|---|---|
| **AC-20(04)** | **KORZYSTANIE Z SYSTEMÓW ZEWNĘTRZNYCH \| SIECIOWE URZĄDZENIA MAGAZYNUJĄCE – ZAKAZ UŻYWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-20(04)_ODP** | ***określono sieciowe urządzenia pamięci masowej, których używanie w systemach zewnętrznych jest zabronione;*** |
| | **AC-20(04)** | W systemach zewnętrznych zabronione jest stosowanie ***<sieciowych urządzeń pamięci masowej AC-20(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-20(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące wykorzystania sieciowych urządzeń pamięci masowej w systemach zewnętrznych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; umowy dotyczące przyłączenia do systemu lub przetwarzania; lista sieciowych urządzeń pamięci masowej, których używanie w systemach zewnętrznych jest zabronione; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-20(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zakaz używania sieciowych urządzeń pamięci masowej w systemach zewnętrznych; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-20(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zakazujące używania sieciowych urządzeń pamięci masowej w systemach zewnętrznych]. |

| | | |
|---|---|---|
| **AC-20(05)** | **KORZYSTANIE Z SYSTEMÓW ZEWNĘTRZNYCH \| PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE - ZAKAZ UŻYWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-20(05)** | korzystanie z kontrolowanych przez organizację przenośnych urządzeń pamięci masowej przez upoważnione osoby jest zabronione w systemach zewnętrznych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-20(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące wykorzystania przenośnych urządzeń pamięci masowej w systemach zewnętrznych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; umowy dotyczące podłączenia do systemu lub przetwarzania danych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-20(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zakaz używania przenośnych urządzeń pamięci masowej w systemach zewnętrznych; administratorzy systemu/sieci;<br>personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **AC-21** | **UDOSTĘPNIANIE INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-21_ODP[01]** | ***określono okoliczności związane z udostępnianiem informacji, w których wymagany jest dostęp uznaniowy, w celu ustalenia czy uprawnienia do dostępu przypisane partnerowi udostępniającemu informacje są zgodne z ograniczeniami dostępu i wykorzystania informacji;*** |

| | | |
|---|---|---|
| **AC-21** | **UDOSTĘPNIANIE INFORMACJI** | |
| | **AC-21_ODP[02]** | ***określono automatyczne mechanizmy lub ręczne procesy, które wspomagają użytkowników w podejmowaniu decyzji dotyczących dzielenia się informacjami i współpracy;*** |
| | **AC-21a.** | autoryzowani użytkownicy mają możliwość określenia czy uprawnienia dostępu przypisane do partnera udostępniającego informacje odpowiadają ograniczeniom dostępu i wykorzystania informacji dla ***<okoliczności związanych z udostępnianiem informacji AC-21_ODP[01]>***; |
| | **AC-21b.** | stosuje się ***<automatyczne mechanizmy AC-21_ODP[02]> w*** celu wspomagania użytkowników w podejmowaniu decyzji co do udostępniania informacji i współpracy. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-21-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące współpracy i udostępniania informacji przez użytkowników (w tym ograniczenia); dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista użytkowników upoważnionych do podejmowania decyzji o udostępnianiu informacji/współpracy; lista okoliczności związanych z udostępnianiem informacji, które wymagają weryfikacji użytkownika; umowy o zachowaniu poufności; umowy dotyczące nabywania/umowy; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; oceny ryzyka w zakresie bezpieczeństwa i prywatności; inne stosowne dokumenty lub zapisy]. |
| | **AC-21-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za decyzje dotyczące udostępniania informacji/współpracy; personel organizacyjny odpowiedzialny za zakupy/umowy; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **AC-21** | **UDOSTĘPNIANIE INFORMACJI** | |
| | **AC-21-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy lub ręczny proces wdrażający autoryzacje dostępu, wspierające decyzje o udostępnianiu informacji/ współpracy użytkowników]. |

| | | |
|---|---|---|
| **AC-21(01)** | **UDOSTĘPNIANIE INFORMACJI \| AUTOMATYCZNE WSPARCIE DECYZJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-21(01)_ODP** | ***określono automatyczne mechanizmy służące do egzekwowania decyzji o udostępnieniu informacji przez uprawnionych użytkowników;*** |
| | **AC-21(01)** | stosuje się ***<automatyczne mechanizmy AC-21(01)_ODP> w*** celu egzekwowania decyzji dotyczących udostępniania informacji przez upoważnionych użytkowników w oparciu o uprawnienia dostępu partnerów udostępniających informacje oraz ograniczenia dostępu do informacji, które mają być udostępnione. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-21(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące współpracy i udostępniania informacji przez użytkowników (w tym ograniczenia); dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista użytkowników upoważnionych do podejmowania decyzji o udostępnianiu informacji/współpracy; wygenerowana przez system lista partnerów udostępniających informacje oraz uprawnień dostępu; wygenerowana przez system lista ograniczeń dostępu dotyczących udostępnianych informacji; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| **AC-21(01)** | **UDOSTĘPNIANIE INFORMACJI \| AUTOMATYCZNE WSPARCIE DECYZJI** | |
|---|---|---|
| | **AC-21(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-21(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające autoryzacje dostępu, wspierające decyzje o udostępnianiu informacji/ współpracy użytkowników]. |

| **AC-21(02)** | **UDOSTĘPNIANIE INFORMACJI \| WYSZUKIWANIE I ODZYSKIWANIE INFORMACJI** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-21(02)_ODP** | ***określono ograniczenia dotyczące udostępniania informacji, które mają być egzekwowane przez usługi wyszukiwania i pozyskiwania informacji;*** |
| | **AC-21(02)** | Wdrożono usługi wyszukiwania i pozyskiwania informacji, które egzekwują stosowanie ***<ograniczeń w udostępnianiu informacji AC-21(02)_ODP>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-21(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące współpracy i udostępniania informacji przez użytkowników (w tym ograniczenia); dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista ograniczeń dostępu dotyczących udostępnianych informacji; zapisy dotyczące wyszukiwania i pozyskiwania informacji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AC-21(02)** | **UDOSTĘPNIANIE INFORMACJI \| WYSZUKIWANIE I ODZYSKIWANIE INFORMACJI** | |
| | **AC-21(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie zasad dostępu do usług wyszukiwania i wyszukiwania w systemie; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **AC-21(02)-Test** | [WYBÓR SPOŚRÓD: Systemowe usługi wyszukiwania i pozyskiwania informacji egzekwujące ograniczenia w udostępnianiu informacji]. |

| | | |
|---|---|---|
| **AC-22** | **TREŚCI PUBLICZNIE DOSTĘPNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-22_ODP** | ***określono częstotliwość, z jaką należy dokonywać przeglądu treści w publicznie dostępnym systemie pod kątem obecności informacji niepublicznych;*** |
| | **AC-22a.** | wyznaczone osoby są uprawnione do publicznego udostępniania informacji; |
| | **AC-22b.** | upoważnione osoby są przeszkolone tak, aby zapewnić, że publicznie dostępne informacje nie zawierają informacji niepublicznych; |
| | **AC-22c.** | proponowana treść informacji jest analizowana przed umieszczeniem jej w publicznie dostępnym systemie w celu zapewnienia, że nie zawiera ona informacji niepublicznych; |
| | **AC-22d.[01]** | zawartość publicznie dostępnego systemu jest sprawdzana pod kątem obecności informacji niepublicznych z***<częstotliwością AC-22_ODP>***; |
| | **AC-22d.[02]** | informacje niepubliczne są usuwane z publicznie dostępnego systemu, jeśli zostaną wykryte. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-22** | **TREŚCI PUBLICZNIE DOSTĘPNE** | |
| | **AC-22-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące publicznie dostępnych treści; lista użytkowników upoważnionych do zamieszczania publicznie dostępnych treści w systemach organizacji; materiały i lub protokoły ze szkoleń; zapisy z przeglądów publicznie dostępnych informacji; zapisy dot. reakcji na obecność niepublicznych informacji na publicznych stronach internetowych; logi z audytu systemu; protokoły ze szkoleń z zakresu bezpieczeństwa; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-22-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie publicznie dostępnymi informacjami zamieszczonymi w systemach organizacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-22-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zarządzanie publicznie dostępnymi treściami]. |

| | | |
|---|---|---|
| **AC-23** | **OCHRONA PRZED PRZESZUKIWANIEM DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-23_ODP[01]** | ***określono techniki zapobiegania i wykrywania przeszukiwania danych;*** |
| | **AC-23_ODP[02]** | ***określono obiekty przechowywania danych, które mają być chronione przed nieautoryzowanym przeszukiwaniem danych;*** |
| | **AC-23** | Stosowane są ***<techniki AC-23_ODP[01]>*** w odniesieniu do ***<obiektów przechowywania danych AC-23_ODP[02]>*** w celu wykrywania i ochrony przed nieautoryzowanym przeszukiwaniem danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AC-23** | **OCHRONA PRZED PRZESZUKIWANIEM DANYCH** | |
| | **AC-23-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury zapobiegania i wykrywania przeszukiwania danych; polityki i procedury dotyczące dozwolonych technik przeszukiwania danych; procedury dotyczące ochrony obiektów przechowywania danych przed przeszukiwaniem danych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; logi z audytu systemu; zapisy audytu systemu; procedury dotyczące technik prywatności różnicowej; powiadomienia o nietypowych zapytaniach lub dostępie do bazy danych; dokumentacja lub raporty z programu dot. zagrożeń wewnętrznych; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-23-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za wdrażanie technik wykrywania i zapobiegania przeszukiwaniu danych w obiektach przechowywania danych; radca prawny; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-23-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające techniki zapobiegania i wykrywania przeszukiwania danych]. |

| | | |
|---|---|---|
| **AC-24** | **PRZYZNAWANIE PRAW DOSTĘPU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-24_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {ustalenie procedur; wdrożenie mechanizmów};*** |
| | **AC-24_ODP[02]** | ***określono decyzje dot. przyznawania praw dostępu, stosowane w przypadku każdego żądania dostępu przed jego spełnieniem;*** |

| | | |
|---|---|---|
| **AC-24** | **PRZYZNAWANIE PRAW DOSTĘPU** | |
| | **AC-24** | stosuje się***<WYBRANĄ WARTOŚĆ PARAMETRU AC-24_ODP[01]> w*** celu zapewnienia, że<br>***<decyzje dot. przyznawania praw dostępu AC-24_ODP[02]>*** są stosowane w odniesieniu do każdego żądania dostępu przed jego spełnieniem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-24-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące decyzji w sprawie kontroli dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-24-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ustanowienie procedur dotyczących decyzji o kontroli dostępu do systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-24-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające ustalone decyzje i procedury przyznawania praw dostępu]. |

| | | |
|---|---|---|
| **AC-24(01)** | **PRZYZNAWANIE PRAW DOSTĘPU \| PRZESYŁANIE INFORMACJI O AUTORYZACJI DOSTĘPU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-24(01)_ODP[01]** | ***określono informacje o autoryzacji dostępu, przekazywane do systemów egzekwujących decyzje ws. przyznawania praw dostępu;*** |
| | **AC-24(01)_ODP[02]** | ***określono zabezpieczenia, które mają być stosowane, gdy informacje o autoryzacji są przekazywane do systemów egzekwujących decyzje w zakresie kontroli dostępu;*** |

| | | |
|---|---|---|
| **AC-24(01)** | **PRZYZNAWANIE PRAW DOSTĘPU \| PRZESYŁANIE INFORMACJI O AUTORYZACJI DOSTĘPU** | |
| | **AC-24(01)_ODP[03]** | ***określono systemy, które egzekwują decyzje w zakresie kontroli dostępu;*** |
| | **AC-24(01)** | ***<informacje o autoryzacji dostępu AC-24(01)_ODP[01]>*** przekazywane są przy użyciu ***<zabezpieczeń AC-24(01)_ODP[02]>*** do ***<systemów AC-24(01)_ODP[03]>***, które egzekwują decyzje dotyczące kontroli dostępu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-24(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-24(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-24(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania uprawnień dostępu]. |

| | | |
|---|---|---|
| **AC-24(02)** | **PRZYZNAWANIE PRAW DOSTĘPU \|BRAK TOŻSAMOŚCI UŻYTKOWNIKA LUB PROCESU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-24(02)_ODP[01]** | ***określono atrybuty bezpieczeństwa, które nie obejmują tożsamości użytkownika lub procesu działającego w imieniu użytkownika (jeśli wybrano);*** |

| | | |
|---|---|---|
| **AC-24(02)** | **PRZYZNAWANIE PRAW DOSTĘPU \|BRAK TOŻSAMOŚCI UŻYTKOWNIKA LUB PROCESU** | |
| | **AC-24(02)_ODP[02]** | ***określono atrybuty prywatności, które nie obejmują tożsamości użytkownika lub procesu działającego w imieniu użytkownika (jeśli wybrano);*** |
| | **AC-24(02)[01]** | Decyzje dot. kontroli dostępu są egzekwowane na podstawie ***<atrybutów bezpieczeństwa AC-24(02)_ODP[01]>***, które nie obejmują tożsamości użytkownika lub procesu działającego w imieniu użytkownika (jeśli wybrano); |
| | **AC-24(02)[02]** | decyzje dot. kontroli dostępu są egzekwowane na podstawie ***<atrybutów prywatności AC-24(02)_ODP[02]>***, które nie obejmują tożsamości użytkownika lub procesu działającego w imieniu użytkownika (jeśli wybrano); |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-24(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania zasad dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AC-24(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-24(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania uprawnień dostępu]. |

| | | |
|---|---|---|
| **AC-25** | **MONITOR REFERENCYJNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AC-25_ODP** | ***określono polityki kontroli dostępu, w odniesieniu do których stosuje się monitor referencyjny;*** |
| | **AC-25** | w odniesieniu do***<polityki kontroli dostępu AC-25_ODP>*** stosuje się monitor referencyjny, który jest odporny na manipulacje, zawsze wywoływany i na tyle niewielki, że można go poddać analizie i testom, co do których istnieje pewność, że są kompletne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AC-25-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące egzekwowania uprawnień dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zpisy]. |
| | **AC-25-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AC-25-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania uprawnień dostępu]. |

## 4.2. KATEGORIA AT - UŚWIADAMIANIE I SZKOLENIA

| | | |
|---|---|---|
| **AT-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-01_ODP[01]** | ***określono personel lub role, wśród których ma być rozpowszechniana polityka uświadamiania i szkolenia;*** |
| | **AT-01_ODP[02]** | ***określono personel lub role, wśród których mają być rozpowszechniane procedury uświadamiania i szkolenia;*** |
| | **AT-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **AT-01_ODP[04]** | ***określono pracownika funkcyjnego odpowiedzialnego za zarządzanie polityką i procedurami uświadamiania i szkolenia;*** |
| | **AT-01_ODP[05]** | ***określono częstotliwość, z jaką polityka uświadamiania i szkolenia jest przeglądana i aktualizowana;*** |
| | **AT-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji obowiązującej polityki uświadamiania i szkolenia;*** |
| | **AT-01_ODP[07]** | ***określono częstotliwość, z jaką aktualne procedury uświadamiania i szkolenia są przeglądane i aktualizowane;*** |
| | **AT-01_ODP[08]** | ***określono zdarzenia skutkujące koniecznością przeprowadzenia przeglądu i aktualizacji procedur;*** |
| | **AT-01a.[01]** | opracowano i udokumentowano politykę uświadamiania i szkolenia; |
| | **AT-01a.[02]** | polityka uświadamiania i szkolenia jest rozpowszechniana wśród ***<personelu lub ról AT-01_ODP[01]>***; |
| | **AT-01a.[03]** | opracowano i udokumentowano procedury uświadamiania i szkolenia ułatwiające wdrożenie polityki w tym zakresie oraz powiązanych zabezpieczeń dostępu; |

| AT-01 | POLITYKA I PROCEDURY | |
|---|---|---|
| | **AT-01a.[04]** | procedury uświadamiające i szkoleniowe są rozpowszechniane wśród ***<personelu lub ról AT-01_ODP[02]>***. |
| | **AT-01a.01(a)[01]** | polityka uświadamiania i szkolenia***<WYBRANA WARTOŚĆ PARAMETRU AT-01_ODP[03]>*** odnosi się do celu; |
| | **AT-01a.01(a)[02]** | polityka uświadamiania i szkolenia ***<WYBRANA WARTOŚĆ PARAMETRU AT-01_ODP[03]>*** odnosi się do zakresu; |
| | **AT-01a.01(a)[03]** | polityka uświadamiania i szkolenia ***<WYBRANA WARTOŚĆ PARAMETRU AT-01_ODP[03]>*** odnosi się do ról; |
| | **AT-01a.01(a)[04]** | polityka uświadamiania i szkolenia***<WYBRANA WARTOŚĆ PARAMETRU AT-01_ODP[03]>*** odnosi się do obowiązków; |
| | **AT-01a.01(a)[05]** | polityka uświadamiania i szkolenia ***<WYBRANA WARTOŚĆ PARAMETRU AT-01_ODP[03]>*** odnosi się do zobowiązań kierownictwa; |
| | **AT-01a.01(a)[06]** | polityka uświadamiania i szkolenia ***<WYBRANA WARTOŚĆ PARAMETRU AT-01_ODP[03]>*** odnosi się do koordynacji pomiędzy jednostkami organizacyjnymi; |
| | **AT-01a.01(a)[07]** | polityka uświadamiania i szkolenia ***<WYBRANA WARTOŚĆ PARAMETRU AT-01_ODP[03]>*** odnosi się do zgodności; oraz |
| | **AT-01a.01(b)** | polityka uświadamiania i szkolenia ***<WYBRANA WARTOŚĆ PARAMETRU AT-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; oraz |
| | **AT-01b.** | ***<urzędnik AT-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur uświadamiania i szkolenia; |
| | **AT-01c.01[01]** | przeglądu i aktualizacji polityki uświadamiania i szkolenia dokonuje się z ***<częstotliwością AT-01_ODP[05]>***; |

| | | |
|---|---|---|
| **AT-01** | **POLITYKA I PROCEDURY** | |
| | **AT-01c.01[02]** | przeglądu i aktualizacji polityki uświadamiania i szkolenia dokonuje się po ***<zdarzeniu AT-01_ODP[06]>***; |
| | **AT-01c.02[01]** | przeglądu i aktualizacji procedur uświadamiania i szkolenia dokonuje się z ***<częstotliwością AT-01_ODP[07]>***; |
| | **AT-01c.02[02]** | przeglądu i aktualizacji procedur uświadamiania i szkolenia dokonuje się po ***<zdarzeniu AT-01_ODP[08]>*.** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-01-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; plan ochrony prywatności; polityka i procedury dotyczące uświadamiania i szkoleń; inne istotne dokumenty lub zapisy]. |
| | **AT-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za uświadamianie i szkolenia; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **AT-02** | **SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-02_ODP[01]** | ***określono częstotliwość, z jaką należy przeprowadzać szkolenia z zakresu znajomości zasad bezpieczeństwa dla użytkowników systemu (w tym menedżerów, wyższej kadry kierowniczej i wykonawców) po przeprowadzeniu szkolenia wstępnego;*** |
| | **AT-02_ODP[02]** | ***określono częstotliwość, z jaką należy przeprowadzać szkolenia z zakresu ochrony prywatności dla użytkowników systemu (w tym kierowników, wyższej kadry kierowniczej i wykonawców) po przeprowadzeniu szkolenia wstępnego;*** |

| AT-02 | SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | |
|---|---|---|
| | **AT-02_ODP[03]** | ***określono zdarzenia, które wymagają szkolenia z zakresu bezpieczeństwa dla użytkowników systemu;*** |
| | **AT-02_ODP[04]** | ***określono zdarzenia, które wymagają szkolenia z zakresu ochrony prywatności dla użytkowników systemu;*** |
| | **AT-02_ODP[05]** | ***określono techniki, które należy zastosować, aby zwiększyć świadomość w zakresie bezpieczeństwa i ochrony prywatności wśród użytkowników systemu;*** |
| | **AT-02_ODP[06]** | ***określono częstotliwość, z jaką należy aktualizować treści szkoleniowe i uświadamiające w zakresie bezpieczeństwa i ochrony prywatności;*** |
| | **AT-02_ODP[07]** | ***określono zdarzenia wymagające aktualizacji treści szkoleniowe i uświadamiające w zakresie bezpieczeństwa i ochrony prywatności;*** |
| | **AT-02a.01[01]** | Szkolenie w zakresie znajomości zagadnień związanych z bezpieczeństwem jest zapewniane użytkownikom systemu (w tym kierownikom, członkom wyższej kadry kierowniczej i wykonawcom) w ramach wstępnego szkolenia dla nowych użytkowników; |
| | **AT-02a.01[02]** | W ramach wstępnego szkolenia dla nowych użytkowników przeprowadza się szkolenie dla użytkowników systemu (w tym kierowników, wyższej kadry kierowniczej i wykonawców) w zakresie ochrony prywatności; |
| | **AT-02a.01[03]** | Następnie szkolenie w zakresie znajomości zasad bezpieczeństwa jest prowadzone dla użytkowników systemu (w tym kierowników, wyższej kadry kierowniczej i wykonawców) z ***<częstotliwością AT-02_ODP[01]>***; |
| | **AT-02a.01[04]** | Następnie szkolenie w zakresie ochrony prywatności jest prowadzone dla użytkowników systemu (w tym kierowników, wyższej kadry kierowniczej i wykonawców) z ***<częstotliwością AT-02_ODP[02]>***; |

| | | |
|---|---|---|
| **AT-02** | **SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA** | |
| | **AT-02a.02[01]** | szkolenie w zakresie zasad bezpieczeństwa jest prowadzone dla użytkowników systemu (w tym kierowników, wyższej kadry kierowniczej i wykonawców), gdy wymagają tego zmiany w systemie lub wystąpiły ***<AT-02_ODP[03] zdarzenia>***; |
| | **AT-02a.02[02]** | szkolenie w zakresie ochrony prywatności jest prowadzone dla użytkowników systemu (w tym kierowników, wyższej kadry kierowniczej i wykonawców), gdy wymagają tego zmiany w systemie lub wystąpiły ***<zdarzenia AT-02_ODP[04]>***; |
| | **AT-02b.** | stosuje się ***<techniki uświadamiania AT-02_ODP[05]>*** w celu zwiększenia świadomości zasad bezpieczeństwa i ochrony prywatności wśród użytkowników systemu; |
| | **AT-02c.[01]** | Treści w zakresie szkolenia i uświadamiania są aktualizowane z ***<częstotliwością AT-02_ODP[06]>***; |
| | **AT-02c.[02]** | Treści w zakresie szkolenia i uświadamiania są aktualizowane po***<zdarzeniach AT-02_ODP[07]>***; |
| | **AT-02d.** | wnioski wyciągnięte z wewnętrznych lub zewnętrznych incydentów lub naruszeń bezpieczeństwa są włączane do technik szkolenia i uświadamiania w zakresie bezpieczeństwa i ochrony prywatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-02-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; plan ochrony prywatności; polityka szkolenia i uświadamiania; procedury dotyczące realizacji szkolenia i uświadamiania; odpowiednie przepisy; program szkolenia w zakresie bezpieczeństwa i ochrony prywatności; materiały szkoleniowe w zakresie bezpieczeństwa i ochrony prywatności; dokumentacja szkoleniowa; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AT-02** | **SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA** | |
| | **AT-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za szkolenie i uświadamianie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny składający się z ogólnej społeczności użytkowników systemu]. |
| | **AT-02-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zarządzania informacjami szkoleniami z zakresu bezpieczeństwa i ochrony prywatności]. |

| | | |
|---|---|---|
| **AT-02(01)** | **SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA \| ĆWICZENIA PRAKTYCZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-02(01)** | w ramach szkolenia i uświadamiania prowadzone są praktyczne ćwiczenia, które symulują zdarzenia i incydenty. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-02(01)-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; plan ochrony prywatności; polityka uświadamiania i szkolenia w zakresie bezpieczeństwa; procedury dotyczące realizacji szkolenia w zakresie uświadamiania bezpieczeństwa; program szkolenia w zakresie uświadamiania bezpieczeństwa; materiały szkoleniowe w zakresie uświadamiania bezpieczeństwa; inne istotne dokumenty lub zapisy]. |
| | **AT-02(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny przeszkolony i uświadomiony w zakresie zasad bezpieczeństwa i ochrony prywatności; personel organizacyjny odpowiedzialny za szkolenie w zakresie uświadamiania bezpieczeństwa; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **AT-02(01)** | **SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA \| ĆWICZENIA PRAKTYCZNE** | |
| | **AT-02(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy pozwalające na symulowanie cyberataków w ćwiczeniach praktycznych]. |

| | | |
|---|---|---|
| **AT-02(02)** | **SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA \| ZAGROŻENIA WEWNĘTRZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-02(02)[01]** | Prowadzone są szkolenia z zakresu rozpoznawania potencjalnych oznak zagrożeń wewnętrznych; |
| | **AT-02(02)[02]** | Prowadzone są szkolenia z zakresu zgłaszania potencjalnych oznak zagrożeń wewnętrznych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; plan ochrony prywatności; polityka szkolenia i uświadamiania w zakresie bezpieczeństwa; procedury dotyczące szkolenia i uświadamiania w zakresie bezpieczeństwa; program szkolenia i uświadamiania w zakresie bezpieczeństwa; materiały szkoleniowe i podnoszące świadomość w zakresie bezpieczeństwa; inne istotne dokumenty lub zapisy]. |
| | **AT-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny, który otrzymał szkolenie w zakresie bezpieczeństwa; personel organizacyjny odpowiedzialny za szkolenie i podnoszenie świadomości w zakresie bezpieczeństwa; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **AT-02(03)** | **SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA \| INŻYNIERIA SPOŁECZNA I POZYSKIWANIE DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-02(03)[01]** | Prowadzone są szkolenia z zakresu rozpoznawania potencjalnych i rzeczywistych przypadków socjotechniki; |
| | **AT-02(03)[02]** | Prowadzone są szkolenia z zakresu zgłaszania potencjalnych i rzeczywistych przypadków socjotechniki; |
| | **AT-02(03)[03]** | Prowadzone są szkolenia z zakresu rozpoznawania potencjalnych i rzeczywistych przypadków tzw. social mining; |
| | **AT-02(03)[04]** | Prowadzone są szkolenia z zakresu zgłaszania potencjalnych i rzeczywistych przypadków tzw. social mining; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-02(03)-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; plan ochrony prywatności; polityka szkolenia i uświadamiania w zakresie bezpieczeństwa; procedury dotyczące szkolenia i uświadamiania w zakresie bezpieczeństwa; program szkolenia i uświadamiania w zakresie bezpieczeństwa; materiały szkoleniowe i podnoszące świadomość w zakresie bezpieczeństwa; inne istotne dokumenty lub zapisy]. |
| | **AT-02(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny, który otrzymał szkolenie w zakresie bezpieczeństwa; personel organizacyjny odpowiedzialny za szkolenie i podnoszenie świadomości w zakresie bezpieczeństwa; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **AT-02(04)** | **SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA \| PODEJRZANA TRANSMISJA I ANOMALIE ZACHOWANIA SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-02(04)_ODP** | ***określono oznaki wskazujące na obecność złośliwego kodu;*** |
| | **AT-02(04)** | Prowadzone jest szkolenie z zakresu rozpoznawania podejrzanej komunikacji i anomalii w działaniu systemów organizacji z wykorzystaniem ***<oznak obecności złośliwego kodu AT-02(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-02(04)-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; plan ochrony prywatności; polityka szkolenia i uświadamiania w zakresie bezpieczeństwa; procedury dotyczące szkolenia i uświadamiania w zakresie bezpieczeństwa; program szkolenia i uświadamiania w zakresie bezpieczeństwa; materiały szkoleniowe i podnoszące świadomość w zakresie bezpieczeństwa; inne istotne dokumenty lub zapisy]. |
| | **AT-02(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny, który otrzymał szkolenie w zakresie bezpieczeństwa; personel organizacyjny odpowiedzialny za podstawowe szkolenie i podnoszenie świadomości w zakresie bezpieczeństwa; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **AT-02(05)** | **SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA \| ZAAWANSOWANE TRWAŁE ZAGROŻENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-02(05)** | Prowadzone są szkolenia dotyczące zaawansowanych, trwałych zagrożeń (APT). |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-02(05)-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; plan ochrony prywatności; polityka szkolenia i uświadamiania w zakresie bezpieczeństwa; procedury dotyczące szkolenia i uświadamiania w zakresie bezpieczeństwa; program szkolenia i uświadamiania w zakresie bezpieczeństwa; materiały szkoleniowe i podnoszące świadomość w zakresie bezpieczeństwa; inne istotne dokumenty lub zapisy]. |
| | **AT-02(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny, który otrzymał szkolenie w zakresie bezpieczeństwa; personel organizacyjny odpowiedzialny za podstawowe szkolenie i podnoszenie świadomości w zakresie bezpieczeństwa; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **AT-02(06)** | **SZKOLENIA W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA \| ŚRODOWISKA CYBERZAGROŻEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-02(06)(a)** | Prowadzone są szkolenia dotyczące środowiska zagrożeń cybernetycznych; |

| | | |
|---|---|---|
| **AT-02(06)** | **SZKOLENIA W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA \| ŚRODOWISKA CYBERZAGROŻEŃ** | |
| | **AT-02(06)(b)** | operacje systemowe są dostosowane do aktualnych informacji o cyberzagrożeniach. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-02(06)-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; plan ochrony prywatności; polityka w zakresie szkolenia i uświadamiania; procedury dotyczące szkolenia i uświadamiania; program szkolenia i uświadamiania; materiały dot. szkolenia i uświadamiania; inne istotne dokumenty lub zapisy]. |
| | **AT-02(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny, który otrzymał szkolenie w zakresie bezpieczeństwa; personel organizacyjny odpowiedzialny za podstawowe szkolenie i podnoszenie świadomości w zakresie bezpieczeństwa; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **AT-03** | **SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-03_ODP[01]** | ***określono role i obowiązki dotyczące szkoleń w zakresie bezpieczeństwa opartego na rolach;*** |
| | **AT-03_ODP[02]** | ***określono role i obowiązki dotyczące szkoleń w zakresie prywatności opartej na rolach;*** |
| | **AT-03_ODP[03]** | ***określono częstotliwość, z jaką należy przeprowadzać szkolenia w zakresie bezpieczeństwa i prywatności w oparciu o role dla wyznaczonego personelu po wstępnym szkoleniu;*** |

| AT-03 | SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | |
|---|---|---|
| | **AT-03_ODP[04]** | ***określono częstotliwość, z jaką należy aktualizować treści do realizacji szkoleń w oparciu o role;*** |
| | **AT-03_ODP[05]** | ***określono zdarzenia, które wymagają aktualizacji treści do realizacji szkoleń w oparciu o role;*** |
| | **AT-03a.01[01]** | Szkolenie w zakresie bezpieczeństwa w oparciu o role jest przeprowadzane w przypadku ***<ról i obowiązków AT-03_ODP[01]>*** przed zatwierdzeniem dostępu do systemu lub informacji bądź podjęciem przydzielonych obowiązków; |
| | **AT-03a.01[02]** | Szkolenie w zakresie ochrony prywatności w oparciu o role jest przeprowadzane w przypadku ***<ról i obowiązków AT-03_ODP[02]>*** przed zatwierdzeniem dostępu do systemu lub informacji bądź podjęciem przydzielonych obowiązków; |
| | **AT-03a.01[03]** | Następnie szkolenie w zakresie bezpieczeństwa w oparciu o role jest przeprowadzane w przypadku ***<ról i obowiązków AT-03_ODP[01]> z <częstotliwością AT-03_ODP[03]>;*** |
| | **AT-03a.01[04]** | Następnie szkolenie w zakresie ochrony prywatności w oparciu o role jest przeprowadzane w przypadku ***<ról i obowiązków AT-03_ODP[02]> z <częstotliwością AT-03_ODP[03]>;*** |
| | **AT-03a.02[01]** | jeśli wymagają tego zmiany w systemie, przeprowadza się szkolenie w zakresie bezpieczeństwa w oparciu o role dla personelu z przypisanymi rolami i obowiązkami w obszarze bezpieczeństwa; |
| | **AT-03a.02[02]** | jeśli wymagają tego zmiany w systemie, przeprowadza się szkolenie w zakresie ochrony prywatności w oparciu o role dla personelu z przypisanymi rolami i obowiązkami w obszarze bezpieczeństwa; |
| | **AT-03b.[01]** | treści do realizacji szkoleń w oparciu o role są aktualizowane z ***<częstotliwością AT-03_ODP[04]>***; |

| | | |
|---|---|---|
| **AT-03** | **SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH** | |
| | **AT-03b.[02]** | treści do realizacji szkoleń w oparciu o role są aktualizowane po***<zdarzeniach AT-03_ODP[05]>***; |
| | **AT-03c.** | wnioski wyciągnięte z wewnętrznych i zewnętrznych incydentów lub naruszeń bezpieczeństwa są włączane do szkoleń opartych na rolach. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-03-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; plan ochrony prywatności; polityka uświadamiania i szkolenia w zakresie bezpieczeństwa i prywatności; procedury dotyczące szkolenia w zakresie bezpieczeństwa i prywatności; program szkolenia w zakresie bezpieczeństwa i prywatności; odpowiednie przepisy; materiały szkoleniowe w zakresie bezpieczeństwa i prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja szkoleniowa; inne istotne dokumenty lub zapisy]. |
| | **AT-03-Wywiad** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; plan ochrony prywatności; polityka uświadamiania i szkolenia w zakresie bezpieczeństwa i prywatności; procedury dotyczące realizacji szkolenia w zakresie bezpieczeństwa i prywatności; odpowiednie przepisy; program szkolenia w zakresie bezpieczeństwa i prywatności; materiały szkoleniowe w zakresie bezpieczeństwa i prywatności; dokumentacja szkoleniowa; inne istotne dokumenty lub zapisy]. |
| | **AT-03-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zarządzające szkoleniami z zakresu bezpieczeństwa i prywatności w oparciu o role]. |

| | | |
|---|---|---|
| **AT-03(01)** | **SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH \| ZABEZPIECZENIA ŚRODOWISKOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-03(01)_ODP[01]** | ***określono personel lub role, którym należy zapewnić szkolenie wstępne i utrwalające w zakresie stosowania zabezpieczeń środowiskowych;*** |
| | **AT-03(01)_ODP[02]** | ***określono częstotliwość, z jaką należy przeprowadzać szkolenia utrwalające w zakresie stosowania zabezpieczeń środowiskowych;*** |
| | **AT-03(01)** | ***<personel lub role AT-03(01)_ODP[01]>*** mają zapewnione szkolenia wstępne i utrwalające, realizowane z ***<częstotliwością AT-03(01)_ODP[02]>***, ***w*** zakresie stosowania zabezpieczeń środowiskowych; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka uświadamiania i szkolenia w zakresie bezpieczeństwa i prywatności; procedury dotyczące szkolenia w zakresie bezpieczeństwa i prywatności; program szkolenia w zakresie bezpieczeństwa i prywatności; materiały szkoleniowe w zakresie bezpieczeństwa i prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja szkoleniowa; inne istotne dokumenty lub zapisy]. |
| | **AT-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za szkolenie w zakresie bezpieczeństwa i prywatności w oparciu o role; personel organizacyjny odpowiedzialny za stosowanie zabezpieczeń środowiskowych]. |

| | | |
|---|---|---|
| **AT-03(02)** | **SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH \| ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-03(02)_ODP[01]** | ***określono personel lub role, którym należy zapewnić szkolenie wstępne i utrwalające w zakresie stosowania fizycznych zabezpieczeń;*** |
| | **AT-03(02)_ODP[02]** | ***określono personel lub role, którym należy zapewnić szkolenie utrwalające w zakresie stosowania fizycznych zabezpieczeń;*** |
| | **AT-03(02)** | ***<personel lub role AT-03(02)_ODP[01]>*** mają zapewnione szkolenia wstępne i utrwalające, realizowane z ***<częstotliwością AT-03(02)_ODP[02]>***, ***w*** zakresie stosowania zabezpieczeń fizycznych; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka uświadamiania i szkolenia w zakresie bezpieczeństwa i prywatności; procedury dotyczące szkolenia w zakresie bezpieczeństwa i prywatności; program szkolenia w zakresie bezpieczeństwa i prywatności; materiały szkoleniowe w zakresie bezpieczeństwa i prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja szkoleniowa; inne istotne dokumenty lub zapisy]. |
| | **AT-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za szkolenie w zakresie bezpieczeństwa i prywatności w oparciu o role; personel organizacyjny odpowiedzialny za stosowanie zabezpieczeń fizycznych]. |

| | | |
|---|---|---|
| **AT-03(03)** | **SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH \| ĆWICZENIA PRAKTYCZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-03(03)[01]** | w ramach szkolenia z zakresu bezpieczeństwa zapewnione są praktyczne ćwiczenia, które wzmacniają efekty szkolenia; |
| | **AT-03(03)[02]** | w ramach szkolenia z zakresu ochrony prywatności zapewnione są praktyczne ćwiczenia, które wzmacniają efekty szkolenia; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka uświadamiania i szkolenia w zakresie bezpieczeństwa i prywatności; procedury dotyczące szkolenia w zakresie bezpieczeństwa i prywatności; program szkolenia w zakresie bezpieczeństwa i prywatności; materiały szkoleniowe w zakresie bezpieczeństwa i prywatności; raporty i wyniki szkolenia w zakresie świadomości bezpieczeństwa i prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AT-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za szkolenie w zakresie bezpieczeństwa opartego na rolach; personel organizacyjny uczestniczący w szkoleniach z zakresu uświadamiania bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **AT-03(04)** | **SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH \| PODEJRZANA TRANSMISJA I ANOMALIE ZACHOWANIA SYSTEMU** | |
| | [WYCOFANE: Włączone do AT-02(04)]. | |

| | | |
|---|---|---|
| **AT-03(05)** | **SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH \| PRZETWARZANIE DANYCH OSOBOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-03(05)_ODP[01]** | ***określono personel lub role, którym należy zapewnić szkolenie wstępne i utrwalające w zakresie przetwarzania danych identyfikacyjnych oraz zabezpieczeń dot. przejrzystości;*** |
| | **AT-03(05)_ODP[02]** | ***określono personel lub role, którym należy zapewnić szkolenie utrwalające w zakresie przetwarzania danych identyfikacyjnych oraz zabezpieczeń dot. przejrzystości;*** |
| | **AT-03(05)** | ***<personel lub role AT-03(05)_ODP[01]>*** mają zapewnione szkolenia wstępne i utrwalające, realizowane z ***<częstotliwością AT-03(05)_ODP[02]>***, ***w*** zakresie przetwarzania danych identyfikacyjnych oraz zabezpieczeń dot. przejrzystości. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-03(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka uświadamiania i szkolenia w zakresie bezpieczeństwa i prywatności; procedury dotyczące szkolenia w zakresie bezpieczeństwa i prywatności; program szkolenia w zakresie bezpieczeństwa i prywatności; materiały szkoleniowe w zakresie bezpieczeństwa i prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; organizacyjne zawiadomienia o ochronie prywatności;<br>polityki organizacji; zawiadomienia dot. systemu rejestrów; oświadczenia zgodne z amerykańską ustawą o prywatności; umowy i zawiadomienia o dopasowaniu zapisów komputerowych; oceny wpływu na prywatność; umowy o wymianie informacji; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AT-03(05)** | **SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH \| PRZETWARZANIE DANYCH OSOBOWYCH** | |
| | **AT-03(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za szkolenie w zakresie bezpieczeństwa opartego na rolach; personel organizacyjny uczestniczący w szkoleniach z zakresu uświadamiania bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **AT-04** | **DOKUMENTACJA SZKOLENIOWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-04_ODP** | ***określono czas przechowywania indywidualnej dokumentacji szkoleniowej;*** |
| | **AT-04a.[01]** | dokumentuje się działania szkoleniowe w zakresie bezpieczeństwa i ochrony prywatności informacji, w tym szkolenia dotyczące świadomości w zakresie bezpieczeństwa i ochrony prywatności oraz szkolenia w zakresie bezpieczeństwa i ochrony prywatności w oparciu o role; |
| | **AT-04a.[02]** | monitorowane są działania szkoleniowe w zakresie bezpieczeństwa i ochrony prywatności informacji, w tym świadomości zasad bezpieczeństwa i ochrony prywatności oraz szkolenia w zakresie bezpieczeństwa i ochrony prywatności w oparciu o role; |
| | **AT-04b.** | indywidualna dokumentacja szkoleniowa jest przechowywana przez ***<okres AT-04_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AT-04** | **DOKUMENTACJA SZKOLENIOWA** | |
| | **AT-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka uświadamiania i szkolenia w zakresie bezpieczeństwa i prywatności; procedury dotyczące uświadamiania i szkolenia w zakresie bezpieczeństwa i prywatności; dokumentacja dotycząca uświadamiania i szkolenia w zakresie bezpieczeństwa i prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AT-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przechowywanie dokumentacji dot. szkoleń w zakresie bezpieczeństwa i prywatności informacji]. |
| | **AT-04-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające zarządzanie dokumentacją dot. szkoleń z zakresu bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **AT-05** | **UTRZYMYWANIE KONTAKTÓW Z ZESPOŁAMI I STOWARZYSZENIAMI SPECJALIZUJĄCYMI SIĘ W CYBERBEZPIECZEŃSTWIE** | |
| | [WYCOFANE: Włączone do PM-15]. | |

| | | |
|---|---|---|
| **AT-06** | **INFORMACJE ZWROTNE O SZKOLENIACH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AT-06_ODP[01]** | ***określono częstotliwość przekazywania informacji zwrotnej o wynikach szkolenia prowadzonego przez organizację;*** |
| | **AT-06_ODP[02]** | ***wyznaczono personel, któremu zostanie przekazana informacja zwrotna o wynikach szkolenia prowadzonego przez organizację;*** |

| | | |
|---|---|---|
| **AT-06** | **INFORMACJE ZWROTNE O SZKOLENIACH** | |
| | **AT-06** | informacje zwrotne na temat wyników szkolenia prowadzonego przez organizację przekazywane są z ***<częstotliwością AT-06_ODP[01]>*** do ***<pracowników AT-06_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AT-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka uświadamiania i szkolenia w zakresie bezpieczeństwa; procedury dotyczące dokumentacji dot. szkoleń w zakresie bezpieczeństwa; dokumentacja dotycząca uświadamiania i szkolenia w zakresie bezpieczeństwa; plan bezpieczeństwa; inne istotne dokumenty lub zapisy]. |
| | **AT-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przechowywanie dokumentacji dot. szkoleń w zakresie bezpieczeństwa i prywatności informacji]. |
| | **AT-06-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające zarządzanie dokumentacją dot. szkoleń w zakresie bezpieczeństwa]. |

## 4.3. KATEGORIA AU - AUDYT I ROZLICZALNOŚĆ

| | | |
|---|---|---|
| **AU-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-01_ODP[01]** | ***określono personel lub role, wśród których ma być rozpowszechniana polityka audytu i rozliczalności;*** |
| | **AU-01_ODP[02]** | ***określono personel lub role, którym należy przekazać procedury dot. audytu i rozliczalności;*** |
| | **AU-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **AU-01_ODP[04]** | ***określono pracownika funkcyjnego, któremu powierzono zarządzanie polityką i procedurami dot. audytu i rozliczalności;*** |
| | **AU-01_ODP[05]** | ***określono częstotliwość przeglądu i aktualizacji polityki audytu i rozliczalności;*** |
| | **AU-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji polityki audytu i rozliczalności;*** |
| | **AU-01_ODP[07]** | ***określono częstotliwość przeglądu i aktualizacji procedur dot. audytu i rozliczalności;*** |
| | **AU-01_ODP[08]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji procedur dot. audytu i rozliczalności;*** |
| | **AU-01a.[01]** | opracowano i udokumentowano politykę audytu i rozliczalności; |
| | **AU-01a.[02]** | polityka audytu i rozliczalności jest rozpowszechniana wśród ***<personelu lub ról AU-01_ODP[01]>***; |
| | **AU-01a.[03]** | opracowano i udokumentowano procedury audytu i rozliczalności ułatwiające wdrożenie polityki audytu i rozliczalności oraz powiązanych zabezpieczeń w tym zakresie; |

| AU-01 | POLITYKA I PROCEDURY | |
|---|---|---|
| | **AU-01a.[04]** | procedury audytu i rozliczalności są rozpowszechniane wśród ***<personelu lub ról AU-01_ODP[02]>***; |
| | **AU-01a.01(a)[01]** | ***<WYBRANA WARTOŚĆ PARAMETRU AU-01_ODP[03]>*** polityki audytu i rozliczalności odnosi się do celu; |
| | **AU-01a.01(a)[02]** | ***<WYBRANA WARTOŚĆ PARAMETRU AU-01_ODP[03]>*** polityki audytu i rozliczalności odnosi się do zakresu; |
| | **AU-01a.01(a)[03]** | ***<WYBRANA WARTOŚĆ PARAMETRU AU-01_ODP[03]>*** polityki audytu i rozliczalności odnosi się do ról; |
| | **AU-01a.01(a)[04]** | ***<WYBRANA WARTOŚĆ PARAMETRU AU-01_ODP[03]>*** polityki audytu i rozliczalności odnosi się do zakresu obowiązków; |
| | **AU-01a.01(a)[05]** | ***<WYBRANA WARTOŚĆ PARAMETRU AU-01_ODP[03]>*** polityki audytu i rozliczalności odnosi się do zobowiązań kierownictwa; |
| | **AU-01a.01(a)[06]** | ***<WYBRANA WARTOŚĆ PARAMETRU AU-01_ODP[03]>*** polityki audytu i rozliczalności odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **AU-01a.01(a)[07]** | ***<WYBRANA WARTOŚĆ PARAMETRU AU-01_ODP[03]>*** polityki audytu i rozliczalności odnosi się do zgodności; |
| | **AU-01a.01(b)** | polityka audytu i rozliczalności ***<WYBRANA WARTOŚĆ PARAMETRU AU-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; oraz |
| | **AU-01b.** | ***<urzędnik AU-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur w zakresie audytu i rozliczalności; |
| | **AU-01c.01[01]** | przegląd i aktualizacja polityki audytu i rozliczalności odbywa się z ***<częstotliwością AU-01_ODP[05]>***; |

| | | |
|---|---|---|
| **AU-01** | **POLITYKA I PROCEDURY** | |
| | **AU-01c.01[02]** | przegląd i aktualizacja polityki audytu i rozliczalności odbywa się po ***<zdarzeniu AU-01_ODP[06]>***; |
| | **AU-01c.02[01]** | przegląd i aktualizacja procedur audytu i rozliczalności odbywa się z ***<częstotliwością AU-01_ODP[07]>***; |
| | **AU-01c.02[02]** | przegląd i aktualizacja procedur audytu i rozliczalności odbywa się po ***<zdarzeniach AU-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AU-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt i rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **AU-02** | **AUDYT ZDARZEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-02_ODP[01]** | ***określono typy zdarzeń, które system może rejestrować w celu wsparcia funkcji audytu;*** |
| | **AU-02_ODP[02]** | ***określono typy zdarzeń (podzbiór AU-02_ODP[01]) podlegających rejestrowaniu w systemie;*** |
| | **AU-02_ODP[03]** | ***w przypadku każdego typu zdarzenia określono częstotliwość rejestrowania lub sytuację jego wymagającą;*** |

| | | |
|---|---|---|
| **AU-02** | **AUDYT ZDARZEŃ** | |
| | **AU-02_ODP[04]** | ***dokonuje się przeglądu i aktualizacji częstotliwości występowania typów zdarzeń podlegających rejestrowaniu;*** |
| | **AU-02a.** | określono ***<typy zdarzeń <AU-02_ODP[01]>***, które system może rejestrować, w celu wsparcia funkcji rejestrowania na potrzeby audytu; |
| | **AU-02b.** | funkcja rejestrowania zdarzeń jest skoordynowana z innymi jednostkami organizacyjnymi wymagającymi informacji związanych z audytem, aby informować o kryteriach wyboru zdarzeń podlegających rejestrowaniu; |
| | **AU-02c.[01]** | określono ***<typy zdarzeń -02_ODP[02] (podzbiór AU-02_ODP[01])>*** podlegających rejestrowaniu w systemie; |
| | **AU-02c.[02]** | określone typy zdarzeń są rejestrowane w systemie z***<częstotliwością lub w sytuacji AU-02_ODP[03]>***; |
| | **AU-02d.** | przedstawiono uzasadnienie, dlaczego rodzaje zdarzeń podlegające rejestracji są odpowiednie do wspierania procesu realizacji badań incydentów po fakcie; |
| | **AU-02e.** | typy zdarzeń podlegające rejestracji są przeglądane i aktualizowane z ***<częstotliwością AU-02_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące zdarzeń podlegających audytowi; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; zdarzenia objęte audytem systemu; inne istotne dokumenty lub zapisy]. |

| **AU-02** | **AUDYT ZDARZEŃ** | |
|---|---|---|
| | **AU-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci]. |
| | **AU-02-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające system audytowania]. |

| **AU-02(01)** | **AUDYT ZDARZEŃ \| KOMPILACJA ZAPISÓW AUDYTU Z WIELU ŹRÓDEŁ** |
|---|---|
| | [WYCOFANE: Włączone do AU-12]. |

| **AU-02(02)** | **AUDYT ZDARZEŃ \| WYBÓR ZDARZEŃ AUDYTOWYCH WEDŁUG KOMPONENTÓW** |
|---|---|
| | [WYCOFANE: Włączone do AU-12]. |

| **AU-02(03)** | **AUDYT ZDARZEŃ \| OPINIE I AKTUALIZACJE** |
|---|---|
| | [WYCOFANE: Włączone do AU-02]. |

| **AU-02(04)** | **AUDYT ZDARZEŃ \| UPRZYWILEJOWANE FUNKCJE** |
|---|---|
| | [WYCOFANE: Włączone do AC-06(09)]. |

| | | |
|---|---|---|
| **AU-03** | **ZAWARTOŚĆ ZAPISÓW Z AUDYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-03a.** | zapisy z audytu zawierają informacje, które pozwalają ustalić, jaki rodzaj zdarzenia miał miejsce; |
| | **AU-03b.** | zapisy z audytu zawierają informacje, które ustalają, kiedy zdarzenie miało miejsce; |
| | **AU-03c.** | zapisy z audytu zawierają informacje, które pozwalają ustalić, gdzie doszło do zdarzenia; |
| | **AU-03d.** | zapisy z audytu zawierają informacje, które pozwalają ustalić przyczynę zdarzenia; |
| | **AU-03e.** | zapisy z audytu zawierają informacje, które pozwalają ustalić rezultat zdarzenia; |
| | **AU-03f.** | zapisy z audytu zawierają informacje, które pozwalają ustalić tożsamość wszelkich osób, lub przedmiotów/podmiotów związanych z danym zdarzeniem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące zawartości zapisów z audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista zdefiniowanych przez organizację zdarzeń podlegających audytowi; zapisy z audytu systemu; raporty o incydentach w systemie; inne istotne dokumenty lub zapisy]. |
| | **AU-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci]. |

| | | |
|---|---|---|
| **AU-03** | **ZAWARTOŚĆ ZAPISÓW Z AUDYTU** | |
| | **AU-03-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające system audytowania zdarzeń podlegających kontroli]. |

| | | |
|---|---|---|
| **AU-03(01)** | **ZAWARTOŚĆ REJESTRÓW AUDYTU \| DODATKOWE INFORMACJE KONTROLNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-03(01)_ODP** | ***określono dodatkowe informacje, które powinny być zawarte w zapisach z audytu;*** |
| | **AU-03(01)** | wygenerowane zapisy z audytu zawierają następujące ***<dodatkowe informacje AU-03(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące zawartości zapisów z audytu; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista zdefiniowanych przez organizację zdarzeń podlegających audytowi; zapisy audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-03(01)-Test** | [WYBÓR SPOŚRÓD: możliwości w zakresie audytu systemu]. |

| | |
|---|---|
| **AU-03(02)** | **ZAWARTOŚĆ REJESTRÓW AUDYTU \| CENTRALNE ZARZĄDZANIE TREŚCIĄ PLANOWANEGO REJESTRU AUDYTU** |
| | [WYCOFANE: Włączone do PL-09]. |

| | | |
|---|---|---|
| **AU-03(03)** | **ZAWARTOŚĆ REJESTRÓW AUDYTU \| OGRANICZENIE INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSÓB** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-03(03)_ODP** | ***definiowane są elementy zidentyfikowane w ocenie ryzyka dla prywatności;*** |
| | **AU-03(03)** | dane identyfikacyjne osób zawarte w dokumentacji audytowej są ograniczone do<br>***<elementów AU-03(03)_ODP>*** określonych w ocenie ryzyka dla prywatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena ryzyka dla prywatności; wyniki oceny ryzyka dla prywatności; procedury dotyczące zawartości zapisów z audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista zdefiniowanych przez organizację zdarzeń podlegających audytowi; zapisy z audytu systemu; umowy ze stronami trzecimi; inne istotne dokumenty lub zapisy]. |
| | **AU-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-03(03)-Test** | [WYBÓR SPOŚRÓD: możliwości w zakresie audytu systemu]. |

| | | |
|---|---|---|
| **AU-04** | **POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-04_ODP** | ***określono wymagania dotyczące przechowywania danych w dzienniku audytu;*** |
| | **AU-04** | Pamięć dla dziennika audytu jest przydzielana tak, by spełnić ***<wymagania dotyczące przechowywania danych w dzienniku audytu AU-04_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące zdolności przechowywania audytu; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wymagania dotyczące przechowywania zapisów z audytu; zdolność do przechowywania zapisów z audytu w komponentach systemu; zapisy z audytu systemu; inne stosowne dokumenty lub zapisy]. |
| | **AU-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-04-Test** | [WYBÓR SPOŚRÓD: Pamięć przeznaczona na zapisy z audytu i związane z nią ustawienia konfiguracyjne]. |

| | | |
|---|---|---|
| **AU-04(01)** | **POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU \| TRANSFER REKORDÓW DO ALTERNATYWNYCH URZĄDZEŃ MAGAZYNUJĄCYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-04(01)_ODP** | ***określono częstotliwość przekazywania dzienników audytowych do innego systemu, komponentu systemu lub na inny nośnik niż system lub komponent systemu prowadzący rejestrację;*** |
| | **AU-04(01)** | dzienniki audytu są przenoszone do innego systemu, komponentu systemu lub na inny nośnik niż system lub komponent systemu prowadzący rejestrację z ***<częstotliwością AU-04(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące pamięci na potrzeby audytu; procedury dotyczące transferu zapisów z audytu systemu do systemów wtórnych lub alternatywnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dzienniki transferu zapisów z audytu do systemów drugorzędnych lub zapasowych; zapisy z audytu systemu przeniesione do systemów drugorzędnych lub zapasowych;<br>dokumentacja z audytu systemu przeniesiona do systemów wtórnych lub alternatywnych; inne stosowne dokumenty lub zapisy]. |
| | **AU-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zapewnienie pamięci niezbędnej do celów audytu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci]. |
| | **AU-04(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające przenoszenie zapisów z audytu do innego systemu]. |

| | | |
|---|---|---|
| **AU-05** | **REAKCJA NA BŁĘDY PROCESÓW AUDYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-05_ODP[01]** | ***określono osoby lub role otrzymujące alerty o błędzie procesu audytu;*** |
| | **AU-05_ODP[02]** | ***określono okres na otrzymanie przez personel lub role alertów o błędzie procesu audytu;*** |
| | **AU-05_ODP[03]** | ***określono dodatkowe działania, które należy podjąć w przypadku błędu procesu audytu;*** |
| | **AU-05a.** | w przypadku błędu procesu audytu ***<personel lub role AU-05_ODP[01]>*** są powiadamiane w ciągu ***<okresu AU-05_ODP[02]>***; |
| | **AU-05b.** | w przypadku błędu procesu audytu podejmowane są ***<dodatkowe działania AU-05_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie audytu i rozliczalności; procedury dotyczące reakcji na błędy w procesie audytu; dokumentacja projektowa systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>lista pracowników, których należy powiadomić w przypadku błędów w procesie audytu; zapisy dotyczące audytu; inne właściwe dokumenty lub zapisy]. |
| | **AU-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt i rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-05-Test** | [WYBÓR SPOŚRÓD: Mechanizmy odpowiedzialne za reakcję systemu na błędy procesu audytu]. |

| | | |
|---|---|---|
| **AU-05(01)** | **REAKCJA NA BŁĘDY PROCESÓW AUDYTU \|OSTRZEŻENIA DOTYCZĄCE LIMITU PAMIĘCI PRZECHOWYWANIA REKORDÓW AUDYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-05(01)_ODP[01]** | ***określono personel, role lub lokalizacje, które należy powiadomić, gdy przydzielony dla dziennika audytu wolumen pamięci osiągnie wyznaczony procent maksymalnej pojemności repozytorium dziennika audytu.*** |
| | **AU-05(01)_ODP[02]** | ***określono okres, w którym personel, role lub lokalizacje są powiadamiane, gdy przydzielony dla dziennika audytu wolumen pamięci osiągnie wyznaczony procent maksymalnej pojemności repozytorium dziennika audytu.*** |
| | **AU-05(01)_ODP[03]** | ***określono procentową wartość maksymalnej pojemności repozytorium dziennika audytu.*** |
| | **AU-05(01)** | ostrzeżenie jest przekazywane do ***<personelu, ról lub lokalizacji AU-05(01)_ODP[01]> w*** ciągu ***<okresu AU-05(01)_ODP[02]>***, jeżeli przydzielony dla dziennika audytu wolumen pamięci osiągnie ***<procent AU-05(01)_ODP[03]>*** maksymalnej pojemności repozytorium dziennika audytu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-05(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie audytu i rozliczalności; procedury dotyczące reakcji na błędy w procesie audytu; dokumentacja projektowa systemu; plan bezpieczeństwa systemu; ustawienia konfiguracyjne systemu ochrony prywatności i związana z nimi dokumentacja; zapisy z audytu systemu; inne stosowne dokumenty lub zapisy]. |
| | **AU-05(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |

| | | |
|---|---|---|
| **AU-05(01)** | **REAKCJA NA BŁĘDY PROCESÓW AUDYTU \|OSTRZEŻENIA DOTYCZĄCE LIMITU PAMIĘCI PRZECHOWYWANIA REKORDÓW AUDYTU** | |
| | **AU-05(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy ostrzegające o limitach dot. przechowywania zapisów z audytu]. |

| | | |
|---|---|---|
| **AU-05(02)** | **REAKCJA NA BŁĘDY PROCESÓW AUDYTU \| ALERTY CZASU RZECZYWISTEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-05(02)_ODP[01]** | ***Określono okres rzeczywistego, po którym wymagany jest alarm w przypadku wystąpienia błędów w procesie audytu (definiowanych w AU-05(02)_ODP[03]);*** |
| | **AU-05(02)_ODP[02]** | ***określono personel, role lub lokalizacje, które mają być ostrzegane w czasie rzeczywistym w przypadku wystąpienia błędów w procesie audytu (określonych w AU-05(02)_ODP[03]);*** |
| | **AU-05(02)_ODP[03]** | ***określono błędy w procesie audytu wymagające alertów w czasie rzeczywistym;*** |
| | **AU-05(02)** | alert przekazywany jest w ciągu ***<okresu rzeczywistego AU-05(02)_ODP[01]>***<br>do ***<personelu, ról lub lokalizacji AU-05(02)_ODP[02]> w*** przypadku wystąpienia<br>***<błędów w procesie audytu, wymagających alertów w czasie rzeczywistym AU-05(02)_ODP[03] >.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AU-05(02)** | **REAKCJA NA BŁĘDY PROCESÓW AUDYTU \| ALERTY CZASU RZECZYWISTEGO** | |
| | **AU-05(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące reakcji na błędy w przetwarzaniu danych w ramach audytu; dokumentacja projektowa systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-05(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |

| | | |
|---|---|---|
| **AU-05(03)** | **REAKCJA NA BŁĘDY PROCESÓW AUDYTU \| KONFIGUROWALNE PROGI NATĘŻENIA RUCHU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-05(03)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {odrzucenie; opóźnienie};*** |
| | **AU-05(03)[01]** | egzekwowane są konfigurowalne progi natężenia ruchu komunikacji sieciowej, odzwierciedlające ograniczenia w pojemności pamięci dziennika audytu; |
| | **AU-05(03)[02]** | Do ruchu sieciowego zastosowanie ma ***<WYBRANA WARTOŚĆ PARAMETRU AU-05(03)_ODP>***, jeśli natężenie ruchu sieciowego przekracza skonfigurowane progi. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AU-05(03)** | **REAKCJA NA BŁĘDY PROCESÓW AUDYTU \| KONFIGUROWALNE PROGI NATĘŻENIA RUCHU** | |
| | **AU-05(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące reakcji na błędy w przetwarzaniu danych w ramach audytu; dokumentacja projektowa systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-05(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |

| | | |
|---|---|---|
| **AU-05(04)** | **REAKCJA NA BŁĘDY PROCESÓW AUDYTU \| WYŁĄCZENIE W PRZYPADKU AWARII** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-05(04)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {całkowite wyłączenie systemu; częściowe wyłączenie systemu; tryb awaryjny z ograniczoną funkcjonalnością dot. misji lub biznesową};*** |
| | **AU-05(04)_ODP[02]** | ***określono błędy w procesie audytu, które powodują zmianę trybu pracy;*** |
| | **AU-05(04)** | ***<WYBRANA WARTOŚĆ PARAMETRU AU-05(04)_ODP[01]>*** jest wywoływana w przypadku ***<błędu w procesie audytu AU-05(04)_ODP[02]>***, chyba że istnieje alternatywna możliwość realizacji audytu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| AU-05(04) | REAKCJA NA BŁĘDY PROCESÓW AUDYTU \| WYŁĄCZENIE W PRZYPADKU AWARII | |
|---|---|---|
| | **AU-05(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące reakcji na błędy w przetwarzaniu danych w ramach audytu; dokumentacja projektowa systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-05(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-05(04)-Test** | [WYBÓR SPOŚRÓD: Zdolność systemu do zainicjowania wyłączenia systemu lub uruchomienia trybu awaryjnego w przypadku błędu w procesie audytu]. |

| AU-05(05) | REAKCJA NA BŁĘDY PROCESÓW AUDYTU \| ZDOLNOŚĆ ALTERNATYWNEGO PROWADZENIA REJESTRU AUDYTÓW | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-05(05)_ODP** | ***określono alternatywne sposoby realizacji audytu w przypadku awarii podstawowej funkcji w tym zakresie;*** |
| | **AU-05(05)** | w przypadku awarii podstawowej funkcji zapewniona jest alternatywna możliwość realizacji audytu, wdrażająca ***<funkcję alternatywnego sposobu realizacji audytu AU-05(05)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AU-05(05)** | **REAKCJA NA BŁĘDY PROCESÓW AUDYTU \| ZDOLNOŚĆ ALTERNATYWNEGO PROWADZENIA REJESTRU AUDYTÓW** | |
| | **AU-05(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące reakcji na błędy w przetwarzaniu danych w ramach audytu; dokumentacja projektowa systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-05(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-05(05)-Test** | [WYBÓR SPOŚRÓD: Alternatywne możliwości realizacji audytu]. |

| | | |
|---|---|---|
| **AU-06** | **PRZEGLĄD ZAPISÓW AUDYTU, ANALIZA I RAPORTOWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-06_ODP[01]** | ***określono częstotliwość, z jaką przeglądane i analizowane są zapisy z audytu systemu;*** |
| | **AU-06_ODP[02]** | ***zdefiniowano nieodpowiednią lub nietypową aktywność;*** |
| | **AU-06_ODP[03]** | ***określono personel lub role, które otrzymują wyniki przeglądów i analiz zapisów systemowych;*** |
| | **AU-06a.** | zapisy z audytu systemu są przeglądane i analizowane z***<częstotliwością AU-06_ODP[01]> pod*** kątem oznak***<niewłaściwej lub nietypowej aktywności AU-06_ODP[02]> oraz*** potencjalnego wpływu niewłaściwej lub nietypowej aktywności; |
| | **AU-06b.** | Wyniki otrzymują***<personel lub role AU-06_ODP[03]>***; |

| | | |
|---|---|---|
| **AU-06** | **PRZEGLĄD ZAPISÓW AUDYTU, ANALIZA I RAPORTOWANIE** | |
| | **AU-06c.** | zakres przeglądu dokumentacji audytowej, analizy i raportowania w ramach systemu jest dostosowywany w przypadku zmiany ryzyka w oparciu o informacje od organów ścigania, informacje wywiadowcze lub inne wiarygodne źródła informacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące przeglądu, analizy i raportowania z audytu; raporty z audytu; zapisy działań podjętych w odpowiedzi na przeglądy/analizy zapisów z audytu; inne istotne dokumenty lub zapisy]. |
| | **AU-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przegląd, analizę i raportowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **AU-06(01)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| ZAUTOMATYZOWANA INTEGRACJA PROCESÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-06(01)_ODP** | ***określono automatyczne mechanizmy wykorzystywane do integracji procesów przeglądu, analizy i raportowania zapisów z audytu;*** |
| | **AU-06(01)** | procesy przeglądu, analizy i raportowania są zintegrowane za pomocą ***<mechanizmów automatycznych AU-06(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AU-06(01)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| ZAUTOMATYZOWANA INTEGRACJA PROCESÓW** | |
| | **AU-06(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące przeglądu, analizy i raportowania zapisów z audytu; procedury dotyczące badania i reagowania na podejrzane działania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-06(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przegląd, analizę i raportowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **AU-06(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy integrujące procesy przeglądu, analizy i raportowania zapisów z audytu]. |

| | | |
|---|---|---|
| **AU-06(02)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| AUTOMATYCZNE ALARMY BEZPIECZEŃSTWA** | |
| | [WYCOFANE: Włączone do SI-04]. | |

| | | |
|---|---|---|
| **AU-06(03)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| KORELACJA ZBIORÓW AUDYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-06(03)** | zapisy z audytów zawarte w różnych repozytoriach są analizowane i korelowane w celu zapewnienia odpowiedniej świadomości sytuacyjnej w całej organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AU-06(03)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| KORELACJA ZBIORÓW AUDYTU** | |
| | **AU-06(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące przeglądu, analizy i raportowania z audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu w różnych repozytoriach; inne istotne dokumenty lub zapisy]. |
| | **AU-06(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przegląd, analizę i raportowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **AU-06(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające analizę i korelację zapisów audytowych]. |

| | | |
|---|---|---|
| **AU-06(04)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| CENTRALNE PRZEGLĄDANIE I ANALIZY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-06(04)[01]** | zapewniona jest możliwość centralnego przeglądu i analizy zapisów z audytu, pozyskanych z wielu komponentów w ramach systemu; |
| | **AU-06(04)[02]** | wdrożono możliwość centralnego przeglądu i analizy zapisów audytowych z wielu komponentów w ramach systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AU-06(04)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| CENTRALNE PRZEGLĄDANIE I ANALIZY** | |
| | **AU-06(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące przeglądu, analizy i raportowania z audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; plan ochrony prywatności; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-06(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przegląd, analizę i raportowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; programiści systemu]. |
| | **AU-06(04)-Test** | [WYBÓR SPOŚRÓD: Zdolność systemu do centralizacji procesu przeglądu i analizy zapisów z audytu]. |

| | | |
|---|---|---|
| **AU-06(05)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| ZINTEGROWANA ANALIZA ZAPISÓW Z AUDYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-06(05)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {informacje o skanowaniu w zakresie podatności; dane dotyczące wydajności; monitorowanie systemu informacji;***<br>***<dane/informacje zebrane z innych źródeł AU-06(05)_ODP[02]>};*** |
| | **AU-06(05)_ODP[02]** | ***określono dane/informacje zebrane z innych źródeł, które mają być analizowane (jeśli wybrano);*** |

| | | |
|---|---|---|
| **AU-06(05)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| ZINTEGROWANA ANALIZA ZAPISÓW Z AUDYTU** | |
| | **AU-06(05)** | analiza zapisów z audytu jest zintegrowana z analizą ***<WYBRANA WARTOŚĆ PARAMETRU AU-06(05)_ODP[01]>***, aby jeszcze bardziej zwiększyć możliwości identyfikacji niewłaściwych lub nietypowych działań. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-06(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące przeglądu, analizy i raportowania z audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zintegrowana analiza zapisów z audytu,<br>informacje dotyczące skanowania w zakresie podatności, dane dotyczące wydajności, informacje dotyczące monitorowania sieci oraz związana z tym dokumentacja; inne istotne dokumenty lub zapisy]. |
| | **AU-06(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przegląd, analizę i raportowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **AU-06(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwości integracji procesu analizy zapisów z audytu z analizą źródeł danych/informacji]. |

| | | |
|---|---|---|
| **AU-06(06)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| KORELACJA AUDYTU Z MONITOROWANIEM FIZYCZNYM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-06(06)** | informacje z zapisów audytowych są skorelowane z informacjami uzyskanymi z monitorowania dostępu fizycznego w celu dalszego zwiększenia zdolności do identyfikacji podejrzanych, niewłaściwych, nietypowych lub szkodliwych działań. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-06(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące przeglądu, analizy i raportowania z audytu; procedury dotyczące monitorowania dostępu fizycznego; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dostarczająca dowodów na korelację informacji z zapisów z audytu i zapisów z monitorowania dostępu fizycznego; plan bezpieczeństwa systemu; plan ochrony prywatności; inne właściwe dokumenty lub zapisy]. |
| | **AU-06(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przegląd, analizę i raportowanie w zakresie audytu; personel organizacyjny odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **AU-06(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwość korelacji informacji z zapisów z audytu z informacjami z monitorowania dostępu fizycznego]. |

| | | |
|---|---|---|
| **AU-06(07)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| DOPUSZCZALNE DZIAŁANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-06(07)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {proces systemowy; rola; użytkownik};*** |
| | **AU-06(07)** | określono dozwolone działania dla każdej ***<WYBRANEJ WARTOŚCI PARAMETRU AU-06(07)_ODP>*** związanej z przeglądem, analizą i raportowaniem informacji o zapisach z audytu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-06(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące procesu, roli lub dozwolonych działań użytkownika objęte przeglądem, analizą i raportowaniem z audytu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AU-06(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przegląd, analizę i raportowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **AU-06(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające dozwolone działania w zakresie przeglądu, analizy i raportowania z audytu]. |

| | | |
|---|---|---|
| **AU-06(08)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| PEŁNA ANALIZA TEKSTU UPRZYWILEJOWANYCH POLECEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-06(08)** | dokonuje się analizy pełnotekstowej zarejestrowanych poleceń uprzywilejowanych w fizycznie odrębnym komponencie, podsystemie systemu lub innym systemie, który jest przeznaczony do tego celu. |

| | | |
|---|---|---|
| **AU-06(08)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| PEŁNA ANALIZA TEKSTU UPRZYWILEJOWANYCH POLECEŃ** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-06(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące przeglądu, analizy i raportowania z audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; narzędzia i techniki analizy tekstu; dokumentacja analizy tekstu audytowanych poleceń uprzywilejowanych; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **AU-06(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przegląd, analizę i raportowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **AU-06(08)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy implementujące możliwość wykonywania analizy pełnotekstowej audytowanych poleceń uprzywilejowanych]. |

| | | |
|---|---|---|
| **AU-06(09)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| KORELACJA Z INFORMACJAMI UZYSKANYMI ZE ŹRÓDEŁ NIETECHNICZNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-06(09)** | informacje ze źródeł nietechnicznych są skorelowane z informacjami z zapisów audytowych w celu zwiększenia świadomości sytuacyjnej w całej organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AU-06(09)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| KORELACJA Z INFORMACJAMI UZYSKANYMI ZE ŹRÓDEŁ NIETECHNICZNYCH** | |
| | **AU-06(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące przeglądu, analizy i raportowania z audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dostarczająca dowodów na skorelowanie informacji uzyskanych z zapisów audytu i zdefiniowanych przez organizację źródeł nietechnicznych; lista typów informacji ze źródeł nietechnicznych do skorelowania z informacjami z audytu; inne istotne dokumenty lub zapisy]. |
| | **AU-06(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przegląd, analizę i raportowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **AU-06(09)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolność do korelacji informacji ze źródeł nietechnicznych]. |

| | | |
|---|---|---|
| **AU-06(10)** | **PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE \| KORYGOWANIE POZIOMU AUDYTU** | |
| | [WYCOFANE: Włączone do AU-06]. | |

| | | |
|---|---|---|
| **AU-07** | **REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-07a.[01]** | zapewniona jest funkcja redukcji audytów i generowania raportów, która wspiera przegląd zapisów z audytu na żądanie, a także proces analizy i wymogi w zakresie sprawozdawczości oraz badania incydentów po fakcie; |

| | | |
|---|---|---|
| **AU-07** | **REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW** | |
| | **AU-07a.[02]** | wdrożona jest funkcja redukcji audytów i generowania raportów, która wspiera przegląd zapisów z audytu na żądanie, a także proces analizy i wymogi w zakresie sprawozdawczości oraz badania incydentów po fakcie; |
| | **AU-07b.[01]** | zapewniona jest możliwość redukcji audytów i generowania raportów, która nie zmienia oryginalnej treści ani kolejności czasowej zapisów z audytu; |
| | **AU-07b.[02]** | wdrożona jest możliwość redukcji audytów i generowania raportów, która nie zmienia oryginalnej treści ani kolejności czasowej zapisów z audytu; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące redukcji audytów i tworzenia raportów; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; narzędzia redukcji audytów, przeglądu, analizy i raportowania; zapisy z audytu systemu; inne stosowne dokumenty lub zapisy]. |
| | **AU-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za redukcję audytów i generowanie raportów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **AU-07-Test** | [WYBÓR SPOŚRÓD: Możliwości w zakresie skracania zapisów audytowych i generowania raportów]. |

| | | |
|---|---|---|
| **AU-07(01)** | **REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW \| AUTOMATYZACJA PROCESU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-07(01)_ODP** | ***W zapisach z audytu definiowane są obszary, które mogą być przetwarzane, sortowane lub przeszukiwane;*** |
| | **AU-07(01)[01]** | zapewniono możliwość przetwarzania, sortowania i przeszukiwania zapisów audytowych pod kątem konkretnych zdarzeń na podstawie ***<obszarów w zapisach z audytu AU-07(01)_ODP>***; |
| | **AU-07(01)[02]** | wdrożono możliwość przetwarzania, sortowania i przeszukiwania zapisów audytowych pod kątem konkretnych zdarzeń na podstawie ***<obszarów w zapisach z audytu AU-07(01)_ODP>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-07(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące redukcji audytów i generowania raportów; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; narzędzia redukcji audytów, przeglądu, analizy i raportowania; kryteria (obszary) zapisów z audytu określające zdarzenia będące przedmiotem zainteresowania; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-07(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za redukcję audytów i generowanie raportów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **AU-07(01)-Test** | [WYBÓR SPOŚRÓD: Możliwości w zakresie skracania zapisów audytowych i generowania raportów]. |

| | |
|---|---|
| **AU-07(02)** | **REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW \| AUTOMATYCZNE SORTOWANIE I WYSZUKIWANIE** |
| | [WYCOFANE: Włączone do AU-07(01)]. |

| | | |
|---|---|---|
| **AU-08** | **ZNACZNIKI CZASU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-08_ODP** | ***określona jest dokładność pomiaru czasu w znacznikach czasu zawartych w zapisach z audytu*** |
| | **AU-08a.** | do generowania znaczników czasu w zapisach z audytu wykorzystywane są wewnętrzne zegary systemowe; |
| | **AU-08b.** | w zapisach z audytu generowane są znaczniki czasu charakteryzujące się ***<dokładnością pomiaru czasu AU-08_ODP>***,<br>i wykorzystujące Uniwersalny Czas Koordynowany (UTC), czas lokalny z przesunięciem o stałej wartości<br>względem czasu UTC lub zawierające wartość przesunięcia czasu lokalnego względem UTC w znaczniku czasu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące generowania znaczników czasu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |

| | | |
|---|---|---|
| **AU-08** | **ZNACZNIKI CZASU** | |
| | **AU-08-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające generowanie znaczników czasu]. |

| | |
|---|---|
| **AU-08(01)** | **ZNACZNIKI CZASU \| SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA** |
| | [WYCOFANE: Włączone do SC-45(01)]. |

| | |
|---|---|
| **AU-08(02)** | **ZNACZNIKI CZASU \| WTÓRNE ŹRÓDŁO CZASU ODNIESIENIA** |
| | [WYCOFANE: Włączone do SC-45(02)]. |

| | | |
|---|---|---|
| **AU-09** | **OCHRONA INFORMACJI AUDYTOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-09_ODP** | ***określono osoby lub role, które mają być alarmowane po wykryciu nieautoryzowanego dostępu, modyfikacji lub usunięcia informacji audytowej;*** |
| | **AU-09a.** | informacje audytowe i narzędzia rejestrujące zapisy z audytu są chronione przed nieautoryzowanym dostępem, modyfikacją i usunięciem; |
| | **AU-09b.** | w przypadku wykrycia nieautoryzowanego dostępu, modyfikacji lub usunięcia informacji audytowych zawiadomienie otrzymują ***<personel lub role AU-09_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AU-09** | **OCHRONA INFORMACJI AUDYTOWYCH** | |
| | **AU-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka i procedury kontroli dostępu; procedury dotyczące ochrony informacji o audycie; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; narzędzia audytowe; inne istotne dokumenty lub zapisy]. |
| | **AU-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-09-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające ochronę informacji audytowych]. |

| | | |
|---|---|---|
| **AU-09(01)** | **OCHRONA INFORMACJI AUDYTOWYCH \| NOŚNIKI JEDNOKROTNEGO ZAPISU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-09(01)** | ścieżki audytu są zapisywane na wymuszonych sprzętowo nośnikach jednokrotnego zapisu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AU-09(01)** | **OCHRONA INFORMACJI AUDYTOWYCH \| NOŚNIKI JEDNOKROTNEGO ZAPISU** | |
| | **AU-09(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka i procedury kontroli dostępu; procedury dotyczące ochrony informacji z audytu; dokumentacja projektowa systemu; ustawienia sprzętowe systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; nośniki pamięci systemu; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-09(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-09(01)-Test** | [WYBÓR SPOŚRÓD: Nośniki systemowe przechowujące ścieżki audytu]. |

| | | |
|---|---|---|
| **AU-09(02)** | **OCHRONA INFORMACJI AUDYTOWYCH \| BACKUP AUDYTU W ODSEPAROWANYM FIZYCZNIE SYSTEMIE/KOMPONENCIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-09(02)_ODP** | ***określono częstotliwość wykonywania kopii zapasowych audytu w repozytorium;*** |
| | **AU-09(02)** | zapisy z audytu są kopiowane do repozytorium, które jest częścią fizycznie odseparowanego systemu lub komponentu innego niż system lub komponent poddawany audytowi, z ***<częstotliwością AU-09(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **AU-09(02)** | **OCHRONA INFORMACJI AUDYTOWYCH \| BACKUP AUDYTU W ODSEPAROWANYM FIZYCZNIE SYSTEMIE/KOMPONENCIE** | |
| | **AU-09(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące ochrony informacji o audycie; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; system lub nośnik przechowujący kopie zapasowe zapisów z audytu systemu; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-09(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-09(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające proces tworzenia kopii zapasowych zapisów z audytu]. |

| | | |
|---|---|---|
| **AU-09(03)** | **OCHRONA INFORMACJI AUDYTOWYCH \| OCHRONA KRYPTOGRAFICZNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-09(03)** | wdrożone są mechanizmy kryptograficzne chroniące integralność informacji oraz narzędzi audytowych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-09(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka i procedury kontroli dostępu; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu; ustawienia sprzętowe systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AU-09(03)** | **OCHRONA INFORMACJI AUDYTOWYCH \| OCHRONA KRYPTOGRAFICZNA** | |
| | **AU-09(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-09(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne chroniące integralność informacji i narzędzi audytowych]. |

| | | |
|---|---|---|
| **AU-09(04)** | **OCHRONA INFORMACJI AUDYTOWYCH \| DOSTĘP DO PODZBIORU UPRZYWILEJOWANYCH UŻYTKOWNIKÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-09(04)_ODP** | ***określono podzbiór uprzywilejowanych użytkowników lub ról uprawnionych do dostępu do funkcji zarządzających procesem rejestrowania zapisów z audytu;*** |
| | **AU-09(04)** | dostęp do zarządzania funkcjami rejestrowania zapisów z audytu posiada wyłącznie<br>***<podzbiór uprzywilejowanych użytkowników lub ról AU-09(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-09(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka i procedury kontroli dostępu; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista uprzywilejowanych użytkowników z dostępem do funkcji zarządzania audytem; upoważnienia do dostępu; lista kontroli dostępu; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AU-09(04)** | **OCHRONA INFORMACJI AUDYTOWYCH \| DOSTĘP DO PODZBIORU UPRZYWILEJOWANYCH UŻYTKOWNIKÓW** | |
| | **AU-09(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci]. |
| | **AU-09(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zarządzające dostępem do funkcji audytu]. |

| | | |
|---|---|---|
| **AU-09(05)** | **OCHRONA INFORMACJI AUDYTOWYCH \| PODWÓJNA AUTORYZACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-09(05)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {przeniesienie; usunięcie};*** |
| | **AU-09(05)_ODP[02]** | ***określono informacje audytowe, w zakresie których stosuje się podwójną autoryzację;*** |
| | **AU-09(05)** | Podwójną autoryzację stosuje się w przypadku***<WYBRANA WARTOŚĆ PARAMETRU AU-09(05)_ODP[01]> w*** odniesieniu do ***<informacji audytowych AU-09(05)_ODP[02]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-09(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka i procedury kontroli dostępu; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; upoważnienia do dostępu; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AU-09(05)** | **OCHRONA INFORMACJI AUDYTOWYCH \| PODWÓJNA AUTORYZACJA** | |
| | **AU-09(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci]. |
| | **AU-09(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające funkcje egzekwowania podwójnej autoryzacji]. |

| | | |
|---|---|---|
| **AU-09(06)** | **OCHRONA INFORMACJI AUDYTOWYCH \| DOSTĘP TYLKO DO ODCZYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-09(06)_ODP** | ***określono podzbiór uprzywilejowanych użytkowników lub ról z autoryzowanym dostępem tylko do odczytu do informacji audytowych;*** |
| | **AU-09(06)** | Dostęp tylko do odczytu do informacji audytowych posiada ***<podzbiór uprzywilejowanych użytkowników lub ról AU-09(06)_ODP>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-09(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka i procedury kontroli dostępu; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista uprzywilejowanych użytkowników z dostępem tylko do odczytu do informacji audytowych; upoważnienia do dostępu; lista kontroli dostępu; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AU-09(06)** | **OCHRONA INFORMACJI AUDYTOWYCH \| DOSTĘP TYLKO DO ODCZYTU** | |
| | **AU-09(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci]. |
| | **AU-09(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zarządzające dostępem do informacji audytowych]. |

| | | |
|---|---|---|
| **AU-09(07)** | **OCHRONA INFORMACJI AUDYTOWYCH \| PRZECHOWYWANIE INFORMACJI NA KOMPONENTACH Z RÓŻNYMI SYSTEMAMI OPERACYJNYMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-09(07)** | informacje audytowe przechowywane są na komponencie działającym pod innym systemem operacyjnym niż system lub komponent poddawany audytowi. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-09(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka i procedury kontroli dostępu; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-09(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt oraz rozliczalność; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci]. |

| | | |
|---|---|---|
| **AU-09(07)** | **OCHRONA INFORMACJI AUDYTOWYCH \| PRZECHOWYWANIE INFORMACJI NA KOMPONENTACH Z RÓŻNYMI SYSTEMAMI OPERACYJNYMI** | |
| | **AU-09(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwość weryfikacji systemu operacyjnego; mechanizmy weryfikujące miejsce przechowywania informacji audytowych]. |

| | | |
|---|---|---|
| **AU-10** | **NON-REPUDIATION** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-10_ODP** | ***określono działania objęte niezaprzeczalnością;*** |
| | **AU-10** | Zapewnia się niezbite dowody na to, że osoba fizyczna (lub proces działające w imieniu osoby fizycznej) wykonała ***<działania AU-10_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące niezaprzeczalności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-10-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-10-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie niezaprzeczalności]. |

| | | |
|---|---|---|
| **AU-10(01)** | **NIEZAPRZECZALNOŚĆ \| POŁĄCZENIE TOŻSAMOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-10(01)_ODP** | ***określono siłę powiązania między tożsamością twórcy informacji a samą informacją;*** |
| | **AU-10(01)(a)** | tożsamość twórcy informacji jest powiązana z informacją z ***<siłą powiązania AU-10(01)_ODP>***; |
| | **AU-10(01)(b)** | zapewnione są środki, dzięki którym osoby uprawnione mogą określić tożsamość twórcy informacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-10(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące niezaprzeczalności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-10(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-10(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie niezaprzeczalności]. |

| | | |
|---|---|---|
| **AU-10(02)** | **NIEZAPRZECZALNOŚĆ \| POWIĄZANIE INFORMACJI Z TOŻSAMOŚCIĄ TWÓRCY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-10(02)_ODP[01]** | ***określona jest częstotliwość weryfikacji powiązania informacji z tożsamością twórcy;*** |

| | | |
|---|---|---|
| **AU-10(02)** | **NIEZAPRZECZALNOŚĆ \| POWIĄZANIE INFORMACJI Z TOŻSAMOŚCIĄ TWÓRCY** | |
| | **AU-10(02)_ODP[02]** | ***definiowane są działania, które mają być wykonane w przypadku wystąpienia błędu weryfikacji;*** |
| | **AU-10(02)(a)** | powiązanie informacji z tożsamością twórcy jest weryfikowane z ***<częstotliwością AU-10(02)_ODP[01]>***; |
| | **AU-10(02)(b)** | w przypadku błędu weryfikacji podejmowane są ***<działania AU-10(02)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-10(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące niezaprzeczalności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy walidacyjne; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-10(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-10(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie niezaprzeczalności]. |

| | | |
|---|---|---|
| **AU-10(03)** | **NIEZAPRZECZALNOŚĆ \| ŁAŃCUCH NADZORU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-10(03)** | dane przeglądającego lub publikującego informacje są zawarte w ustanowionym łańcuchu nadzoru informacji podlegających przeglądowi lub udostępnieniu. |

| **AU-10(03)** | **NIEZAPRZECZALNOŚĆ \| ŁAŃCUCH NADZORU** | |
|---|---|---|
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-10(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące niezaprzeczalności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy przeglądów i udostępniania informacji; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-10(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-10(03)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające zdolności w zakresie niezaprzeczalności]. |

| **AU-10(04)** | **NIEZAPRZECZALNOŚĆ \| POTWIERDZANIE TOŻSAMOŚCI PRZEGLĄDAJĄCEGO INFORMACJE** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-10(04)_ODP[01]** | ***określono domeny bezpieczeństwa, w przypadku których przy przekazywaniu lub udostępnianiu informacji weryfikuje się powiązanie tożsamości przeglądającego informacje z informacjami;*** |
| | **AU-10(04)_ODP[02]** | ***określono działania, które mają być wykonane w przypadku błędu weryfikacji;*** |
| | **AU-10(04)(a)** | powiązanie tożsamości przeglądającego informacje z informacjami w punktach transferu lub udostępniania przed udostępnieniem lub transferem między ***<domenami bezpieczeństwa AU-10(04)_ODP[01]>*** jest weryfikowane; |

| | | |
|---|---|---|
| **AU-10(04)** | **NIEZAPRZECZALNOŚĆ \| POTWIERDZANIE TOŻSAMOŚCI PRZEGLĄDAJĄCEGO INFORMACJE** | |
| | **AU-10(04)(b)** | w przypadku błędu weryfikacji wykonywane są ***<działania AU-10(04)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-10(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące niezaprzeczalności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy walidacyjne; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-10(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-10(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie niezaprzeczalności]. |

| | |
|---|---|
| **AU-10(05)** | **NIEZAPRZECZALNOŚĆ \| PODPISY CYFROWE** |
| | [WYCOFANE: Włączone do SI-07]. |

| | | |
|---|---|---|
| **AU-11** | **RETENCJA ZAPISÓW AUDYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-11_ODP** | ***określono okres przechowywania zapisów z audytu zgodny z polityką przechowywania dokumentacji;*** |

| | | |
|---|---|---|
| **AU-11** | **RETENCJA ZAPISÓW AUDYTU** | |
| | **AU-11** | zapisy z audytu przechowywane są przez ***<okres AU-11_ODP>*** w celu zapewnienia wsparcia dla przeprowadzanych po fakcie dochodzeń dot. incydentów oraz w celu spełnienia wymagań prawnych i organizacyjnych dotyczących przechowywania informacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-11-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka i procedury przechowywania zapisów audytu; plan bezpieczeństwa; ustalony przez organizację okres przechowywania zapisów audytu; archiwa zapisów audytu; dzienniki audytu; zapisy audytu; inne istotne dokumenty lub zapisy]. |
| | **AU-11-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przechowywanie zapisów z audytu; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci]. |

| | | |
|---|---|---|
| **AU-11(01)** | **RETENCJA ZAPISÓW AUDYTU \| DŁUGOTERMINOWA ZDOLNOŚĆ DO ODZYSKU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-11(01)_ODP** | ***określono środki stosowane w celu zapewnienia długoterminowej zdolności do odzyskiwania zapisów z audytu wygenerowanych przez system;*** |
| | **AU-11(01)** | stosuje się ***<środki AU-11(01)_ODP> w*** celu zapewnienia długoterminowej zdolności do odzyskiwania zapisów z audytu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| AU-11(01) | RETENCJA ZAPISÓW AUDYTU \| DŁUGOTERMINOWA ZDOLNOŚĆ DO ODZYSKU | |
|---|---|---|
| | **AU-11(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka i procedury przechowywania zapisów z audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; archiwa z zapisami z audytu; dzienniki audytu; zapisy z audytu; inne istotne dokumenty lub zapisy]. |
| | **AU-11(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przechowywanie zapisów z audytu; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci]. |
| | **AU-11(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwości w zakresie retencji zapisów z audytu]. |

| AU-12 | TWORZENIE ZAPISÓW AUDYTU | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-12_ODP[01]** | ***określono elementy systemu, które zapewniają możliwość generowania zapisów z audytu dla typów zdarzeń (definiowanych w AU-02_ODP[02]);*** |
| | **AU-12_ODP[02]** | ***określono personel lub role uprawnione do wyboru typów zdarzeń, które mają być rejestrowane przez określone komponenty systemu;*** |
| | **AU-12a.** | możliwości generowania zapisów z audytu dla typów zdarzeń, które system może audytować (definiowanych w AU-02_ODP[01]) zapewniają ***<komponenty systemu AU-12_ODP[01]>***; |
| | **AU-12b.** | ***<personel lub role AU-12_ODP[02]>*** mogą wybierać typy zdarzeń, które mają być rejestrowane przez określone komponenty systemu; |

| | | |
|---|---|---|
| **AU-12** | **TWORZENIE ZAPISÓW AUDYTU** | |
| | **AU-12c.** | dla typów zdarzeń definiowanych w AU-02_ODP[02] generowane są zapisy z audytu, które zawierają treść definiowaną w AU-03. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-12-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; procedury dotyczące tworzenia zapisów z audytu; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista zdarzeń podlegających audytowi; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-12-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sporządzanie zapisów z audytu; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-12-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwości w zakresie generowania zapisów z audytu]. |

| | | |
|---|---|---|
| **AU-12(01)** | **TWORZENIE ZAPISÓW AUDYTU \| OGÓLNOSYSTEMOWE/SKORELOWANE W CZASIE ŚCIEŻKI AUDYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-12(01)_ODP[01]** | ***określono komponenty systemu, z których zapisy audytowe mają być zestawione w ogólnosystemową (logiczną lub fizyczną) ścieżkę audytu;*** |
| | **AU-12(01)_ODP[02]** | ***określono poziom tolerancji dla relacji pomiędzy znacznikami czasu poszczególnych zapisów w ramach ścieżki audytu;*** |

| | | |
|---|---|---|
| **AU-12(01)** | **TWORZENIE ZAPISÓW AUDYTU \| OGÓLNOSYSTEMOWE/SKORELOWANE W CZASIE ŚCIEŻKI AUDYTU** | |
| | **AU-12(01)** | zapisy z audytu z ***<komponentów systemu AU-12(01)_ODP[01]>*** są kompilowane w ogólnosystemową (logiczną lub fizyczną) ścieżkę audytu, która jest skorelowana w czasie, w granicach ***<poziomu tolerancji AU-12(01)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-12(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące generowania zapisów z audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; ścieżka audytu całego systemu (logiczna lub fizyczna); zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-12(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sporządzanie zapisów z audytu; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-12(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwości w zakresie generowania zapisów z audytu]. |

| | | |
|---|---|---|
| **AU-12(02)** | **TWORZENIE ZAPISÓW AUDYTU \| UJEDNOLICONE FORMATY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-12(02)** | Ogólnosystemowa (logiczna lub fizyczna) ścieżka audytu składająca się z zapisów z audytu jest tworzona w standardowym formacie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| AU-12(02) | TWORZENIE ZAPISÓW AUDYTU \| UJEDNOLICONE FORMATY | |
|---|---|---|
| | **AU-12(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące generowania zapisów z audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; ścieżka audytu całego systemu (logiczna lub fizyczna); zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-12(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za tworzenie zapisów z audytu; personel organizacyjny odpowiedzialny za bezpieczeństwo; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-12(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwości w zakresie generowania zapisów z audytu]. |

| AU-12(03) | TWORZENIE ZAPISÓW AUDYTU \| ZMIANY DOKONYWANE PRZEZ UPRAWNIONE OSOBY | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-12(03)_ODP[01]** | ***określono osoby lub role uprawnione do zmiany rejestrowania w elementach systemu;*** |
| | **AU-12(03)_ODP[02]** | ***określono elementy systemu, w których ma być prowadzone rejestrowanie;*** |
| | **AU-12(03)_ODP[03]** | ***określono możliwe do wybrania kryteria dot. zdarzeń, w oparciu o które ma się odbywać rejestrowanie zmian;*** |
| | **AU-12(03)_ODP[04]** | ***określono progi czasowe, w których odbywa się zmiana czynności dot. rejestrowania;*** |

| | | |
|---|---|---|
| **AU-12(03)** | **TWORZENIE ZAPISÓW AUDYTU \| ZMIANY DOKONYWANE PRZEZ UPRAWNIONE OSOBY** | |
| | **AU-12(03)[01]** | ***<osoby lub funkcje AU-12(03)_ODP[01]>*** mają możliwość wprowadzenia zmian w rejestrowaniu realizowanym w ***<komponentach systemu AU-12(03)_ODP[02]> na*** podstawie<br>***<kryteriów zdarzeń do wyboru AU-12(03)_ODP[03]> w*** ramach ***<progów czasowych AU-12(03)_ODP[04]>;*** |
| | **AU-12(03)[02]** | ***<osoby lub funkcje AU-12(03)_ODP[01]>*** mają możliwość wprowadzenia zmian w rejestrowaniu realizowanym w ***<komponentach systemu AU-12(03)_ODP[02]> na*** podstawie<br>***<kryteriów zdarzeń do wyboru AU-12(03)_ODP[03]> w*** ramach ***<progów czasowych AU-12(03)_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-12(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące generowania zapisów z audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; generowana przez system lista osób lub ról upoważnionych do zmiany przeprowadzanego audytu; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-12(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sporządzanie zapisów z audytu; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-12(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwości w zakresie generowania zapisów z audytu]. |

| | | |
|---|---|---|
| **AU-12(04)** | **TWORZENIE ZAPISÓW AUDYTU \| AUDYT PARAMETRÓW ZAPYTAŃ O DANE IDENTYFIKACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-12(04)[01]** | zapewniona jest możliwość kontroli parametrów zdarzeń dot. zapytań użytkowników o zbiory danych zawierające dane identyfikacyjne; |
| | **AU-12(04)[02]** | zapewniona jest możliwość audytów parametrów zdarzeń dot. zapytań użytkowników o zbiory danych zawierające dane identyfikacyjne; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-12(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące generowania zapisów z audytu; zapisy dot. zapytań użytkowników o zbiory danych zawierające dane identyfikacyjne; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; mapa działań w zakresie danych systemowych; zapisy audytowe systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-12(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sporządzanie zapisów z audytu; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-12(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwości w zakresie generowania zapisów z audytu]. |

| | | |
|---|---|---|
| **AU-13** | **MONITOROWANIE UJAWNIANIA INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-13_ODP[01]** | ***określono informacje z otwartych źródeł lub strony z informacjami, które mają być monitorowane pod kątem dowodów na nieuprawnione ujawnienie informacji organizacji;*** |
| | **AU-13_ODP[02]** | ***określono częstotliwość monitorowania informacji z otwartych źródeł lub stron z informacjami pod kątem dowodów na nieuprawnione ujawnienie informacji organizacji;*** |
| | **AU-13_ODP[03]** | ***określono personel lub role, które należy powiadomić w razie wykrycia przypadku ujawnienia informacji;*** |
| | **AU-13_ODP[04]** | ***określono dodatkowe czynności, które należy podjąć w razie wykrycia przypadku ujawnienia informacji;*** |
| | **AU-13a.** | ***<otwarte źródła lub strony z informacjami AU-13_ODP[01]>*** są/będą monitorowane z ***<częstotliwością AU-13_ODP[02]>*** pod kątem dowodów na nieuprawnione ujawnienie informacji organizacji; |
| | **AU-13b.01** | w przypadku wykrycia ujawnienia informacji powiadomienie otrzymują ***<personel lub role AU-13_ODP[03]>*** |
| | **AU-13b.02** | w przypadku wykrycia ujawnienia informacji podejmowane są ***<dodatkowe działania AU-13_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-13-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące monitorowania ujawniania informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące monitorowania; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AU-13** | **MONITOROWANIE UJAWNIANIA INFORMACJI** | |
| | **AU-13-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie informacji z otwartych źródeł lub stron z informacjami; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność]. |
| | **AU-13-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające monitorowanie ujawniania informacji]. |

| | | |
|---|---|---|
| **AU-13(01)** | **MONITOROWANIE UJAWNIANIA INFORMACJI \| WYKORZYSTYWANIE ZAUTOMATYZOWANYCH NARZĘDZI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-13(01)_ODP** | ***opracowano automatyczne mechanizmy monitorowania otwartych źródeł informacji i stron z informacjami;*** |
| | **AU-13(01)** | otwarte źródła informacji i strony z informacjami są monitorowane za pomocą ***<mechanizmów automatycznych AU-13(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-13(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące monitorowania ujawniania informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; narzędzia automatycznego monitorowania; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-13(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie ujawniania informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności. |

| | | |
|---|---|---|
| **AU-13(01)** | **MONITOROWANIE UJAWNIANIA INFORMACJI \| WYKORZYSTYWANIE ZAUTOMATYZOWANYCH NARZĘDZI** | |
| | **AU-13(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające monitorowanie ujawniania informacji]. |

| | | |
|---|---|---|
| **AU-13(02)** | **MONITOROWANIE UJAWNIANIA INFORMACJI \| PRZEGLĄD MONITOROWANYCH STRON** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-13(02)_ODP** | ***określono częstotliwość przeglądania monitorowanych stron z informacjami z otwartych źródeł;*** |
| | **AU-13(02)** | lista monitorowanych stron z informacjami z otwartych źródeł jest przeglądana z ***<częstotliwością AU-13(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-13(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące monitorowania ujawniania informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; przeglądy monitorowanych stron z informacjami z otwartych źródeł; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-13(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie stron informacjami z otwartych źródeł; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **AU-13(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające monitorowanie ujawniania informacji]. |

| | | |
|---|---|---|
| **AU-13(03)** | **MONITOROWANIE UJAWNIANIA INFORMACJI \| NIEAUTORYZOWANE POWIELANIE INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-13(03)** | stosowane są techniki wykrywania, procesy i narzędzia w celu określenia czy podmioty zewnętrzne powielają informacje organizacji w nieuprawniony sposób. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-13(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące monitorowania ujawniania informacji; procedury dotyczące powielania informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; zasoby szkoleniowe dla pracowników w zakresie rozpoznawania nieuprawnionego wykorzystania informacji organizacji; inne istotne dokumenty lub zapisy]. |
| | **AU-13(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie nieautoryzowanego powielania informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **AU-13(03)-Test** | [WYBÓR SPOŚRÓD: Narzędzia do identyfikacji przypadków nieautoryzowanego powielania informacji]. |

| | | |
|---|---|---|
| **AU-14** | **AUDYT SESJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-14_ODP[01]** | ***określono użytkowników lub role, które mogą audytować zawartość sesji użytkownika;*** |

| | | |
|---|---|---|
| **AU-14** | **AUDYT SESJI** | |
| | **AU-14_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {zapis; widok; odsłuch; dziennik};*** |
| | **AU-14_ODP[03]** | ***określono okoliczności, w których zawartość sesji użytkownika może zostać poddana audytowi;*** |
| | **AU-14a.[01]** | ***<użytkownicy lub role AU-14_ODP[01]>*** mają możliwość ***<WYBRANA WARTOŚĆ PARAMETRU AU-14_ODP[02]> w*** odniesieniu do zawartości sesji użytkownika w ***<okolicznościach AU-14_ODP[03]>***; |
| | **AU-14a.[02]** | wdrożono możliwość dla ***<użytkowników lub ról AU-14_ODP[01]>***, aby mogli oni ***<WYBRANA WARTOŚĆ PARAMETRU AU-14_ODP[02]> w*** odniesieniu do zawartości sesji użytkownika w ***<okolicznościach AU-14_ODP[03]>***; |
| | **AU-14b.[01]** | opracowano działania związane z audytem sesji w porozumieniu z radcą prawnym i zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, regulacjami, politykami, standardami i wytycznymi; |
| | **AU-14b.[02]** | zintegrowano działania związane z audytem sesji w porozumieniu z radcą prawnym i zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, regulacjami, politykami, standardami i wytycznymi; |
| | **AU-14b.[03]** | realizuje się działania związane z audytem sesji w porozumieniu z radcą prawnym i zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, regulacjami, politykami, standardami i wytycznymi; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-14-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące audytu sesji użytkownika; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **AU-14** | **AUDYT SESJI** | |
| | **AU-14-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu; radca prawny; personel odpowiedzialny za zapewnienie swobód obywatelskich]. |
| | **AU-14-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwości w zakresie audytu sesji użytkownika]. |

| | | |
|---|---|---|
| **AU-14(01)** | **AUDYT SESJI \| URUCHAMIANIE SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-14(01)** | audyty sesji są inicjowane automatycznie przy uruchomieniu systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-14(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące audytu sesji użytkownika; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-14(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **AU-14(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwości w zakresie audytu sesji użytkownika]. |

| | |
|---|---|
| **AU-14(02)** | **AUDYT SESJI \| PRZECHWYTYWANIE I ZAPISYWANIE TREŚCI** |
| | [WYCOFANE: Włączone do AU-14]. |

| | | |
|---|---|---|
| **AU-14(03)** | **AUDYT SESJI \| ZDALNE WYŚWIETLANIE I ODSŁUCHIWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-14(03)[01]** | zapewnia się możliwość zdalnego wyświetlania i odsłuchiwania przez uprawnionych użytkowników treści związanych z ustanowioną sesją użytkownika w czasie rzeczywistym; |
| | **AU-14(03)[02]** | wdrożono możliwość zdalnego wyświetlania i odsłuchiwania przez uprawnionych użytkowników treści związanych z ustanowioną sesją użytkownika w czasie rzeczywistym; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-14(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące audytu sesji użytkownika; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-14(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu; radca prawny; personel odpowiedzialny za zapewnienie swobód obywatelskich]. |
| | **AU-14(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwości w zakresie audytu sesji użytkownika]. |

| | |
|---|---|
| **AU-15** | **ZDOLNOŚĆ DO ALTERNATYWNEGO AUDYTU** |
| | [WYCOFANE: Włączone do AU-05(05)]. |

| | | |
|---|---|---|
| **AU-16** | **AUDYT MIĘDZYORGANIZACYJNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-16_ODP[01]** | ***określono metody koordynacji pomiędzy organizacjami zewnętrznymi w zakresie informacji audytowych, gdy takie informacje są przekazywane poza obręb organizacji;*** |
| | **AU-16_ODP[02]** | ***określono informacje audytowe podlegające koordynacji pomiędzy organizacjami zewnętrznymi w przypadku gdy informacje audytowe są przekazywane poza obręb organizacji;*** |
| | **AU-16** | określono ***<metody AU-16_ODP[01]>*** koordynacji pomiędzy organizacjami zewnętrznymi w zakresie ***<informacji audytowych AU-16_ODP[02]>***, gdy takie informacje są przekazywane poza obręb organizacji; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-16-Badanie** | [WYBÓR SPOŚRÓD: Polityka audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące metod koordynacji pomiędzy organizacjami zewnętrznymi w zakresie informacji audytowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-16-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za koordynację pomiędzy organizacjami zewnętrznymi w zakresie informacji audytowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **AU-16** | **AUDYT MIĘDZYORGANIZACYJNY** | |
| | **AU-16-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające audyt międzyorganizacyjny]. |

| | | |
|---|---|---|
| **AU-16(01)** | **AUDYT MIĘDZYORGANIZACYJNY \| OCHRONA TOŻSAMOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-16(01)** | tożsamość osób w międzyorganizacyjnych ścieżkach audytu jest chroniona. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-16(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące międzyorganizacyjnych ścieżek audytu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne stosowne dokumenty lub zapisy]. |
| | **AU-16(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za audyt międzyorganizacyjny; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **AU-16(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające audyt międzyorganizacyjny (jeśli dotyczy)]. |

| | | |
|---|---|---|
| **AU-16(02)** | **AUDYT MIĘDZYORGANIZACYJNY \| UDOSTĘPNIANIE INFORMACJI AUDYTOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-16(02)_ODP[01]** | ***określono organizacje, którym mają być udostępnione informacje dot. audytu międzyorganizacyjnego;*** |
| | **AU-16(02)_ODP[02]** | ***zdefiniowano międzyorganizacyjne umowy o udostępnianiu informacji, które mają zastosowanie w przypadku przekazywania organizacjom informacji dot. audytów międzyorganizacyjnych;*** |
| | **AU-16(02)** | informacje dot. audytów międzyorganizacyjnych są przekazywane do ***<organizacji AU-16(02)_ODP[01]>*** na podstawie ***<międzyorganizacyjnych umów o udostępnianiu informacji AU-16(02)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-16(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące międzyorganizacyjnej wymiany informacji dotyczących audytu; umowy o udostępnianiu informacji; inne stosowne dokumenty lub zapisy]. |
| | **AU-16(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przekazywanie informacji z audytów międzyorganizacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **AU-16(03)** | **AUDYT MIĘDZYORGANIZACYJNY \| ODDZIELANIE DANYCH OSOBOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **AU-16(03)_ODP** | ***określono środki pozwalające oddzielić dane osobowe od informacji audytowych przekazywanych poza obręb organizacji;*** |
| | **AU-16(03)** | stosuje się ***<środki AU-16(03)_ODP> w*** celu oddzielenia danych osobowych od informacji audytowych przekazywanych poza obręb organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **AU-16(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie audytu i rozliczalności; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury dotyczące międzyorganizacyjnej wymiany informacji audytowych; polityka lub procedury dotyczące usuwania danych identyfikacyjnych z informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **AU-16(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przekazywanie informacji z audytów międzyorganizacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **AU-16(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające możliwość oddzielania danych osobowych]. |

## 4.4. KATEGORIA CA - OCENA, AUTORYZACJA I MONITORING

| | | |
|---|---|---|
| **CA-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-01_ODP[01]** | ***określono personel lub role, którym należy przekazać politykę oceny, autoryzacji i monitorowania;*** |
| | **CA-01_ODP[02]** | ***określono personel lub role, którym należy przekazać procedury oceny, autoryzacji i monitorowania;*** |
| | **CA-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **CA-01_ODP[04]** | ***określono pracownika funkcyjnego odpowiedzialnego za zarządzanie polityką i procedurami oceny, autoryzacji i monitorowania;*** |
| | **CA-01_ODP[05]** | ***określono częstotliwość, z jaką polityka oceny, autoryzacji i monitorowania jest przeglądana i aktualizowana;*** |
| | **CA-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji polityki oceny, autoryzacji i monitorowania;*** |
| | **CA-01_ODP[07]** | ***określono częstotliwość, z jaką aktualne procedury oceny, autoryzacji i monitorowania są przeglądane i aktualizowane;*** |
| | **CA-01_ODP[08]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji procedur oceny, autoryzacji i monitorowania;*** |
| | **CA-01a.[01]** | opracowano i udokumentowano politykę oceny, autoryzacji i monitorowania; |
| | **CA-01a.[02]** | polityka oceny, autoryzacji i monitorowania jest rozpowszechniana wśród ***<personelu lub ról CA-01_ODP[01]>***; |

| **CA-01** | **POLITYKA I PROCEDURY** | |
|---|---|---|
| | **CA-01a.[03]** | opracowano i udokumentowano procedury oceny, autoryzacji i monitorowania ułatwiające realizację polityki w tym obszarze, a także stosowanie powiązanych zabezpieczeń w zakresie oceny, autoryzacji i monitorowania; |
| | **CA-01a.[04]** | procedury oceny, autoryzacji i monitorowania są rozpowszechniane wśród ***<personelu lub ról CA-01_ODP[02]>***; |
| | **CA-01a.01(a)[01]** | polityka oceny, autoryzacji i monitorowania ***<WYBRANA WARTOŚĆ PARAMETRU CA-01_ODP[03]>*** odnosi się do celu; |
| | **CA-01a.01(a)[02]** | polityka oceny, autoryzacji i monitorowania ***<WYBRANA WARTOŚĆ PARAMETRU CA-01_ODP[03]>*** odnosi się do zakresu; [03] WYBRANY PARAMETR> polityka oceny, autoryzacji i monitorowania odnosi się do zakresu; |
| | **CA-01a.01(a)[03]** | polityka oceny, autoryzacji i monitorowania ***<WYBRANA WARTOŚĆ PARAMETRU CA-01_ODP[03]>*** odnosi się do ról; [03] WYBRANY PARAMETR> polityka oceny, autoryzacji i monitorowania odnosi się do ról; |
| | **CA-01a.01(a)[04]** | polityka oceny, autoryzacji i monitorowania ***<WYBRANA WARTOŚĆ PARAMETRU CA-01_ODP[03]>*** odnosi się do obowiązków; |
| | **CA-01a.01(a)[05]** | polityka oceny, autoryzacji i monitorowania ***<WYBRANA WARTOŚĆ PARAMETRU CA-01_ODP[03]>*** odnosi się do zaangażowania kierownictwa; |
| | **CA-01a.01(a)[06]** | ***<WYBRANA WARTOŚĆ PARAMETRU CA-01_ODP[03]>***polityka oceny, autoryzacji i monitorowania odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **CA-01a.01(a)[07]** | ***<WYBRANA WARTOŚĆ PARAMETRU CA-01_ODP[03]>***polityka oceny, autoryzacji i monitorowania odnosi się do zgodności; |

| | | |
|---|---|---|
| **CA-01** | **POLITYKA I PROCEDURY** | |
| | **CA-01a.01(b)** | polityka oceny, autoryzacji i monitorowania ***<WYBRANA WARTOŚĆ PARAMETRU CA-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **CA-01b.** | ***<urzędnik CA-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur oceny, autoryzacji i monitorowania; |
| | **CA-01c.01[01]** | aktualna polityka oceny, autoryzacji i monitorowania jest poddawana przeglądowi i aktualizacji z ***<częstotliwością CA-01_ODP[05]>***; |
| | **CA-01c.01[02]** | aktualna polityka oceny, autoryzacji i monitorowania jest poddawana przeglądowi i aktualizacji po ***<zdarzeniach CA-01_ODP[06]>***; |
| | **CA-01c.02[01]** | aktualne procedury oceny, autoryzacji i monitorowania są poddawane przeglądowi i aktualizacji z ***<częstotliwością CA-01_ODP[07]>***; |
| | **CA-01c.02[02]** | aktualne procedury oceny, autoryzacji i monitorowania są poddawane przeglądowi i aktualizacji po ***<zdarzeniach CA-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury oceny, autoryzacji i monitorowania; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za politykę oceny, autoryzacji i monitorowania; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **CA-02** | **OCENA ZABEZPIECZEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-02_ODP[01]** | ***określono częstotliwość oceny zabezpieczeń systemu i jego środowiska działania;*** |
| | **CA-02_ODP[02]** | ***określono osoby lub role, którym mają być przekazywane wyniki oceny;*** |
| | **CA-02a.** | wybrano odpowiedniego oceniającego lub zespół oceniający zgodnie z rodzajem przeprowadzanej oceny; |
| | **CA-02b.01** | opracowano plan oceny zabezpieczeń, który opisuje zakres oceny, w tym zabezpieczenia i ich udoskonalenia podlegające ocenie; |
| | **CA-02b.02** | opracowano plan oceny zabezpieczeń, który opisuje zakres oceny, w tym procedury oceny wykorzystane do określenia skuteczności zabezpieczeń; |
| | **CA-02b.03[01]** | opracowano plan oceny zabezpieczeń, który opisuje zakres oceny, w tym środowisko oceny; |
| | **CA-02b.03[02]** | opracowano plan oceny zabezpieczeń, który opisuje zakres oceny, w tym zespół oceniający; |
| | **CA-02b.03[03]** | opracowano plan oceny zabezpieczeń, który opisuje zakres oceny, w tym role i obowiązki w zakresie oceny; |
| | **CA-02c.** | przed przeprowadzeniem oceny plan oceny zabezpieczeń jest przeglądany i zatwierdzany przez pracownika funkcyjnego zatwierdzającego lub przez wyznaczonego przedstawiciela; |

| | | |
|---|---|---|
| **CA-02** | **OCENA ZABEZPIECZEŃ** | |
| | **CA-02d.[01]** | zabezpieczenia są oceniane w systemie i jego środowisku operacyjnym<br>z ***<częstotliwością oceny CA-02_ODP[01]>*** w celu określenia zakresu, w jakim zabezpieczenia są wdrożone prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w odniesieniu do spełnienia ustalonych wymagań dot. bezpieczeństwa; |
| | **CA-02d.[02]** | zabezpieczenia są oceniane w systemie i jego środowisku operacyjnym<br>z ***<częstotliwością oceny CA-02_ODP[01]>*** w celu określenia zakresu, w jakim zabezpieczenia są wdrożone prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w odniesieniu do spełnienia ustalonych wymagań dot. prywatności; |
| | **CA-02e.** | sporządza się sprawozdanie z oceny zabezpieczeń, które dokumentuje jej wyniki; |
| | **CA-02f.** | wyniki oceny zabezpieczeń otrzymują ***<osoby lub role CA-02_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; procedury dotyczące planowania oceny; procedury dotyczące oceny zabezpieczeń; plan oceny zabezpieczeń; raport z oceny zabezpieczeń; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę zabezpieczeń; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-02-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające ocenę zabezpieczeń, opracowanie planu oceny zabezpieczeń lub sprawozdawczość w zakresie oceny zabezpieczeń]. |

| | | |
|---|---|---|
| **CA-02(01)** | **OCENA ZABEZPIECZEŃ\| NIEZALEŻNE OCENY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-02(01)** | do przeprowadzenia ocen zabezpieczeń zatrudnia się niezależnych oceniających lub zespoły oceniające. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-02(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; procedury dotyczące oceny zabezpieczeń; poprzedni plan oceny zabezpieczeń; poprzedni raport z oceny zabezpieczeń; plan i etapy działania; istniejące upoważnienie; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-02(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę zabezpieczeń; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności. |

| | | |
|---|---|---|
| **CA-02(02)** | **OCENA ZABEZPIECZEŃ\| OCENY SPECJALISTYCZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-02(02)_ODP[01]** | ***określono częstotliwość, z jaką należy włączać oceny specjalistyczne do oceny zabezpieczeń;*** |
| | **CA-02(02)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {zapowiedziane; niezapowiedziane};*** |

| | | |
|---|---|---|
| **CA-02(02)** | **OCENA ZABEZPIECZEŃ\| OCENY SPECJALISTYCZNE** | |
| | **CA-02(02)_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {szczegółowe monitorowanie; narzędzia bezpieczeństwa; automatyczne testy bezpieczeństwa; skanowanie podatności; testowanie złośliwych użytkowników; ocena zagrożeń wewnętrznych; test wydajności i obciążenia; ocena wycieku lub utraty danych; <inne sposoby oceny CA-02(02)_ODP[04]>};*** |
| | **CA-02(02)_ODP[04]** | ***określono inne sposoby oceny (jeśli wybrano);*** |
| | **CA-02(02)** | ***<częstotliwość oceny specjalistycznej CA-02(02)_ODP[01]> <WYBRANA WARTOŚĆ PARAMETRU CA-02(02)_ODP[02]> <WYBRANA WARTOŚĆ PARAMETRU CA-02(02)_ODP[03]>*** stanowią element ocen zabezpieczeń. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; procedury dotyczące ocen zabezpieczeń; plan oceny zabezpieczeń; sprawozdanie z oceny zabezpieczeń; dowody oceny zabezpieczeń; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę zabezpieczeń; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-02(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające ocenę zabezpieczeń]. |

| | | |
|---|---|---|
| **CA-02(03)** | **OCENA ZABEZPIECZEŃ\| KORZYSTANIE Z WYNIKÓW UZYSKANYCH OD ORGANIZACJI ZEWNĘTRZNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-02(03)_ODP[01]** | ***określono organizacje zewnętrzne, od których uzyskuje się wyniki ocen zabezpieczeń;*** |
| | **CA-02(03)_ODP[02]** | ***określono system, w przypadku którego ocenę zabezpieczeń przeprowadziła organizacja zewnętrzna;*** |
| | **CA-02(03)_ODP[03]** | ***określono wymagania, jakie powinna spełniać ocena zabezpieczeń systemu przeprowadzana przez organizację zewnętrzną;*** |
| | **CA-02(03)** | wyniki ocen zabezpieczeń przeprowadzonych przez ***<organizacje zewnętrzne CA-02(03)_ODP[01]> w <systemie CA-02(03)_ODP[02]>*** są wykorzystywane, jeżeli ocena spełnia ***<wymagania CA-02(03)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-02(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; procedury dot. oceny zabezpieczeń; wymagania dotyczące oceny zabezpieczeń; plan oceny zabezpieczeń; sprawozdanie z oceny zabezpieczeń; dowody oceny zabezpieczeń; plan i etapy działania; plan bezpieczeństwa systemu; plan ochrony prywatności; inne stosowne dokumenty lub zapisy]. |
| | **CA-02(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę zabezpieczeń; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; personel wykonujący oceny zabezpieczeń dla określonych organizacji zewnętrznych]. |

| | | |
|---|---|---|
| **CA-03** | **WYMIANA INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-03_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{umowy o bezpieczeństwie połączeń wzajemnych; umowy o bezpieczeństwie wymiany informacji; protokoły ustaleń lub umowy; umowy o poziomie usług; umowy z użytkownikami; umowy o zachowaniu poufności <typ umowy CA-03_ODP[02]>};*** |
| | **CA-03_ODP[02]** | ***określono rodzaj umowy, której celem jest zatwierdzanie i zarządzanie wymianą informacji (jeśli wybrano);*** |
| | **CA-03_ODP[03]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji umów;*** |
| | **CA-03a.** | wymiana informacji między systemem a innymi systemami jest zatwierdzana i zarządzana za pomocą ***<WYBRANA WARTOŚĆ PARAMETRU CA-03_ODP[01]>***; |
| | **CA-03b.[01]** | charakterystyka interfejsu jest wyszczególniona w każdej umowie o wymianie informacji; |
| | **CA-03b.[02].** | wymagania dotyczące bezpieczeństwa są wyszczególnione w każdej umowie o wymianie informacji; |
| | **CA-03b.[03]** | wymagania dotyczące prywatności są wyszczególnione w każdej umowie o wymianie informacji; |
| | **CA-03b.[04]** | zabezpieczenia są wyszczególnione w każdej umowie o wymianie informacji; |
| | **CA-03b.[05]** | obowiązki dotyczące każdego systemu są wyszczególnione w każdej umowie o wymianie informacji; |
| | **CA-03b.[06]** | wpływ przekazywanych informacji jest wyszczególniony w każdej umowie o wymianie informacji; |

| | | |
|---|---|---|
| **CA-03** | **WYMIANA INFORMACJI** | |
| | **CA-03c.** | umowy są poddawane przeglądowi i aktualizacji z ***<częstotliwością CA-03_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące połączeń systemowych; polityka ochrony systemu i komunikacji; umowy dotyczące bezpieczeństwa połączeń systemowych; umowy dotyczące bezpieczeństwa wymiany informacji; protokoły ustaleń lub porozumienia; umowy o poziomie usług; umowy o zachowaniu poufności; dokumentacja projektowa systemu; architektura firmowa; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za opracowywanie, wdrażanie lub zatwierdzanie umów o połączeniach międzysystemowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel zarządzający systemem lub systemami, których dotyczy umowa o bezpieczeństwie połączenia]. |

| | |
|---|---|
| **CA-03(01)** | **WYMIANA INFORMACJI \| POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW KRAJOWYCH** |
| | [WYCOFANE: Włączone do SC-07(25)]. |

| | |
|---|---|
| **CA-03(02)** | **WYMIANA INFORMACJI \| POŁĄCZENIA NIEJAWNYCH SYSTEMÓW KRAJOWYCH** |
| | [WYCOFANE: Włączone do SC-07(26)]. |

| | |
|---|---|
| **CA-03(03)** | **WYMIANA INFORMACJI \| POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW TRANSGRANICZNYCH** |
| | [WYCOFANE: Włączone do SC-07(27)]. |

| | |
|---|---|
| **CA-03(04)** | **WYMIANA INFORMACJI \| POŁĄCZENIA Z SIECIAMI PUBLICZNYMI** |
| | [WYCOFANE: Włączone do SC-07(28)]. |

| | |
|---|---|
| **CA-03(05)** | **WYMIANA INFORMACJI \| OGRANICZENIA DOTYCZĄCE POŁĄCZEŃ SYSTEMÓW ZEWNĘTRZNYCH** |
| | [WYCOFANE: Włączone do SC-07(05)]. |

| | | |
|---|---|---|
| **CA-03(06)** | **WYMIANA INFORMACJI \| AUTORYZACJE PRZESYŁU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-03(06)** | osoby lub systemy przesyłające dane pomiędzy połączonymi systemami posiadają wymagane autoryzacje (tj. uprawnienia lub przywileje wymagane do zapisu) przed przyjęciem takich danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| CA-03(06) | WYMIANA INFORMACJI \| AUTORYZACJE PRZESYŁU | |
|---|---|---|
| | **CA-03(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące połączeń systemowych; polityka dotycząca ochrony systemu i komunikacji; umowy dotyczące wzajemnych połączeń między systemami; umowy dotyczące bezpieczeństwa wymiany informacji; protokoły ustaleń lub umowy; umowy o poziomie usług; umowy o poufności; dokumentacja projektowa systemy; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; raport z oceny zabezpieczeń; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-03(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie połączeniami z systemami zewnętrznymi; administratorzy sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-03(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające ograniczenia w zakresie łączenia się z systemami zewnętrznymi]. |

| CA-03(07) | WYMIANA INFORMACJI \| POBIERANIE INFORMACJI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-03(07)(a)** | zdefiniowano wymianę informacji pobieranych z innymi systemami poprzez systemy zidentyfikowane w CA-03a; |
| | **CA-03(07)(b)** | podejmowane są środki w celu zapewnienia, że wymiana informacji pobieranych zostanie przerwana, jeżeli zabezpieczenia zidentyfikowanych systemów pobierających nie mogą zostać zweryfikowane lub zatwierdzone. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CA-03(07)** | **WYMIANA INFORMACJI \| POBIERANIE INFORMACJI** | |
| | **CA-03(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka kontroli dostępu; procedury dotyczące połączeń systemowych; polityka dotycząca ochrony systemu i komunikacji; umowy dotyczące wzajemnych połączeń między systemami; umowy dotyczące bezpieczeństwa wymiany informacji; protokoły ustaleń lub umowy; umowy o poziomie usług; umowy o poufności; dokumentacja projektowa systemy; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; raport z oceny zabezpieczeń; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-03(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie połączeniami z systemami zewnętrznymi; administratorzy sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-03(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające ograniczenia w zakresie łączenia się z systemami zewnętrznymi]. |

| | |
|---|---|
| **CA-04** | **CERTYFIKACJA BEZPIECZEŃSTWA** |
| | [WYCOFANE: Włączone do CA-02]. |

| | | |
|---|---|---|
| **CA-05** | **PLAN I ETAPY DZIAŁANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-05_ODP** | ***określono częstotliwość, z jaką należy aktualizować istniejący plan i etapy działania w oparciu o wnioski z ocen zabezpieczeń, niezależnych audytów lub przeglądów oraz działań w zakresie ciągłego monitorowania;*** |

| | | |
|---|---|---|
| **CA-05** | **PLAN I ETAPY DZIAŁANIA** | |
| | **CA-05a.** | opracowano plan i etapy działania dla systemu, aby udokumentować planowane działania naprawcze organizacji w celu skorygowania słabych punktów lub braków wykrytych w ramach oceny kontroli oraz zmniejszenia lub wyeliminowania znanych podatności w systemie; |
| | **CA-05b.** | istniejący plan i etapy działania są aktualizowane z ***<częstotliwością CA-05_ODP>*** na podstawie wyników ocen zabezpieczeń, niezależnych audytów lub przeglądów oraz działań związanych z ciągłym monitorowaniem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; procedury dotyczące planu i etapów działania; plan oceny zabezpieczeń; sprawozdanie z oceny zabezpieczeń; dowody oceny zabezpieczeń; plan działania i etapów działania; plan bezpieczeństwa systemu; plan ochrony prywatności; inne właściwe dokumenty lub zapisy]. |
| | **CA-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za opracowywanie i wdrażanie planu i etapów działania; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-05-Test** | [WYBÓR SPOŚRÓD: Mechanizmy opracowywania, wdrażania i utrzymywania planu działania oraz etapów działania]. |

| | | |
|---|---|---|
| **CA-05(01)** | **PLAN I ETAPY DZIAŁANIA \| AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ/SZCZEGÓŁOWOŚĆ PLANÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-05(01)_ODP** | ***automatyczne mechanizmy służące do zapewnienia dokładności, aktualności i dostępności planu i etapów działania w ramach systemu;*** |
| | **CA-05(01)** | stosuje się ***<mechanizmy automatyczne CA-05(01)_ODP> w*** celu zapewnienia dokładności, aktualności i dostępności planu i etapów działania w ramach systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-05(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; procedury dotyczące planu i etapów działania; dokumentacja projektu systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan i etapy działania; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-05(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za opracowywanie i wdrażanie planu i etapów działania; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-05(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy opracowywania, wdrażania i utrzymywania planu i etapów działania]. |

| | | |
|---|---|---|
| **CA-06** | **AUTORYZACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-06_ODP** | ***określono częstotliwość, z jaką należy aktualizować autoryzacje;*** |
| | **CA-06a.** | jako pracownika funkcyjnego autoryzującego system wyznaczono pracownika funkcyjnego wyższego stopniem; |
| | **CA-06b.** | jako osobę autoryzującą wspólne zabezpieczenia do dziedziczenia przez systemy organizacji wyznaczono pracownika funkcyjnego wyższego stopniem; |
| | **CA-06c.01** | przed rozpoczęciem działań urzędnik autoryzujący system autoryzuje stosowanie wspólnych zabezpieczeń dziedziczonych przez system; |
| | **CA-06c.02** | przed rozpoczęciem działań urzędnik autoryzujący system zezwala na jego działanie; |
| | **CA-06d.** | urzędnik autoryzujący wspólne zabezpieczenia zezwala na użytkowanie zabezpieczeń do dziedziczenia przez systemy organizacyjne; |
| | **CA-06e.** | autoryzacje są aktualizowane z ***<częstotliwością CA-06_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie oceny, autoryzacji i monitorowania; procedury dotyczące autoryzacji; plan bezpieczeństwa systemu; plan ochrony prywatności; raport z oceny; plan i etapy działania; upoważnienie; inne istotne dokumenty lub zapisy]. |
| | **CA-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za autoryzację; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-06-Test** | [WYBÓR SPOŚRÓD: Mechanizmy ułatwiające autoryzację i aktualizacje]. |

| CA-06(01) | AUTORYZACJA \| AUTORYZACJA WSPÓLNA — WEWNĄTRZORGANIZACYJNA | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-06(01)[01]** | w systemie stosuje się wspólny proces autoryzacji. |
| | **CA-06(01)[02]** | Wspólny procesu autoryzacji w systemie obejmuje wielu urzędników z tej samej organizacji, którzy przeprowadzają autoryzację. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-06(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie oceny, autoryzacji i monitorowania; procedury dotyczące autoryzacji; plan bezpieczeństwa systemu; plan ochrony prywatności; raport z oceny; plan i etapy działania; upoważnienie; inne istotne dokumenty lub zapisy]. |
| | **CA-06(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za autoryzację; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-06(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy ułatwiające autoryzację i aktualizacje]. |

| CA-06(02) | AUTORYZACJA \| WSPÓLNA AUTORYZACJA — MIĘDZYORGANIZACYJNA | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-06(02)[01]** | w systemie stosuje się wspólny proces autoryzacji. |
| | **CA-06(02)[02]** | Wspólny procesu autoryzacji w systemie obejmuje wielu autoryzujących urzędników, z co najmniej jednym autoryzującym pracownikiem funkcyjnym z organizacji zewnętrznej w stosunku do organizacji prowadzącej autoryzację. |

| | | |
|---|---|---|
| **CA-06(02)** | **AUTORYZACJA \| WSPÓLNA AUTORYZACJA — MIĘDZYORGANIZACYJNA** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-06(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie oceny, autoryzacji i monitorowania; procedury dotyczące autoryzacji; plan bezpieczeństwa systemu; plan ochrony prywatności; raport z oceny; plan i etapy działania; upoważnienie; inne istotne dokumenty lub zapisy]. |
| | **CA-06(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za autoryzację; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-06(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy ułatwiające autoryzację i aktualizacje]. |

| | | |
|---|---|---|
| **CA-07** | **CIĄGŁE MONITOROWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-07_ODP[01]** | ***określono metryki na poziomie systemu, które mają być monitorowane;*** |
| | **CA-07_ODP[02]** | ***określono częstotliwość monitorowania skuteczności zabezpieczeń;*** |
| | **CA-07_ODP[03]** | ***określono częstotliwość oceny skuteczności zabezpieczeń;*** |
| | **CA-07_ODP[04]** | ***określono personel lub role, którym raportuje się stan bezpieczeństwa systemu;*** |
| | **CA-07_ODP[05]** | ***określono częstotliwość, z jaką raportuje się stan bezpieczeństwa systemu;*** |
| | **CA-07_ODP[06]** | ***określono personel lub role, którym raportuje się stan ochrony prywatności systemu;*** |

| CA-07 | CIĄGŁE MONITOROWANIE | |
|---|---|---|
| | **CA-07_ODP[07]** | ***określono częstotliwość, z jaką raportuje się stan ochrony prywatności systemu;*** |
| | **CA-07[01]** | opracowano strategię ciągłego monitorowania na poziomie systemu; |
| | **CA-07[02]** | ciągłe monitorowanie na poziomie systemu jest realizowane zgodnie ze strategią ciągłego monitorowania na poziomie organizacji; |
| | **CA-07a.** | ciągłe monitorowanie na poziomie systemu obejmuje ustanowienie następujących metryk systemowych, które mają być monitorowane: ***<metryki na poziomie systemu CA-07_ODP[01]>***; |
| | **CA-07b.[01]** | ciągłe monitorowanie na poziomie systemu obejmuje ustalone ***<częstotliwości CA-07_ODP[02]> w*** zakresie monitorowania; |
| | **CA-07b.[02]** | ciągłe monitorowanie na poziomie systemu obejmuje ustalone ***<częstotliwości CA-07_ODP[02]> w*** zakresie oceny skuteczności zabezpieczeń; |
| | **CA-07c.** | ciągłe monitorowanie na poziomie systemu obejmuje bieżące oceny zabezpieczeń zgodnie ze strategią ciągłego monitorowania; |
| | **CA-07d.** | ciągłe monitorowanie na poziomie systemu obejmuje bieżące monitorowanie metryk zdefiniowanych przez system i organizację zgodnie ze strategią ciągłego monitorowania; |
| | **CA-07e.** | ciągłe monitorowanie na poziomie systemu obejmuje korelację i analizę informacji generowanych w ramach oceny i monitorowania zabezpieczeń; |
| | **CA-07f.** | ciągłe monitorowanie na poziomie systemu obejmuje działania w zakresie reagowania na wyniki analizy oceny zabezpieczeń i informacji dotyczących monitorowania; |
| | **CA-07g.[01]** | ciągłe monitorowanie na poziomie systemu obejmuje raportowanie stanu bezpieczeństwa systemu do ***<CA-07_ODP[04] personelu lub ról>*** z ***<częstotliwością CA-07_ODP[05]>***; |

| | | |
|---|---|---|
| **CA-07** | **CIĄGŁE MONITOROWANIE** | |
| | **CA-07g.[02]** | ciągłe monitorowanie na poziomie systemu obejmuje raportowanie stanu prywatności systemu do ***<CA-07_ODP[06] personelu lub ról>*** z ***<częstotliwością CA-07_ODP[07]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; strategia ciągłego monitorowania organizacji; strategia ciągłego monitorowania na poziomie systemu; procedury dotyczące ciągłego monitorowania zabezpieczeń systemu; procedury dotyczące zarządzania konfiguracją; raport z oceny zabezpieczeń ; plan i etapy działania; zapisy dotyczące monitorowania systemu; zapisy dotyczące zarządzania konfiguracją; analizy wpływu; raporty o stanie; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ciągłe monitorowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci]. |
| | **CA-07-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające ciągłe monitorowanie; mechanizmy wspierające reakcję na wyniki oceny i monitorowania; mechanizmy wspierające raportowanie o stanie bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **CA-07(01)** | **CIĄGŁE MONITOROWANIE \| NIEZALEŻNA OCENA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-07(01)** | do bieżącego monitorowania zabezpieczeń w systemie zatrudniono niezależnych oceniających lub zespoły oceniające. |

| | | |
|---|---|---|
| **CA-07(01)** | **CIĄGŁE MONITOROWANIE \| NIEZALEŻNA OCENA** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-07(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; strategia ciągłego monitorowania na poziomie organizacji; strategia ciągłego monitorowania na poziomie systemu; procedury dotyczące ciągłego monitorowania zabezpieczeń systemu; raport z oceny zabezpieczeń; plan i etapy działania; zapisy dotyczące monitorowania systemu; analizy wpływu; sprawozdania; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-07(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ciągłe monitorowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **CA-07(02)** | **CIĄGŁE MONITOROWANIE \| RODZAJE OCEN** | |
| | [WYCOFANE: Włączone do CA-02]. | |

| | | |
|---|---|---|
| **CA-07(03)** | **CIĄGŁE MONITOROWANIE \| ANALIZY TRENDÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-07(03)[01]** | analiza trendów jest stosowana w celu określenia czy wdrożone zabezpieczenia stosowane w procesie ciągłego monitorowania wymagają modyfikacji na podstawie danych empirycznych; |
| | **CA-07(03)[02]** | analiza trendów jest stosowana w celu określenia czy częstotliwość działań w zakresie monitorowania ciągłego wymaga modyfikacji w oparciu o dane empiryczne; |

| | | |
|---|---|---|
| **CA-07(03)** | **CIĄGŁE MONITOROWANIE \| ANALIZY TRENDÓW** | |
| | **CA-07(03)[03]** | analiza trendów jest stosowana w celu określenia czy rodzaje działań stosowanych w procesie ciągłego monitorowania wymagają modyfikacji na podstawie danych empirycznych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-07(03)-Badanie** | [WYBÓR SPOŚRÓD: Strategia ciągłego monitorowania na poziomie organizacji; strategia ciągłego monitorowania na poziomie systemu; polityka oceny, autoryzacji i monitorowania; procedury dotyczące ciągłego monitorowania zabezpieczeń systemu; zabezpieczenia prywatności; sprawozdanie z oceny; plan etapy działania; zapisy z monitorowania systemu; analizy wpływu; raporty o stanie; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-07(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ciągłe monitorowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-07(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające analizy trendów]. |

| | | |
|---|---|---|
| **CA-07(04)** | **CIĄGŁE MONITOROWANIE \| MONITOROWANIE RYZYKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-07(04)** | monitorowanie ryzyka jest integralną częścią strategii ciągłego monitorowania; |
| | **CA-07(04)(a)** | monitorowanie skuteczności jest elementem procesu monitorowania ryzyka; |

| CA-07(04) | CIĄGŁE MONITOROWANIE \| MONITOROWANIE RYZYKA | |
|---|---|---|
| | **CA-07(04)(b)** | monitorowanie zgodności jest elementem procesu monitorowania ryzyka; |
| | **CA-07(04)(c)** | monitorowanie zmian jest elementem procesu monitorowania ryzyka. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-07(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; strategia ciągłego monitorowania na poziomie organizacji; strategia ciągłego monitorowania na poziomie systemu; procedury dotyczące ciągłego monitorowania zabezpieczeń systemu; raport z oceny; plan i etapy działania; zapisy dotyczące monitorowania systemu; analizy wpływu; sprawozdania; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-07(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ciągłe monitorowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-07(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające monitorowanie ryzyka]. |

| CA-07(05) | CIĄGŁE MONITOROWANIE \| ANALIZA SPÓJNOŚCI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-07(05)_ODP[01]** | ***określono działania mające na celu sprawdzenie, czy ustanowiono politykę;*** |
| | **CA-07(05)_ODP[02]** | ***określono działania mające na celu sprawdzenie, czy wdrożone zabezpieczenia działają w sposób spójny;*** |
| | **CA-07(05)[01]** | stosuje się ***<działania CA-07(05)_ODP[01]> w*** celu potwierdzenia, że polityka została ustanowiona; |

| | | |
|---|---|---|
| **CA-07(05)** | **CIĄGŁE MONITOROWANIE \| ANALIZA SPÓJNOŚCI** | |
| | **CA-07(05)[02]** | stosuje się ***<działania CA-07(05)_ODP[02]> w*** celu potwierdzenia, że wdrożone zabezpieczenia działają w sposób spójny; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-07(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; strategia ciągłego monitorowania na poziomie organizacji; strategia ciągłego monitorowania na poziomie systemu; procedury dotyczące ciągłego monitorowania zabezpieczeń systemu; raport z oceny; plan i etapy działania; zapisy z monitorowania systemu; analizy wpływu na bezpieczeństwo; raporty o stanie; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CA-07(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ciągłe monitorowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-07(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające analizy spójności]. |

| | | |
|---|---|---|
| **CA-07(06)** | **CIĄGŁE MONITOROWANIE \| AUTOMATYZACJA WSPARCIA MONITOROWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-07(06)_ODP** | ***określono automatyczne mechanizmy stosowane w celu zapewnienia dokładności, aktualności i dostępności wyników monitorowania systemu;*** |
| | **CA-07(06)** | stosuje się ***<mechanizmy automatyczne CA-07(06)_ODP>*** w celu zapewnienia dokładności, aktualności i dostępności wyników monitorowania systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CA-07(06)** | **CIĄGŁE MONITOROWANIE \| AUTOMATYZACJA WSPARCIA MONITOROWANIA** | |
| | **CA-07(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; strategia ciągłego monitorowania na poziomie organizacji; strategia ciągłego monitorowania na poziomie systemu; procedury dotyczące ciągłego monitorowania zabezpieczeń systemu; raport z oceny; plan i etapy działania; zapisy dotyczące monitorowania systemu; analizy wpływu; sprawozdania; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-07(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ciągłe monitorowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-07(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające automatyczne monitorowanie]. |

| | | |
|---|---|---|
| **CA-08** | **TESTY PENETRACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-08_ODP[01]** | ***określono częstotliwość, z jaką należy przeprowadzać testy penetracyjne systemu lub komponentów systemu;*** |
| | **CA-08_ODP[02]** | ***określono systemy lub komponenty systemu, które mają być poddawane testom penetracyjnym;*** |
| | **CA-08** | testowanie penetracyjne przeprowadza się z ***<częstotliwością CA-08_ODP[01]> na <systemach lub komponentach systemu CA-08_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CA-08** | **TESTY PENETRACYJNE** | |
| | **CA-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; procedury dotyczące testów penetracyjnych; plan oceny; raport z testów penetracyjnych; raport z oceny; dowody oceny; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę zabezpieczeń; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci]. |
| | **CA-08-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające przeprowadzanie testów penetracyjnych]. |

| | | |
|---|---|---|
| **CA-08(01)** | **TESTY PENETRACYJNE \| NIEZALEŻNY TESTER LUB ZESPÓŁ PENETRACYJNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-08(01)** | do wykonania testów penetracyjnych na systemie lub komponentach systemu zatrudniono niezależnego testera lub zespół. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-08(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny, autoryzacji i monitorowania; procedury dotyczące testów penetracyjnych; plan oceny; raport z testów penetracyjnych; raport z oceny; dowody oceny bezpieczeństwa; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-08(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oceny; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **CA-08(02)** | **TESTY PENETRACYJNE \| ĆWICZENIA RED TEAM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-08(02)_ODP** | ***zdefiniowano ćwiczenia typu „red team", symulujące próby włamania do systemów organizacji przez przeciwników;*** |
| | **CA-08(02)** | stosuje się ***<ćwiczenia red team CA-08(02)_ODP> do*** symulacji prób włamania do systemów organizacji przez przeciwników, zgodnie z obowiązującymi zasadami działania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-08(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie oceny, autoryzacji i monitorowania; procedury dotyczące testowania penetracyjnego; procedury dotyczące ćwiczeń red team; plan oceny; wyniki ćwiczeń red team; raport z testowania penetracyjnego; raport z oceny; reguły prowadzenia cyberataku i obrony przed nim; dowody oceny; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-08(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oceny; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci]. |
| | **CA-08(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające stosowanie ćwiczeń red team]. |

| | | |
|---|---|---|
| **CA-08(03)** | **TESTY PENETRACYJNE \| LOKALNE TESTY PENETRACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-08(03)_ODP[01]** | ***określono częstotliwość, z jaką należy stosować testy penetracyjne obejmujące próby ominięcia lub obejścia zabezpieczeń na punktach umożliwiających fizyczny dostęp do obiektu;*** |
| | **CA-08(03)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {zapowiedziane; niezapowiedziane};*** |
| | **CA-08(03)** | procedura testów penetracyjnych obejmuje ***<częstotliwość CA-08(03)_ODP[01]>***.<br>***<WYBRANA WARTOŚĆ PARAMETRU CA-08(03)_ODP[02]>*** prób ominięcia lub<br>obejścia zabezpieczeń na punktach umożliwiających fizyczny dostęp do obiektu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CA-08(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie oceny, autoryzacji i monitorowania; procedury dotyczące testowania penetracyjnego; procedury dotyczące ćwiczeń red team; plan oceny; wyniki ćwiczeń red team; raport z testowania penetracyjnego; raport z oceny; reguły prowadzenia cyberataku i obrony przed nim; dowody oceny; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-08(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oceny; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci]. |
| | **CA-08(03)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspierające realizację ćwiczeń red team]. |

| | | |
|---|---|---|
| **CA-09** | **POŁĄCZENIA WEWNĘTRZSYSTEMOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-09_ODP[01]** | ***określono komponenty systemu lub klasy komponentów wymagające połączeń wewnątrzsystemowych;*** |
| | **CA-09_ODP[02]** | ***określono warunki wymagające zakończenia połączeń wewnątrzsystemowych;*** |
| | **CA-09_ODP[03]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu dalszego zapotrzebowania na każde połączenie wewnątrzsystemowe;*** |
| | **CA-09a.** | połączenia wewnątrzsystemowe ***<komponentów systemu CA-09_ODP[01]> z*** systemem podlegają autoryzacji; |
| | **CA-09b.[01]** | w przypadku każdego połączenia wewnątrzsystemowego dokumentuje się charakterystykę interfejsu; |
| | **CA-09b.[02]** | w przypadku każdego połączenia wewnątrzsystemowego dokumentuje się wymagania bezpieczeństwa; |
| | **CA-09b.[03]** | w przypadku każdego połączenia wewnątrzsystemowego dokumentuje się wymagania dotyczące prywatności; |
| | **CA-09b.[04]** | w przypadku każdego połączenia wewnątrzsystemowego dokumentuje się charakter przekazywanych informacji; |
| | **CA-09c.** | połączenia wewnątrzsystemowe są przerywane w przypadku wystąpienia ***<warunków CA-09_ODP[02]>***; |
| | **CA-09d.** | zapotrzebowanie na każde połączenie wewnątrzsystemowe jest weryfikowane z ***<częstotliwością CA-09_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **CA-09** | **POŁĄCZENIA WEWNĘTRZSYSTEMOWE** | |
|---|---|---|
| | **CA-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie oceny, autoryzacji i monitorowania; polityka kontroli dostępu; procedury dotyczące połączeń systemowych; polityka dotycząca ochrony systemu i komunikacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista komponentów lub klas komponentów zatwierdzonych jako połączenia wewnątrzsystemowe; raport z oceny; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za opracowywanie, wdrażanie i autoryzację połączeń wewnątrzsystemowych; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-09-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające połączenia wewnątrzsystemowe]. |

| **CA-09(01)** | **POŁĄCZENIA WEWNĄTRZSYSTEMOWE\| KONTROLE ZGODNOŚCI** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CA-09(01)[01]** | przed ustanowieniem połączenia wewnątrzsystemowego przeprowadzane są kontrole zgodności z zasadami bezpieczeństwa w odniesieniu do składowych komponentów systemu; |
| | **CA-09(01)[02]** | przed ustanowieniem połączenia wewnątrzsystemowego przeprowadzane są kontrole zgodności z zasadami prywatności w odniesieniu do składowych komponentów systemu; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| CA-09(01) | POŁĄCZENIA WEWNĄTRZSYSTEMOWE\| KONTROLE ZGODNOŚCI | |
|---|---|---|
| | **CA-09(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie oceny, autoryzacji i monitorowania; polityka kontroli dostępu; procedury dotyczące połączeń systemowych; polityka dotycząca ochrony systemu i komunikacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista komponentów lub klas komponentów zatwierdzonych jako połączenia wewnątrzsystemowe; raport z oceny; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CA-09(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za opracowywanie, wdrażanie i autoryzację połączeń wewnątrzsystemowych; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **CA-09(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające kontrole zgodności]. |

## 4.5. KATEGORIA CM - ZARZĄDZANIE KONFIGURACJĄ

| | | |
|---|---|---|
| **CM-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-01_ODP[01]** | ***określono personel lub role, wśród których ma być rozpowszechniana polityka zarządzania konfiguracją;*** |
| | **CM-01_ODP[02]** | ***określono personel lub role, wśród których mają być rozpowszechniane procedury zarządzania konfiguracją;*** |
| | **CM-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **CM-01_ODP[04]** | ***określono pracownika funkcyjnego odpowiedzialnego za zarządzanie polityką i procedurami zarządzania konfiguracją;*** |
| | **CM-01_ODP[05]** | ***określono częstotliwość, z jaką polityka zarządzania konfiguracją jest przeglądana i aktualizowana;*** |
| | **CM-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji polityki zarządzania konfiguracją;*** |
| | **CM-01_ODP[07]** | ***określono częstotliwość przeglądu i aktualizacji procedur zarządzania konfiguracją;*** |
| | **CM-01_ODP[08]** | ***określono zdarzenia skutkujące koniecznością przeprowadzenia procedur zarządzania konfiguracją;*** |
| | **CM-01a.[01]** | opracowano i udokumentowano politykę zarządzania konfiguracją; |
| | **CM-01a.[02]** | polityka zarządzania konfiguracją jest rozpowszechniana wśród ***<personelu lub ról CM-01_ODP[01]>***; |
| | **CM-01a.[03]** | opracowano i udokumentowano procedury zarządzania konfiguracją ułatwiające realizację polityki zarządzania konfiguracją i związanych z nią zabezpieczeń w tym obszarze; |

| **CM-01** | **POLITYKA I PROCEDURY** | |
|---|---|---|
| | **CM-01a.[04]** | procedury zarządzania konfiguracją są rozpowszechniane wśród ***<personelu lub ról CM-01_ODP[02]>***; |
| | **CM-01a.01(a)[01]** | ***<WYBRANA WARTOŚĆ PARAMETRU CM-01_ODP[03]>*** polityki zarządzania konfiguracją odnosi się do celu; |
| | **CM-01a.01(a)[02]** | ***<WYBRANA WARTOŚĆ PARAMETRU CM-01_ODP[03]>*** polityki zarządzania konfiguracją odnosi się do zakresu; |
| | **CM-01a.01(a)[03]** | ***<WYBRANA WARTOŚĆ PARAMETRU CM-01_ODP[03]>*** polityki zarządzania konfiguracją odnosi się do ról; |
| | **CM-01a.01(a)[04]** | ***<WYBRANA WARTOŚĆ PARAMETRU CM-01_ODP[03]>*** polityki zarządzania konfiguracją odnosi się do obowiązków; |
| | **CM-01a.01(a)[05]** | ***<WYBRANA WARTOŚĆ PARAMETRU CM-01_ODP[03]>*** polityki zarządzania konfiguracją odnosi się do zaangażowania kierownictwa; |
| | **CM-01a.01(a)[06]** | ***<WYBRANA WARTOŚĆ PARAMETRU CM-01_ODP[03]>*** polityki zarządzania konfiguracją odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **CM-01a.01(a)[07]** | ***<WYBRANA WARTOŚĆ PARAMETRU CM-01_ODP[03]>*** polityki zarządzania konfiguracją odnosi się do zgodności; |
| | **CM-01a.01(b)** | polityka zarządzania konfiguracją jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **CM-01b.** | ***<urzędnik CM-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur zarządzania konfiguracją; |
| | **CM-01c.01[01]** | aktualna polityka zarządzania konfiguracją jest przeglądana i aktualizowana z ***<częstotliwością CM-01_ODP[05]>***; |
| | **CM-01c.01[02]** | aktualna polityka zarządzania konfiguracją jest przeglądana |

| | | |
|---|---|---|
| **CM-01** | **POLITYKA I PROCEDURY** | |
| | | i aktualizowana po ***<zdarzeniach CM-01_ODP[06]>***; |
| | **CM-01c.02[01]** | aktualne procedury zarządzania konfiguracją są przeglądane i aktualizowane z ***<częstotliwością CM-01_ODP[07]>***; |
| | **CM-01c.02[02]** | aktualne procedury zarządzania konfiguracją są przeglądane i aktualizowane po ***<zdarzeniach CM-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania konfiguracją; polityka i procedury programu bezpieczeństwa i prywatności; wyniki oceny lub audytu; dokumentacja incydentów lub naruszeń bezpieczeństwa; plan bezpieczeństwa systemu; plan ochrony prywatności;<br>strategia zarządzania ryzykiem; inne istotne artefakty, dokumenty lub zapisy]. |
| | **CM-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **CM-02** | **KONFIGURACJA BAZOWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-02_ODP[01]** | ***określono częstotliwość przeglądu i aktualizacji konfiguracji bazowej;*** |
| | **CM-02_ODP[02]** | ***określono okoliczności wymagające przeglądu i aktualizacji konfiguracji bazowej;*** |
| | **CM-02a.[01]** | opracowano i udokumentowano aktualną konfigurację bazową systemu; |

| **CM-02** | **KONFIGURACJA BAZOWA** | |
|---|---|---|
| | **CM-02a.[02]** | w ramach kontroli konfiguracji utrzymywana jest aktualna konfiguracja bazowa systemu; |
| | **CM-02b.01** | konfiguracja bazowa systemu jest przeglądana i aktualizowana z ***<częstotliwością CM-02_ODP[01]>***; |
| | **CM-02b.02** | konfiguracja bazowa systemu jest poddawana przeglądowi i aktualizowana w razie wystąpienia ***<okoliczności CM-02_ODP[02]>***; |
| | **CM-02b.03** | konfiguracja bazowa systemu jest przeglądana i aktualizowana przy instalacji lub modernizacji komponentów systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące konfiguracji bazowej systemu; plan zarządzania konfiguracją; dokumentacja architektury firmowej; dokumentacja projektowa systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja architektury i konfiguracji systemu;<br>ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inwentaryzacja komponentów systemu; zapisy kontroli zmian; inne istotne dokumenty lub zapisy]. |
| | **CM-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci]. |
| | **CM-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zarządzania konfiguracjami bazowymi; mechanizmy wspierające kontrolę konfiguracji bazowych]. |

| **CM-02(01)** | **KONFIGURACJA BAZOWA\| PRZEGLĄDY I AKTUALIZACJE** |
|---|---|
| | [WYCOFANE: Włączone do CM-02]. |

| | | |
|---|---|---|
| **CM-02(02)** | **KONFIGURACJA BAZOWA \| AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ/SZCZEGÓŁOWOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-02(02)_ODP** | ***określono automatyczne mechanizmy utrzymywania bazowej konfiguracji systemu;*** |
| | **CM-02(02)[01]** | w celu zapewnienia aktualności konfiguracji bazowej systemu stosuje się ***<Mechanizmy automatyczne CM-02(02)_ODP>***; |
| | **CM-02(02)[02]** | w celu zapewnienia kompletności konfiguracji bazowej systemu stosuje się ***<Mechanizmy automatyczne CM-02(02)_ODP>***; |
| | **CM-02(02)[03]** | w celu zapewnienia dokładności konfiguracji bazowej systemu stosuje się ***<Mechanizmy automatyczne CM-02(02)_ODP>***; |
| | **CM-02(02)[04]** | w celu zapewnienia dostępności konfiguracji bazowej systemu stosuje się ***<Mechanizmy automatyczne CM-02(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące konfiguracji bazowej systemu; plan zarządzania konfiguracją; dokumentacja projektowa systemu; architektura systemu i dokumentacja konfiguracyjna; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inwentaryzacja komponentów systemu; zapisy kontroli zmian konfiguracyjnych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-02(02)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |

| | | |
|---|---|---|
| **CM-02(03)** | **KONFIGURACJA BAZOWA \| RETENCJA ZACHOWANYCH KONFIGURACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-02(03)_ODP** | ***określono liczbę poprzednich wersji konfiguracji bazowych, które mają być zachowane;*** |
| | **CM-02(03)** | ***<liczba CM-02(03)_ODP>*** poprzednich wersji konfiguracji bazowej systemu jest/będzie zachowana w celu obsługi wycofanych wersji konfiguracji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-02(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące konfiguracji bazowej systemu; plan zarządzania konfiguracją; architektura systemu i dokumentacja konfiguracyjna; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; kopie poprzednich wersji konfiguracji bazowej; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-02(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-02(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania konfiguracjami bazowymi]. |

| | | |
|---|---|---|
| **CM-02(04)** | **KONFIGURACJA BAZOWA\| NIEAUTORYZOWANE OPROGRAMOWANIE** | |
| | [WYCOFANE: Włączone do CM-07(04)]. | |

| | |
|---|---|
| **CM-02(05)** | **KONFIGURACJA BAZOWA\| AUTORYZOWANE OPROGRAMOWANIE** |
| | [WYCOFANE: Włączone do CM-07(05)]. |

| | | |
|---|---|---|
| **CM-02(06)** | **KONFIGURACJA BAZOWA \| ŚRODOWISKA PROGRAMISTYCZNE I TESTOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-02(06)[01]** | utrzymuje się konfigurację bazową dla środowisk programistycznych systemu, która jest zarządzana oddzielnie od podstawowej, operacyjnej konfiguracji bazowej; |
| | **CM-02(06)[02]** | utrzymuje się konfigurację bazową dla środowisk testowych, która jest zarządzana oddzielnie od podstawowej, operacyjnej konfiguracji bazowej; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-02(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące konfiguracji bazowej systemu; plan zarządzania konfiguracją; dokumentacja projektowa systemu; architektura systemu i dokumentacja konfiguracyjna; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-02(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-02(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania konfiguracjami bazowymi; mechanizmy wdrażające odrębne konfiguracje bazowe dla środowisk rozwojowych, testowych i operacyjnych]. |

| | | |
|---|---|---|
| **CM-02(07)** | **KONFIGURACJA BAZOWA \| KONFIGURACJA SYSTEMÓW I KOMPONENTÓW W OBSZARACH WYSOKIEGO RYZYKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-02(07)_ODP[01]** | ***określono systemy lub komponenty systemu przydzielane osobom podróżującym do obszarów wysokiego ryzyka;*** |
| | **CM-02(07)_ODP[02]** | ***określono konfiguracje systemów lub komponentów systemu przydzielanych osobom podróżującym do obszarów wysokiego ryzyka;*** |
| | **CM-02(07)_ODP[03]** | ***określono zabezpieczenia, które mają być stosowane po powrocie osób z podróży;*** |
| | **CM-02(07)(a)** | osobom podróżującym do miejsc uznanych przez organizację za obszary wysokiego ryzyka przydziela się ***<systemy lub elementy systemu CM-02(07)_ODP[01]>*** wraz z ***<konfiguracjami CM-02(07)_ODP[02]>***. |
| | **CM-02(07)(b)** | stosuje się ***<zabezpieczenia CM-02(07)_ODP[03]> w*** systemie lub komponentach systemu, gdy osoby wracają z podróży. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-02(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; plan zarządzania konfiguracją; procedury dotyczące konfiguracji bazowej systemu; procedury dotyczące instalacji i modernizacji komponentów systemu; architektura systemu i dokumentacja konfiguracyjna; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inwentaryzacja komponentów systemu; zapisy przeglądów i aktualizacji konfiguracji bazowej systemu; instalacje/aktualizacje komponentów systemu i związane z nimi zapisy; zapisy kontroli zmian; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-02(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |

| | | |
|---|---|---|
| **CM-02(07)** | **KONFIGURACJA BAZOWA \| KONFIGURACJA SYSTEMÓW I KOMPONENTÓW W OBSZARACH WYSOKIEGO RYZYKA** | |
| | **CM-02(07)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania konfiguracjami bazowymi]. |

| | | |
|---|---|---|
| **CM-03** | **ZABEZPIECZANIE ZMIAN KONFIGURACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-03_ODP[01]** | ***określono okres przechowywania zapisów dotyczących zmian zabezpieczanych konfiguracyjnie;*** |
| | **CM-03_ODP[02]** | ***określono zespół zabezpieczeń zmiany konfiguracji odpowiedzialny za koordynację i nadzorowanie działań związanych z kontrolą zmian;*** |
| | **CM-03_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{<częstotliwość CM-03_ODP[04]>; w przypadku <warunku zmiany konfiguracji CM-03_ODP[05]>};*** |
| | **CM-03_ODP[04]** | ***określono częstotliwość, z jaką zbiera się zespół zabezpieczeń zmiany konfiguracji (jeśli wybrano);*** |
| | **CM-03_ODP[05]** | ***określono warunki zmiany konfiguracji, które wywołują działanie zespołu zabezpieczeń zmiany konfiguracji (jeśli wybrano);*** |
| | **CM-03a.** | określono i udokumentowano rodzaje zmian w systemie, które są zabezpieczone konfiguracyjnie; |
| | **CM-03b.[01]** | dokonuje się przeglądu zmian w systemie, które są zabezpieczone konfiguracyjnie; |
| | **CM-03b.[02]** | proponowane zabezpieczone konfiguracyjnie zmiany w systemie są zatwierdzane lub odrzucane z wyraźnym uwzględnieniem analiz wpływu na bezpieczeństwo i prywatność; |

| | | |
|---|---|---|
| **CM-03** | **ZABEZPIECZANIE ZMIAN KONFIGURACJI** | |
| | **CM-03c.** | dokumentuje się decyzje o zmianie konfiguracji związane z systemem; |
| | **CM-03d.** | dokonuje się wdrożenia zatwierdzonych zmian w systemie, które są zabezpieczone konfiguracyjnie; |
| | **CM-03e.** | zapisy dot. zmian w systemie, które są zabezpieczone konfiguracyjnie, są przechowywane przez ***<okres CM-03_ODP[01]>***; |
| | **CM-03f.[01]** | monitoruje się czynności dot. zmian w systemie, które są zabezpieczone konfiguracyjnie; |
| | **CM-03f.[02]** | dokonuje się przeglądu czynności dot. zmian w systemie, które są zabezpieczone konfiguracyjnie; |
| | **CM-03g.[01]** | czynności dot. zmian w systemie, które są zabezpieczone konfiguracyjnie, są koordynowane i nadzorowane przez ***<zespół zabezpieczeń zmiany konfiguracji CM-03_ODP[02]>***; |
| | **CM-03g.[02]** | zespół zabezpieczeń zmiany konfiguracji wywołuje ***<WYBRANA WARTOŚĆ PARAMETRU CM-03_ODP[03]>*.** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian konfiguracji systemu; plan zarządzania konfiguracją; architektura systemu i dokumentacja konfiguracyjna; zapisy dotyczące zabezpieczania zmian; zapisy z audytu systemu; audyty i przeglądy kontroli zmian; porządki obrad/protokoły/dokumentacja z posiedzeń nadzorczych dotyczących zabezpieczania zmian konfiguracji; plan bezpieczeństwa systemu; plan ochrony prywatności; oceny wpływu na prywatność; zawiadomienia dot. systemu zapisów; inne istotne dokumenty lub zapisy]. |

| **CM-03** | **ZABEZPIECZANIE ZMIAN KONFIGURACJI** | |
|---|---|---|
| | **CM-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę zmian konfiguracyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci; członkowie zespołu kontroli konfiguracji lub podobnych]. |
| | **CM-03-Test** | [WYBÓR SPOŚRÓD: Organizacyjne procesy zabezpieczania zmian konfiguracji; mechanizmy wdrażające zabezpieczanie zmian konfiguracji]. |

| **CM-03(01)** | **ZABEZPIECZENIE ZMIAN KONFIGURACJI \| AUTOMATYCZNA DOKUMENTACJA/POWIADAMIANIE/ZAKAZ WPROWADZANIA ZMIAN** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-03(01)_ODP[01]** | ***określono mechanizmy wykorzystywane do automatyzacji zabezpieczania zmian konfiguracji;*** |
| | **CM-03(01)_ODP[02]** | ***określono organy zatwierdzające, które mają być powiadamiane o proponowanych zmianach w systemie i wnioskować o ich zatwierdzenie;*** |
| | **CM-03(01)_ODP[03]** | ***określono okres, po którym należy wskazać zmiany, które nie zostały zatwierdzone lub odrzucone;*** |
| | **CM-03(01)_ODP[04]** | ***określono personel, który ma być powiadamiany o zakończeniu wprowadzania zatwierdzonych zmian;*** |
| | **CM-03(01)(a)** | stosuje się ***<mechanizmy automatyczne CM-03(01)_ODP[01]> w*** celu udokumentowania proponowanych zmian w systemie; |
| | **CM-03(01)(b)** | ***<Mechanizmy automatyczne CM-03(01)_ODP[01]>*** są używane do powiadamiania ***<personelu ds. zatwierdzania CM-03(01)_ODP[02]> o*** proponowanych zmianach w systemie i żądania zatwierdzenia zmian; |

| | | |
|---|---|---|
| **CM-03(01)** | **ZABEZPIECZENIE ZMIAN KONFIGURACJI \| AUTOMATYCZNA DOKUMENTACJA/POWIADAMIANIE/ZAKAZ WPROWADZANIA ZMIAN** | |
| | **CM-03(01)(c)** | stosuje się ***<automatyczne mechanizmy CM-03(01)_ODP[01]>*** ***do*** zaznaczania proponowanych zmian w systemie, które nie zostały zatwierdzone lub odrzucone w ***<okresie CM-03(01)_ODP[03]>***; |
| | **CM-03(01)(d)** | stosuje się ***<mechanizmy automatyczne CM-03(01)_ODP[01]> w*** celu zakazania wprowadzania zmian w systemie do czasu otrzymania zatwierdzenia; |
| | **CM-03(01)(e)** | stosuje się ***<mechanizmy automatyczne CM-03(01)_ODP[01]> w*** celu dokumentowania wszelkich zmian w systemie; |
| | **CM-03(01)(f)** | ***<Mechanizmy automatyczne CM-03(01)_ODP[01]>*** są używane do powiadamiania ***<personelu CM-03(01)_ODP[04]>*** ***po*** zakończeniu wprowadzania zatwierdzonych zmian w systemie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian w konfiguracji systemu; plan zarządzania konfiguracją; dokumentacja projektowa systemu; dokumentacja architektury i konfiguracji systemu; automatyczne mechanizmy zabezpieczania konfiguracji; ustawienia konfiguracji systemu i związana z nimi dokumentacja; zapisy kontroli zmian; zapisy audytu systemu; wnioski o zatwierdzenie zmian; zatwierdzenia zmian; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczanie zmian w konfiguracji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; członkowie zespołu kontroli konfiguracji lub podobnego organu]. |

| | | |
|---|---|---|
| **CM-03(01)** | **ZABEZPIECZENIE ZMIAN KONFIGURACJI \| AUTOMATYCZNA DOKUMENTACJA/POWIADAMIANIE/ZAKAZ WPROWADZANIA ZMIAN** | |
| | **CM-03(01)-Test** | [WYBÓR SPOŚRÓD: Organizacyjne procesy zabezpieczania zmian konfiguracji; mechanizmy wdrażające działania w zakresie zabezpieczania zmian konfiguracji]. |

| | | |
|---|---|---|
| **CM-03(02)** | **ZABEZPIECZANIE ZMIAN KONFIGURACJI \| TESTOWANIE, WALIDACJA I DOKUMENTACJA ZMIAN** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-03(02)[01]** | zmiany w systemie są testowane przed zakończeniem wdrażania zmian; |
| | **CM-03(02)[02]** | zmiany w systemie są zatwierdzane przed zakończeniem wdrażania zmian; |
| | **CM-03(02)[03]** | zmiany w systemie są dokumentowane przed zakończeniem wdrażania zmian; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; plan zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian konfiguracji systemu; dokumentacja projektowa systemu; dokumentacja architektury i konfiguracji systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy testów; zapisy walidacji; zapisy zabezpieczania zmian; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-03(02)** | **ZABEZPIECZANIE ZMIAN KONFIGURACJI \| TESTOWANIE, WALIDACJA I DOKUMENTACJA ZMIAN** | |
| | **CM-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczanie zmian w konfiguracji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; członkowie zespołu kontroli konfiguracji lub podobnego organu]. |
| | **CM-03(02)-Test** | [WYBÓR SPOŚRÓD: Organizacyjne procesy zabezpieczania zmian konfiguracyjnych; mechanizmy wspierające lub wdrażające, testujące, walidujące i dokumentujące zmiany w systemie]. |

| | | |
|---|---|---|
| **CM-03(03)** | **ZABEZPIECZANIE ZMIAN KONFIGURACJI \| AUTOMATYCZNE WPROWADZANIE ZMIAN** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-03(03)_ODP** | ***określono mechanizmy służące do automatyzacji wdrażania zmian oraz zaktualizowanej konfiguracji bazowej w zainstalowanej bazie;*** |
| | **CM-03(03)[01]** | zmiany w stosunku do aktualnej konfiguracji bazowej są wdrażane przy użyciu ***<mechanizmów automatycznych CM-03(03)_ODP>;*** |
| | **CM-03(03)[02]** | uaktualniona konfiguracja bazowa jest wdrażana w całej bazie przy użyciu ***<mechanizmów automatycznych CM-03(03)_ODP>;*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CM-03(03)** | **ZABEZPIECZANIE ZMIAN KONFIGURACJI \| AUTOMATYCZNE WPROWADZANIE ZMIAN** | |
| | **CM-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; plan zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian konfiguracji systemu; dokumentacja projektowa systemu; dokumentacja architektury i konfiguracji systemu; automatyczne mechanizmy zabezpieczania konfiguracji; zapisy kontroli zmian; inwentaryzacja komponentów systemu; zapisy audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczanie zmian w konfiguracji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; członkowie zespołu kontroli konfiguracji lub podobnego organu]. |
| | **CM-03(03)-Test** | [WYBÓR SPOŚRÓD: Organizacyjne procesy zabezpieczania zmian w konfiguracji; mechanizmy wdrażające zmiany w aktualnej konfiguracji bazowej systemu]. |

| | | |
|---|---|---|
| **CM-03(04)** | **ZABEZPIECZENIE ZMIAN KONFIGURACJI \| FUNKCYJNI DS. BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-03(04)_ODP[01]** | ***określono urzędników ds. bezpieczeństwa, którzy muszą być członkami zespołu zabezpieczeń zmiany konfiguracji;*** |
| | **CM-03(04)_ODP[02]** | ***określono urzędników ds. prywatności, którzy muszą być członkami zespołu zabezpieczeń zmiany konfiguracji;*** |
| | **CM-03(04)_ODP[03]** | ***określono zespół zabezpieczeń zmiany konfiguracji, którego członkami mają być urzędnicy ds. bezpieczeństwa i prywatności;*** |

| | | |
|---|---|---|
| **CM-03(04)** | **ZABEZPIECZENIE ZMIAN KONFIGURACJI \| FUNKCYJNI DS. BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **CM-03(04)[01]** | ***<urzędnicy ds. bezpieczeństwa CM-03(04)_ODP[01]>*** muszą być członkami ***<zespołu zabezpieczeń zmiany konfiguracji CM-03(04)_ODP[03]>***; |
| | **CM-03(04)[02]** | ***<urzędnicy ds. prywatności CM-03(04)_ODP[02]>*** muszą być członkami ***<zespołu zabezpieczeń zmiany konfiguracji CM-03(04)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-03(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian konfiguracji systemu; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CM-03(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolowanie zmian w konfiguracji; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu; członkowie zespołu kontroli konfiguracji lub podobnego organu]. |
| | **CM-03(04)-Test** | [WYBÓR SPOŚRÓD: Organizacyjne procesy zabezpieczania zmian konfiguracji]. |

| | | |
|---|---|---|
| **CM-03(05)** | **KONTROLA ZMIAN W KONFIGURACJI \| AUTOMATYCZNA REAKCJA BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-03(05)_ODP** | ***określono reakcje bezpieczeństwa, które mają następować automatycznie;*** |

| | | |
|---|---|---|
| **CM-03(05)** | **KONTROLA ZMIAN W KONFIGURACJI \| AUTOMATYCZNA REAKCJA BEZPIECZEŃSTWA** | |
| | **CM-03(05)** | ***<reakcje bezpieczeństwa CM-03(05)_ODP>*** następują automatycznie, jeśli konfiguracja bazowa zostanie zmieniona w nieautoryzowany sposób. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-03(05)-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian konfiguracji systemu; plan zarządzania konfiguracją; dokumentacja projektowa systemu; architektura systemu i dokumentacja konfiguracyjna; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; alerty/powiadomienia o nieautoryzowanych zmianach konfiguracji bazowej; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-03(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczanie zmian w konfiguracji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; członkowie zespołu kontroli konfiguracji lub podobnego organu]. |
| | **CM-03(05)-Test** | [WYBÓR SPOŚRÓD: Organizacyjne procesy zabezpieczania zmian konfiguracji; automatyczne mechanizmy wdrażające reakcje bezpieczeństwa na nieautoryzowane zmiany konfiguracji bazowej]. |

| | | |
|---|---|---|
| **CM-03(06)** | **ZABEZPIECZENIE ZMIAN KONFIGURACJI \| ZARZĄDZANIE KRYPTOGRAFICZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-03(06)_ODP** | ***określono zabezpieczenia zapewniane przez mechanizmy kryptograficzne, które mają być objęte procesem zarządzania konfiguracją;*** |

| **CM-03(06)** | **ZABEZPIECZENIE ZMIAN KONFIGURACJI \| ZARZĄDZANIE KRYPTOGRAFICZNE** | |
|---|---|---|
| | **CM-03(06)** | Mechanizmy kryptograficzne używane do zapewnienia ***<zabezpieczeń CM-03(06)_ODP>*** są objęte procesem zarządzania konfiguracją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-03(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian konfiguracji systemu; plan zarządzania konfiguracją; dokumentacja projektowa systemu; architektura systemu i dokumentacja konfiguracyjna; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-03(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczanie zmian w konfiguracji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; członkowie zespołu kontroli konfiguracji lub podobnego organu]. |
| | **CM-03(06)-Test** | [WYBÓR SPOŚRÓD: Organizacyjne zabezpieczania zmian konfiguracji; mechanizmy kryptograficzne wdrażające organizacyjne zabezpieczenia]. |

| **CM-03(07)** | **ZABEZPIECZANIE ZMIAN KONFIGURACJI \| PRZEGLĄD ZMIAN W SYSTEMIE** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-03(07)_ODP[01]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu zmian;*** |
| | **CM-03(07)_ODP[02]** | ***określono okoliczności, w których należy dokonywać przeglądu zmian;*** |

| | | |
|---|---|---|
| **CM-03(07)** | **ZABEZPIECZANIE ZMIAN KONFIGURACJI \| PRZEGLĄD ZMIAN W SYSTEMIE** | |
| | **CM-03(07)** | zmiany w systemie są przeglądane z ***<częstotliwością CM-03(07)_ODP[01]> lub w*** przypadku wystąpienia ***<okoliczności CM-03(07)_ODP[02]> w*** celu określenia, doszło do nieautoryzowanych zmian. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-03(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian konfiguracji systemu; plan zarządzania konfiguracją; zapisy dotyczące zabezpieczania zmian; dokumentacja dotycząca architektury i konfiguracji systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>zapisy z audytu systemu; inwentaryzacja komponentów systemu; plan bezpieczeństwa systemu; inne stosowne dokumenty lub zapisy]. |
| | **CM-03(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczanie zmian konfiguracyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo; administratorzy systemu/sieci; członkowie zespołu kontroli konfiguracji lub podobnego organu]. |
| | **CM-03(07)-Test** | [WYBÓR SPOŚRÓD: Organizacyjne procesy zabezpieczania zmian konfiguracyjnych; mechanizmy wdrażające sporządzanie zapisów audytowych dotyczących zmian]. |

| | | |
|---|---|---|
| **CM-03(08)** | **ZABEZPIECZANIE ZMIAN KONFIGURACJI \| ZAPOBIEGANIE ZMIANOM W KONFIGURACJI LUB ICH OGRANICZANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-03(08)_ODP** | ***określono okoliczności, w których należy zapobiegać zmianom lub je ograniczać;*** |

| | | |
|---|---|---|
| **CM-03(08)** | **ZABEZPIECZANIE ZMIAN KONFIGURACJI \| ZAPOBIEGANIE ZMIANOM W KONFIGURACJI LUB ICH OGRANICZANIE** | |
| | **CM-03(08)** | wdrożenie zmian w konfiguracji systemu jest uniemożliwione lub ograniczone w przypadku ***<okoliczności CM-03(08)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-03(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian w konfiguracji systemu; plan zarządzania konfiguracją; zapisy dotyczące zabezpieczania zmian; dokumentacja dotycząca architektury i konfiguracji systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inwentaryzacja komponentów systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-04** | **ANALIZY WPŁYWU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-04[01]** | zmiany w systemie są analizowane w celu określenia potencjalnego wpływu na bezpieczeństwo przed ich wdrożeniem; |
| | **CM-04[02]** | zmiany w systemie są analizowane w celu określenia potencjalnego wpływu na prywatność przed ich wdrożeniem; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| CM-04 | ANALIZY WPŁYWU | |
|---|---|---|
| | **CM-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące analiz wpływu na bezpieczeństwo w przypadku zmian w systemie; procedury dotyczące analiz wpływu na prywatność w przypadku zmian w systemie; plan zarządzania konfiguracją; dokumentacja dotycząca analizy wpływu na bezpieczeństwo; dokumentacja dotycząca analizy wpływu na prywatność; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka w zakresie prywatności, dokumentacja projektowa systemu; narzędzia analizy i związane z nimi dane wyjściowe; zapisy dotyczące zabezpieczania zmian; zapisy dotyczące audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CM-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przeprowadzanie analiz wpływu na bezpieczeństwo; personel organizacyjny odpowiedzialny za przeprowadzanie analiz wpływu na prywatność; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu; administratorzy systemu/sieci; członkowie zespołu kontroli konfiguracji lub podobnego organu]. |
| | **CM-04-Test** | [WYBÓR SPOŚRÓD: Organizacyjne procesy dotyczące analiz wpływu na bezpieczeństwo; organizacyjne procesy dotyczące analiz wpływu na prywatność]. |

| CM-04(01) | ANALIZY WPŁYWU \| ODDZIELNE ŚRODOWISKA TESTOWE | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-04(01)[01]** | zmiany do wdrożenia w systemie są analizowane w oddzielnym środowisku testowym przed wdrożeniem w środowisku operacyjnym; |

| | | |
|---|---|---|
| **CM-04(01)** | **ANALIZY WPŁYWU \| ODDZIELNE ŚRODOWISKA TESTOWE** | |
| | **CM-04(01)[02]** | zmiany w systemie są analizowane pod kątem wpływu na bezpieczeństwo na skutek istnienia wad; |
| | **CM-04(01)[03]** | zmiany w systemie są analizowane pod kątem wpływu na prywatność na skutek istnienia wad; |
| | **CM-04(01)[04]** | zmiany w systemie są analizowane pod kątem wpływu na bezpieczeństwo na skutek istnienia słabych punktów; |
| | **CM-04(01)[05]** | zmiany w systemie są analizowane pod kątem wpływu na prywatność na skutek istnienia słabych punktów; |
| | **CM-04(01)[06]** | zmiany w systemie są analizowane pod kątem wpływu na bezpieczeństwo na skutek istnienia niekompatybilności; |
| | **CM-04(01)[07]** | zmiany w systemie są analizowane pod kątem wpływu na prywatność na skutek istnienia niekompatybilności; |
| | **CM-04(01)[08]** | zmiany w systemie są analizowane pod kątem wpływu na bezpieczeństwo na skutek celowego złośliwego działania; |
| | **CM-04(01)[09]** | zmiany w systemie są analizowane pod kątem wpływu na prywatność na skutek celowego złośliwego działania; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| CM-04(01) | ANALIZY WPŁYWU \| ODDZIELNE ŚRODOWISKA TESTOWE | |
|---|---|---|
| | **CM-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące analiz wpływu na bezpieczeństwo w przypadku zmian w systemie; procedury dotyczące analiz wpływu na prywatność w przypadku zmian w systemie; plan zarządzania konfiguracją; dokumentacja dotycząca analizy wpływu na bezpieczeństwo; dokumentacja dotycząca analizy wpływu na prywatność; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka związanego z prywatnością; narzędzia analizy i związane z nimi dane wyjściowe dokumentacja projektowa systemu; dokumentacja dotycząca architektury i konfiguracji systemu; zapisy dotyczące zabezpieczania zmian; procedury dotyczące uprawnień do przeprowadzania testów z wykorzystaniem danych identyfikacyjnych; zapisy dotyczące audytu systemu; dokumentacja dotycząca oddzielnych środowisk testowych i operacyjnych; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CM-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przeprowadzanie analiz wpływu na bezpieczeństwo i prywatność; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci; członkowie zespołu kontroli konfiguracji lub podobnego organu]. |
| | **CM-04(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące analiz w zakresie wpływu na bezpieczeństwo i prywatność; mechanizmy wspierające lub wdrażające analizy wpływu zmian na bezpieczeństwo i prywatność]. |

| | | |
|---|---|---|
| **CM-04(02)** | **ANALIZY WPŁYWU \| WERYFIKACJA ZABEZPIECZEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-04(02)[01]** | zmienione zabezpieczenia są wdrożone prawidłowo i spełniają określone wymagania bezpieczeństwa obowiązujące po zmianach systemu; |
| | **CM-04(02)[02]** | zmienione zabezpieczenia są wdrożone prawidłowo i spełniają określone wymagania prywatności obowiązujące po zmianach systemu; |
| | **CM-04(02)[03]** | zmienione zabezpieczenia funkcjonują prawidłowo i spełniają określone wymagania bezpieczeństwa obowiązujące po zmianach systemu; |
| | **CM-04(02)[04]** | zmienione zabezpieczenia funkcjonują prawidłowo i spełniają określone wymagania prywatności obowiązujące po zmianach systemu; |
| | **CM-04(02)[05]** | zmienione zabezpieczenia przynoszą oczekiwane skutki i spełniają określone wymagania bezpieczeństwa obowiązujące po zmianach systemu; |
| | **CM-04(02)[06]** | zmienione zabezpieczenia przynoszą oczekiwane skutki i spełniają określone wymagania prywatności obowiązujące po zmianach systemu; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-04(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące analiz wpływu na bezpieczeństwo w przypadku zmian w systemie; procedury dotyczące analiz wpływu na prywatność w przypadku zmian w systemie; dokumentacja oceny ryzyka w zakresie prywatności; plan zarządzania konfiguracją; dokumentacja dotycząca analizy wpływu na bezpieczeństwo i prywatność; ocena wpływu na prywatność; narzędzia analizy i związane z nimi dane wyjściowe;<br>zapisy dotyczące zabezpieczania zmian; inwentaryzacja komponentów systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne właściwe dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-04(02)** | **ANALIZY WPŁYWU \| WERYFIKACJA ZABEZPIECZEŃ** | |
| | **CM-04(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przeprowadzanie analiz wpływu na bezpieczeństwo i prywatność; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci; osoby oceniające bezpieczeństwo i prywatność]. |
| | **CM-04(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące analiz w zakresie wpływu na bezpieczeństwo i prywatność; mechanizmy wspierające lub wdrażające analizy wpływu zmian na bezpieczeństwo i prywatność]. |

| | | |
|---|---|---|
| **CM-05** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-05[01]** | zdefiniowano i udokumentowano fizyczne ograniczenia dostępu związane ze zmianami w systemie; |
| | **CM-05[02]** | zatwierdzono fizyczne ograniczenia dostępu związane ze zmianami w systemie; |
| | **CM-05[03]** | egzekwuje się stosowanie fizycznych ograniczeń dostępu związanych ze zmianami w systemie; |
| | **CM-05[04]** | zdefiniowano i udokumentowano logiczne ograniczenia dostępu związane ze zmianami w systemie; |
| | **CM-05[05]** | zatwierdzono logiczne ograniczenia dostępu związane ze zmianami w systemie; |
| | **CM-05[06]** | egzekwuje się stosowanie logicznych ograniczeń dostępu związanych ze zmianami w systemie; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CM-05** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN** | |
| | **CM-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące ograniczeń w dostępie do zmian w systemie; plan zarządzania konfiguracją; dokumentacja projektowa systemu; dokumentacja architektury i konfiguracji systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zatwierdzenia dostępu logicznego; zatwierdzenia dostępu fizycznego; poświadczenia dostępu; zapisy dotyczące zabezpieczania zmian; zapisy audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za logiczną kontrolę dostępu; personel organizacyjny odpowiedzialny za fizyczną kontrolę dostępu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-05-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania ograniczeniami dostępu do zmian; mechanizmy wspierające, wdrażające lub egzekwujące ograniczenia dostępu związane ze zmianami w systemie]. |

| | | |
|---|---|---|
| **CM-05(01)** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN \| AUTOMATYCZNE EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU I ZAPISY Z AUDYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-05(01)_ODP** | ***określono mechanizmy wykorzystywane do automatyzacji egzekwowania ograniczeń dostępu;*** |
| | **CM-05(01)(a)** | ograniczenia dostępu do zmian są egzekwowane przy użyciu ***<mechanizmów automatycznych CM-05(01)_ODP>***; |
| | **CM-05(01)(b)** | zapisy z audytu dotyczące czynności w zakresie egzekwowania są generowane automatycznie. |

| | | |
|---|---|---|
| **CM-05(01)** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN \| AUTOMATYCZNE EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU I ZAPISY Z AUDYTU** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-05(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące ograniczania dostępu do zmian w systemie; dokumentacja projektowa systemu; architektura systemu i dokumentacja konfiguracyjna; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy kontroli zmian; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-05(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za logiczną kontrolę dostępu; personel organizacyjny odpowiedzialny za fizyczną kontrolę dostępu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-05(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania ograniczeniami dostępu do zmian; automatyczne mechanizmy egzekwujące ograniczenia dostępu do zmian w systemie; automatyczne mechanizmy wspierające audyt działań w zakresie egzekwowania ograniczeń dostępu]. |

| | |
|---|---|
| **CM-05(02)** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN \| PODPISANE KOMPONENTY** |
| | [WYCOFANE: Włączone do CM-03(07)]. |

| | |
|---|---|
| **CM-05(03)** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN \| PODPISYWANIE KOMPONENTÓW** |
| | [WYCOFANE: Włączone do CM-14]. |

| | | |
|---|---|---|
| **CM-05(04)** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIANY \| PODWÓJNA AUTORYZACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-05(04)_ODP[01]** | ***określono komponenty systemu wymagające podwójnej autoryzacji przy wprowadzaniu zmian;*** |
| | **CM-05(04)_ODP[02]** | ***określono informacje systemowe wymagające podwójnej autoryzacji przy wprowadzaniu zmian;*** |
| | **CM-05(04)[01]** | stosuje się podwójną autoryzację przy wdrażaniu zmian w ***<komponentach systemu CM-05(04)_ODP[01]>***. |
| | **CM-05(04)[02]** | stosuje się podwójną autoryzację przy wdrażaniu zmian w ***<informacjach systemowych CM-05(04)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-05(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące ograniczania dostępu do zmian w systemie; plan zarządzania konfiguracją; dokumentacja projektowa systemu; dokumentacja architektury i konfiguracji systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące zabezpieczania zmian; zapisy z audytu systemu; inwentaryzacja komponentów systemu; informacje o typach informacji w systemie; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-05(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za egzekwowanie stosowania podwójnej autoryzacji w zakresie wdrażania zmian w systemie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |

| | | |
|---|---|---|
| **CM-05(04)** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIANY \| PODWÓJNA AUTORYZACJA** | |
| | **CM-05(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania ograniczeniami dostępu do zmian; mechanizmy wdrażające egzekwowanie podwójnej autoryzacji]. |

| | | |
|---|---|---|
| **CM-05(05)** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN \| OGRANICZANIE UPRAWNIEŃ W ZAKRESIE WYTWARZANIA I EKSPLOATACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-05(05)_ODP[01]** | ***Określono częstotliwość, z jaką należy dokonywać przeglądu uprawnień;*** |
| | **CM-05(05)_ODP[02]** | ***Określono częstotliwość, z jaką należy dokonywać ponownej oceny uprawnień;*** |
| | **CM-05(05)(a)[01]** | uprawnienia do zmiany komponentów systemu w środowisku produkcyjnym lub operacyjnym są ograniczone; |
| | **CM-05(05)(a)[02]** | uprawnienia do zmiany informacji związanych z systemem w środowisku produkcyjnym lub operacyjnym są ograniczone; |
| | **CM-05(05)(b)[01]** | uprawnienia są weryfikowane z ***<częstotliwością CM-05(05)_ODP[01]>***; |
| | **CM-05(05)(b)[02]** | uprawnienia są ponownie oceniane z ***<częstotliwością CM-05(05)_ODP[02]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CM-05(05)** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN \| OGRANICZANIE UPRAWNIEŃ W ZAKRESIE WYTWARZANIA I EKSPLOATACJI** | |
| | **CM-05(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące ograniczania dostępu do zmian w systemie; plan zarządzania konfiguracją; dokumentacja projektowa systemu; dokumentacja architektury i konfiguracji systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; przeglądy uprawnień użytkowników; ponowna ocena uprawnień użytkowników; inwentaryzacja komponentów systemu; zapisy dotyczące zabezpieczania zmian; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-05(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-05(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania ograniczeniami możliwości dokonywania zmian; mechanizmy wspierające lub wdrażające ograniczenia możliwości dokonywania zmian]. |

| | | |
|---|---|---|
| **CM-05(06)** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN \| OGRANICZENIE UPRAWNIEŃ W BIBLIOTEKACH OPROGRAMOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-05(06)** | uprawnienia do zmiany oprogramowania znajdującego się w bibliotekach oprogramowania są ograniczone. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CM-05(06)** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN \| OGRANICZENIE UPRAWNIEŃ W BIBLIOTEKACH OPROGRAMOWANIA** | |
| | **CM-05(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące ograniczania dostępu do zmian w systemie; plan zarządzania konfiguracją; dokumentacja projektowa systemu; dokumentacja architektury i konfiguracji systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inwentaryzacja komponentów systemu; zapisy dotyczące zabezpieczania zmian; zapisy audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-05(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-05(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania ograniczeniami możliwości dokonywania zmian; mechanizmy wspierające lub wdrażające ograniczenia możliwości dokonywania zmian]. |

| | | |
|---|---|---|
| **CM-05(07)** | **OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN \| AUTOMATYCZNE WDRAŻANIE ZABEZPIECZEŃ** | |
| | [WYCOFANE: Włączone do SI-07]. | |

| | | |
|---|---|---|
| **CM-06** | **USTAWIENIA KONFIGURACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-06_ODP[01]** | ***określono wspólne, bezpieczne konfiguracje w celu ustalenia i udokumentowania ustawień konfiguracyjnych dla komponentów systemu;*** |

| | | |
|---|---|---|
| **CM-06** | **USTAWIENIA KONFIGURACYJNE** | |
| | **CM-06_ODP[02]** | ***określono elementy systemu, w przypadku których konieczna jest zgoda na odstępstwo;*** |
| | **CM-06_ODP[03]** | ***określono wymagania operacyjne wymagające zatwierdzenia odstępstw;*** |
| | **CM-06a.** | w odniesieniu do komponentów zastosowanych w systemie ustanowiono i udokumentowano najbardziej restrykcyjne ustawienia konfiguracyjne zgodne z wymaganiami operacyjnymi, z zastosowaniem ***<wspólnych bezpiecznych konfiguracji CM-06_ODP[01]>***; |
| | **CM-06b.** | wdrożono ustawienia konfiguracyjne udokumentowane w CM-06a; |
| | **CM-06c.[01]** | wszelkie odstępstwa od ustalonych ustawień konfiguracyjnych ***<komponentów systemu CM-06_ODP[02]>*** są identyfikowane i dokumentowane w oparciu o ***<wymagania operacyjne CM-06_ODP[03]>***; |
| | **CM-06c.[02]** | wszelkie odstępstwa od ustalonych ustawień konfiguracyjnych ***<komponentów systemu CM-06_ODP[02]>*** podlegają zatwierdzeniu; |
| | **CM-06d.[01]** | zmiany ustawień konfiguracyjnych są monitorowane zgodnie z zasadami i procedurami organizacji; |
| | **CM-06d.[02]** | zmiany ustawień konfiguracyjnych są kontrolowane zgodnie z zasadami i procedurami organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **CM-06** | **USTAWIENIA KONFIGURACYJNE** | |
|---|---|---|
| | **CM-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące ustawień konfiguracyjnych systemu; plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wspólne bezpieczne listy kontrolne konfiguracji;<br>inwentaryzacja komponentów systemu; dowody potwierdzające zatwierdzone odstępstwa od ustalonych ustawień konfiguracyjnych; zapisy dotyczące zabezpieczania zmian; zezwolenia na przetwarzanie i przechowywanie danych w systemie; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne stosowne dokumenty lub zapisy]. |
| | **CM-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie konfiguracją bezpieczeństwa; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją prywatności; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci]. |
| | **CM-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zarządzania ustawieniami konfiguracyjnymi; mechanizmy wdrażające, monitorujące lub kontrolujące ustawienia konfiguracyjne systemu; mechanizmy identyfikujące lub dokumentujące odstępstwa od ustalonych ustawień konfiguracyjnych]. |

| **CM-06(01)** | **USTAWIENIA KONFIGURACYJNE \| AUTOMATYCZNE ZARZĄDZANIE, STOSOWANIE I WERYFIKACJA** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-06(01)_ODP[01]** | ***określono komponenty systemu, w przypadku których ma miejsce automatyczne zarządzanie, stosowanie i sprawdzanie ustawienia konfiguracyjnych;*** |

| | | |
|---|---|---|
| **CM-06(01)** | **USTAWIENIA KONFIGURACYJNE \| AUTOMATYCZNE ZARZĄDZANIE, STOSOWANIE I WERYFIKACJA** | |
| | **CM-06(01)_ODP[02]** | ***określono automatyczne mechanizmy zarządzania ustawieniami konfiguracyjnymi;*** |
| | **CM-06(01)_ODP[03]** | ***określono automatyczne mechanizmy stosowania ustawień konfiguracyjnych;*** |
| | **CM-06(01)_ODP[04]** | ***określono automatyczne mechanizmy weryfikacji ustawień konfiguracyjnych;*** |
| | **CM-06(01)[01]** | ustawienia konfiguracyjne***<komponentów systemu CM-06(01)_ODP[01]>*** są zarządzane za pomocą ***<mechanizmów automatycznych CM-06(01)_ODP[02]>***; |
| | **CM-06(01)[02]** | ustawienia konfiguracyjne***<komponentów systemu CM-06(01)_ODP[01]>*** są stosowane za pomocą ***<mechanizmów automatycznych CM-06(01)_ODP[03]>***; |
| | **CM-06(01)[03]** | ustawienia konfiguracyjne***<komponentów systemu CM-06(01)_ODP[01]>*** są weryfikowane za pomocą ***<mechanizmów automatycznych CM-06(01)_ODP[04]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-06(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące ustawień konfiguracyjnych systemu; plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inwentaryzacja komponentów systemu; wspólne bezpieczne listy kontrolne konfiguracji; zapisy dotyczące zabezpieczania zmian; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-06(01)** | **USTAWIENIA KONFIGURACYJNE \| AUTOMATYCZNE ZARZĄDZANIE, STOSOWANIE I WERYFIKACJA** | |
| | **CM-06(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie konfiguracją bezpieczeństwa; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci; programiści systemu]. |
| | **CM-06(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania ustawieniami konfiguracyjnymi; automatyczne mechanizmy zarządzania, stosowania i weryfikacji ustawień konfiguracyjnych systemu]. |

| | | |
|---|---|---|
| **CM-06(02)** | **USTAWIENIA KONFIGURACYJNE \| REAKCJA NA NIEAUTORYZOWANE ZMIANY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-06(02)_ODP[01]** | ***działania, które należy podjąć w przypadku nieautoryzowanej zmiany;*** |
| | **CM-06(02)_ODP[02]** | ***określono ustawienia konfiguracyjne wymagające działania w przypadku nieautoryzowanej zmiany;*** |
| | **CM-06(02)** | podejmowane są***<działania CM-06(02)_ODP[01]> w*** odpowiedzi na nieautoryzowane zmiany w ***<ustawieniach konfiguracyjnych CM-06(02)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CM-06(02)** | **USTAWIENIA KONFIGURACYJNE \| REAKCJA NA NIEAUTORYZOWANE ZMIANY** | |
| | **CM-06(02)-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; plan ochrony prywatności; polityka zarządzania konfiguracją; procedury dotyczące ustawień konfiguracyjnych systemu; plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; alerty/powiadomienia o nieuprawnionych zmianach w ustawieniach konfiguracyjnych systemu;<br>inwentaryzacja komponentów systemu; udokumentowane reakcje na nieautoryzowane zmiany w ustawieniach konfiguracyjnych systemu; zapisy dotyczące zabezpieczania zmian; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-06(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie konfiguracją bezpieczeństwa; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność; administratorzy systemu/sieci]. |
| | **CM-06(02)-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny w zakresie reagowania na nieautoryzowane zmiany w ustawieniach konfiguracyjnych systemu; mechanizmy wspierające lub realizujące działania w odpowiedzi na nieautoryzowane zmiany]. |

| | |
|---|---|
| **CM-06(03)** | **USTAWIENIA KONFIGURACYJNE \| WYKRYWANIE NIEAUTORYZOWANYCH ZMIAN** |
| | [WYCOFANE: Włączone do SI-07]. |

| | |
|---|---|
| **CM-06(04)** | **USTAWIENIA KONFIGURACYJNE \| WYKAZANIE ZGODNOŚCI** |
| | [WYCOFANE: Włączone do CM-04]. |

| | | |
|---|---|---|
| **CM-07** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-07_ODP[01]** | ***określono funkcje systemu, które są niezbędne do realizacji misji organizacji;*** |
| | **CM-07_ODP[02]** | ***określono funkcje, które mają być zakazane lub objęte ograniczeniami;*** |
| | **CM-07_ODP[03]** | ***określono porty, których użytkowanie ma być zakazane lub ograniczone;*** |
| | **CM-07_ODP[04]** | ***określono protokoły, których użytkowanie ma być zakazane lub ograniczone;*** |
| | **CM-07_ODP[05]** | ***określono oprogramowanie, którego użytkowanie ma być zakazane lub ograniczone;*** |
| | **CM-07_ODP[06]** | ***określono usługi, których użytkowanie ma być zakazane lub ograniczone;*** |
| | **CM-07a.** | system jest skonfigurowany tak, aby zapewniać jedynie ***<funkcje niezbędne do realizacji misji CM-07_ODP[01]>***; |
| | **CM-07b.[01]** | korzystanie z ***<funkcji CM-07_ODP[02]>*** jest zabronione lub ograniczone; |
| | **CM-07b.[02]** | korzystanie z ***<portów CM-07_ODP[03]>*** jest zabronione lub ograniczone; |
| | **CM-07b.[03]** | korzystanie z ***<protokołów CM-07_ODP[04]>*** jest zabronione lub ograniczone; |
| | **CM-07b.[04]** | korzystanie z ***<oprogramowania CM-07_ODP[05]>*** jest zabronione lub ograniczone; |
| | **CM-07b.[05]** | korzystanie z ***<usług CM-07_ODP[06]>*** jest zabronione lub ograniczone. |

| | | |
|---|---|---|
| **CM-07** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zasady minimalnej funkcjonalności; plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inwentaryzacja komponentów systemu; wspólne bezpieczne listy kontrolne konfiguracji; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie konfiguracją bezpieczeństwa; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **CM-07-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zakazujące lub ograniczające korzystanie z funkcji, portów, protokołów, oprogramowania lub usług; mechanizmy ograniczające lub uniemożliwiające korzystanie z funkcji, portów, protokołów, oprogramowania lub usług]. |

| | | |
|---|---|---|
| **CM-07(01)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| PRZEGLĄDY OKRESOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-07(01)_ODP[01]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu systemu w celu zidentyfikowania zbędnych lub niezabezpieczonych funkcji, portów, protokołów, oprogramowania lub usług;*** |
| | **CM-07(01)_ODP[02]** | ***określono funkcje, które mają być wyłączone lub usunięte, gdy zostaną uznane za zbędne lub niezabezpieczone;*** |

| CM-07(01) | ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| PRZEGLĄDY OKRESOWE | |
|---|---|---|
| | **CM-07(01)_ODP[03]** | ***określono porty, które mają być wyłączone lub usunięte, gdy zostaną uznane za zbędne lub niezabezpieczone;*** |
| | **CM-07(01)_ODP[04]** | ***określono protokoły, które mają być wyłączone lub usunięte, gdy zostaną uznane za zbędne lub niezabezpieczone;*** |
| | **CM-07(01)_ODP[05]** | ***określono oprogramowanie, które ma być wyłączone lub usunięte, gdy zostanie uznane za zbędne lub niezabezpieczone;*** |
| | **CM-07(01)_ODP[06]** | ***określono usługi, które mają być wyłączone lub usunięte, gdy zostaną uznane za zbędne lub niezabezpieczone;*** |
| | **CM-07(01)(a)** | system jest poddawany przeglądowi z ***<częstotliwością CM-07(01)_ODP[01]> w*** celu zidentyfikowania zbędnych lub niezabezpieczonych funkcji, portów, protokołów, oprogramowania i usług: |
| | **CM-07(01)(b)[01]** | ***<funkcje CM-07(01)_ODP[02]>*** uznane za zbędne lub niezabezpieczone są wyłączane lub usuwane; |
| | **CM-07(01)(b)[02]** | ***<porty CM-07(01)_ODP[03]>*** uznane za zbędne lub niezabezpieczone są wyłączane lub usuwane; |
| | **CM-07(01)(b)[03]** | ***<protokoły CM-07(01)_ODP[04]>*** uznane za zbędne lub niezabezpieczone są wyłączane lub usuwane; |
| | **CM-07(01)(b)[04]** | ***<oprogramowanie CM-07(01)_ODP[05]>*** uznane za zbędne lub niezabezpieczone są wyłączane lub usuwane; |
| | **CM-07(01)(b)[05]** | ***<usługi CM-07(01)_ODP[06]>*** uznane za zbędne lub niezabezpieczone są wyłączane lub usuwane; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| CM-07(01) | ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| PRZEGLĄDY OKRESOWE | |
|---|---|---|
| | **CM-07(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zasady minimalnej funkcjonalności; plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wspólne bezpieczne listy kontrolne konfiguracji; udokumentowane przeglądy funkcji, portów, protokołów lub usług; zapisy dotyczące zabezpieczania zmian; zapisy audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-07(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przegląd funkcji, portów, protokołów i usług w systemie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **CM-07(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przeglądu lub wyłączania funkcji, portów, protokołów i usług w systemie; mechanizmy realizujące przegląd i wyłączanie funkcji, portów, protokołów lub usług]. |

| | | |
|---|---|---|
| **CM-07(02)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| ZAPOBIEGANIE WYKONYWANIU PROGRAMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-07(02)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: <polityki, zasady postępowania lub umowy o dostęp dotyczące użytkowania i ograniczeń programu komputerowego CM-07(02)_ODP[02]>; zasady zatwierdzające warunki użytkowania programu komputerowego};*** |
| | **CM-07(02)_ODP[02]** | ***określono polityki, zasady postępowania lub umowy o dostęp dotyczące użytkowania i ograniczeń programu komputerowego (jeśli wybrano);*** |
| | **CM-07(02)** | wykonanie programu jest uniemożliwione zgodnie z ***<WYBRANA WARTOŚĆ PARAMETRU CM-07(02)_ODP[01]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-07(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zasady minimalnej funkcjonalności; plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inwentaryzacja komponentów systemu; wspólne bezpieczne listy kontrolne konfiguracji; specyfikacje dotyczące zapobiegania wykonywaniu programu komputerowego; zapisy dotyczące zabezpieczania zmian; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-07(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |

| | | |
|---|---|---|
| **CM-07(02)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| ZAPOBIEGANIE WYKONYWANIU PROGRAMU** | |
| | **CM-07(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zapobiegające wykonywaniu programów w systemie; procesy organizacyjne dotyczące użytkowania i ograniczeń programów; mechanizmy zapobiegające wykonywaniu programów w systemie; mechanizmy wspierające lub realizujące wykorzystanie i ograniczenia programów]. |

| | | |
|---|---|---|
| **CM-07(03)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| STOSOWANIE REJESTRACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-07(03)_ODP** | ***określono wymagania dotyczące rejestracji funkcji, portów, protokołów i usług;*** |
| | **CM-07(03)** | spełnione są ***<wymagania dotyczące rejestracji CM-07(03)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-07(03)-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; polityka zarządzania konfiguracją; procedury dotyczące zasady minimalnej funkcjonalności; plan zarządzania konfiguracją; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inwentaryzacja komponentów systemu; przeglądy audytowe i zgodności; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-07(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo; administratorzy systemu/sieci; programiści systemu]. |

| | | |
|---|---|---|
| **CM-07(03)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| STOSOWANIE REJESTRACJI** | |
| | **CM-07(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zapewniające zgodność z wymaganiami dotyczącymi rejestracji funkcji, portów, protokołów lub usług; mechanizmy wdrażające zgodność z wymaganiami dotyczącymi rejestracji funkcji, portów, protokołów lub usług]. |

| | | |
|---|---|---|
| **CM-07(04)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| NIEAUTORYZOWANE OPROGRAMOWANIE — „CZARNA LISTA”** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-07(04)_ODP[01]** | ***określono programy, które nie mogą być wykonywane w systemie;*** |
| | **CM-07(04)_ODP[02]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji listy nieautoryzowanych programów;*** |
| | **CM-07(04)(a)** | zdefiniowano ***<programy CM-07(04)_ODP[01]>;*** |
| | **CM-07(04)(b)** | stosuje się politykę „zezwalaj na wszystko za wyjątkiem” (*ang.: allow-all, deny-by-exception*), aby zabronić wykonywania nieautoryzowanych programów w systemie; |
| | **CM-07(04)(c)** | lista nieautoryzowanych programów jest przeglądana i aktualizowana z ***<częstotliwością CM-07(04)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CM-07(04)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| NIEAUTORYZOWANE OPROGRAMOWANIE — „CZARNA LISTA”** | |
| | **CM-07(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zasady minimalnej funkcjonalności; plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista programów, które nie mogą być wykonywane w systemie; inwentaryzacja komponentów systemu; wspólne bezpieczne listy kontrolne konfiguracji; zapisy dotyczące przeglądu i aktualizacji związane z listą nieuprawnionych programów; zapisy dotyczące kontroli zmian; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-07(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za identyfikację programów, które nie mogą być wykonywane w systemie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-07(04)-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny w zakresie identyfikacji, przeglądu i aktualizacji listy programów, które nie mogą być wykonywane w systemie; proces organizacyjny w zakresie wdrażania polityki dotyczącej nieautoryzowanych programów; mechanizmy wspierające lub wdrażające politykę w zakresie nieautoryzowanych programów]. |

| | | |
|---|---|---|
| **CM-07(05)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| AUTORYZOWANE OPROGRAMOWANIE — „BIAŁA LISTA”** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-07(05)_ODP[01]** | ***określono programy, których wykonywanie w systemie jest dozwolone;*** |

| | | |
|---|---|---|
| **CM-07(05)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| AUTORYZOWANE OPROGRAMOWANIE — „BIAŁA LISTA”** | |
| | **CM-07(05)_ODP[02]** | ***Określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji listy programów, których wykonywanie w systemie jest dozwolone;*** |
| | **CM-07(05)(a)** | zdefiniowano ***<programy CM-07(05)_ODP[01]>***; |
| | **CM-07(05)(b)** | stosuje się politykę „odmawiaj wszystkiego za wyjątkiem” (*ang.: deny-all, permit-by-exception*) w celu umożliwienia wykonywania autoryzowanych programów w systemie; |
| | **CM-07(05)(c)** | lista autoryzowanych programów jest przeglądana i aktualizowana z ***<częstotliwością CM-07(05)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-07(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zasady minimalnej funkcjonalności w systemie; plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista programów, których wykonywanie w systemie jest dozwolone; inwentaryzacja komponentów systemu; wspólne bezpieczne listy kontrolne konfiguracji; zapisy dotyczące przeglądu i aktualizacji listy autoryzowanych programów komputerowych; zapisy dotyczące kontroli zmian; zapisy dotyczące audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-07(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za identyfikację programów, które mogą być wykonywane w systemie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |

| | | |
|---|---|---|
| **CM-07(05)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| AUTORYZOWANE OPROGRAMOWANIE — „BIAŁA LISTA”** | |
| | **CM-07(05)-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny w zakresie identyfikacji, przeglądu i aktualizacji listy programów, które mogą być wykonywane w systemie; proces organizacyjny w zakresie wdrażania polityki dotyczącej autoryzowanych programów; mechanizmy wspierające lub wdrażające politykę w zakresie autoryzowanych programów]. |

| | | |
|---|---|---|
| **CM-07(06)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| ZAMKNIĘTE ŚRODOWISKA Z OGRANICZONYMI UPRAWNIENIAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-07(06)_ODP** | ***określono oprogramowanie instalowane przez użytkownika, które musi być wykonywane w środowisku zamkniętym;*** |
| | **CM-07(06)** | ***<oprogramowanie instalowane przez użytkownika CM-07(06)_ODP >*** musi być wykonywane w zamkniętym środowisku maszyny fizycznej lub wirtualnej z ograniczonymi uprawnieniami. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-07(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zasady minimalnej funkcjonalności; plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista lub zapisy dotyczące oprogramowania, które musi być wykonywane w środowisku zamkniętym; inwentaryzacja komponentów systemu; wspólne bezpieczne listy kontrolne konfiguracji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-07(06)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| ZAMKNIĘTE ŚRODOWISKA Z OGRANICZONYMI UPRAWNIENIAMI** | |
| | **CM-07(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za identyfikację lub zarządzanie oprogramowaniem instalowanym przez użytkownika i związanymi z nim uprawnieniami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-07(06)-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny w zakresie identyfikacji oprogramowania instalowanego przez użytkownika, które musi być wykonywane w środowisku zamkniętym; mechanizmy wspierające lub wdrażające ograniczenia w zakresie oprogramowania instalowanego przez użytkownika w środowiskach maszyn fizycznych lub wirtualnych; mechanizmy wspierające lub wdrażające ograniczenia uprawnień w zakresie oprogramowania instalowanego przez użytkownika]. |

| | | |
|---|---|---|
| **CM-07(07)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| WYKONYWANIE KODU W CHRONIONYCH ŚRODOWISKACH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-07(07)_ODP** | ***określono personel lub role, które mają jednoznacznie zatwierdzać wykonanie kodu binarnego lub maszynowego;*** |
| | **CM-07(07)** | wykonywanie kodu binarnego lub maszynowego jest dozwolone wyłącznie w zamkniętych środowiskach maszyn fizycznych lub wirtualnych; |
| | **CM-07(07)(a)** | wykonywanie kodu binarnego lub maszynowego uzyskanego ze źródeł niezaufanych lub o ograniczonym zaufaniu jest dozwolone tylko za wyraźną zgodą ***<personelu lub ról CM-07(07)_ODP>***; |

| | | |
|---|---|---|
| **CM-07(07)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| WYKONYWANIE KODU W CHRONIONYCH ŚRODOWISKACH** | |
| | **CM-07(07)(b)** | wykonywanie kodu binarnego lub maszynowego bez dostarczenia kodu źródłowego jest dozwolone tylko za wyraźną zgodą ***<personelu lub ról CM-07(07)_ODP>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-07(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zasady minimalnej funkcjonalności; plan zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista lub zapisy dotyczące kodu binarnego lub maszynowego; inwentaryzacja komponentów systemu; wspólne bezpieczne listy kontrolne konfiguracji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-07(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zatwierdzanie wykonania kodu binarnego lub maszynowego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie oprogramowaniem; administratorzy systemu/sieci; programiści systemu]. |
| | **CM-07(07)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zatwierdzanie wykonania kodu binarnego lub maszynowego; proces organizacyjny ograniczający wykonywanie kodu binarnego lub maszynowego do środowisk maszyn fizycznych lub wirtualnych; mechanizmy wspierające lub wdrażające zasady ograniczające wykonywanie kodu binarnego lub maszynowego do środowisk maszyn fizycznych lub wirtualnych]. |

| | | |
|---|---|---|
| **CM-07(08)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| KOD BINARNY LUB MASZYNOWY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-07(08)(a)** | użycie kodu binarnego lub maszynowego jest zabronione, jeśli pochodzi on ze źródeł niezaufanych lub o ograniczonym zaufaniu, a także w przypadku gdy nie jest dostępny kod źródłowy; |
| | **CM-07(08)(b)[01]** | wyjątki od zakazu stosowania kodu binarnego lub maszynowego pochodzącego ze źródeł niezaufanych lub o ograniczonym zaufaniu lub bez podania kodu źródłowego są dopuszczalne jedynie w przypadku istotnych wymogów dotyczących misji lub operacji; |
| | **CM-07(08)(b)[02]** | wyjątki od zakazu stosowania kodu binarnego lub maszynowego pochodzącego ze źródeł niezaufanych lub o ograniczonym zaufaniu lub bez podania kodu źródłowego są dopuszczalne jedynie za zgodną autoryzowanego pracownika funkcyjnego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-07(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące zasady minimalnej funkcjonalności; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista lub zapisy dotyczące kodu binarnego lub maszynowego; inwentaryzacja komponentów systemu; wspólne bezpieczne listy kontrolne konfiguracji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-07(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie misji i wymagań operacyjnych; urzędnik zatwierdzający system; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie oprogramowaniem; administratorzy systemu/sieci]. |

| | | |
|---|---|---|
| **CM-07(08)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| KOD BINARNY LUB MASZYNOWY** | |
| | **CM-07(08)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zatwierdzanie wykonania kodu binarnego lub maszynowego; mechanizmy wspierające lub wdrażające zakaz stosowania kodu binarnego lub maszynowego]. |

| | | |
|---|---|---|
| **CM-07(09)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| ZAKAZ UŻYWANIA NIEAUTORYZOWANEGO SPRZĘTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-07(09)_ODP[01]** | ***określono komponenty sprzętowe dopuszczone do użytku w systemie;*** |
| | **CM-07(09)_ODP[02]** | ***określono częstotliwość przeglądu i aktualizacji listy autoryzowanych komponentów sprzętowych;*** |
| | **CM-07(09)(a)** | określono ***<komponenty sprzętowe CM-07(09)_ODP[01]>;*** |
| | **CM-07(09)(b)** | używanie lub podłączanie nieautoryzowanych komponentów sprzętowych jest zabronione; |
| | **CM-07(09)(c)** | przeglądu i aktualizacji listy autoryzowanych komponentów sprzętowych dokonuje się z ***<częstotliwością CM-07(09)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-07(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; polityka i procedury dotyczące połączeń sieciowych; plan zarządzania konfiguracją; plan bezpieczeństwa systemu;<br>dokumentacja projektowa systemu; inwentaryzacja komponentów systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-07(09)** | **ZASADA MINIMALNEJ FUNKCJONALNOŚCI \| ZAKAZ UŻYWANIA NIEAUTORYZOWANEGO SPRZĘTU** | |
| | **CM-07(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie sprzętem systemowym; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-07(09)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zatwierdzanie wykonania kodu binarnego lub maszynowego; mechanizmy wspierające lub wdrażające zakaz stosowania kodu binarnego lub maszynowego]. |

| | | |
|---|---|---|
| **CM-08** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-08_ODP[01]** | ***określono informacje uznane za niezbędne do osiągnięcia skutecznej rozliczalności w zakresie komponentów systemu;*** |
| | **CM-08_ODP[02]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji listy komponentów systemu;*** |
| | **CM-08a.01** | opracowano i udokumentowano listę komponentów systemu, która dokładnie odzwierciedla jego strukturę; |
| | **CM-08a.02** | opracowano i udokumentowano listę komponentów systemu, która obejmuje wszystkie jego elementy; |
| | **CM-08a.03** | opracowano i udokumentowano listę komponentów systemu, która nie zawiera zdublowanych wpisów dot. pojedynczych komponentów lub komponentów przypisanych do innego systemu; |

| | | |
|---|---|---|
| **CM-08** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU** | |
| | **CM-08a.04** | opracowano i udokumentowano listę komponentów systemu o poziomie szczegółowości uznanym za niezbędny do realizacji śledzenia i raportowania; |
| | **CM-08a.05** | opracowano i udokumentowano listę komponentów systemu, która obejmuje ***<informacje CM-08_ODP[01]>***; |
| | **CM-08b.** | lista komponentów systemu jest przeglądana i aktualizowana z ***<częstotliwością CM-08_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; inwentaryzacja komponentów systemu; przeglądy inwentaryzacyjne i ich aktualizacje; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie inwentaryzacją komponentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania inwentaryzacją komponentów systemu; mechanizmy wspierające lub wdrażające inwentaryzację komponentów systemu]. |

| | | |
|---|---|---|
| **CM-08(01)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| AKTUALIZACJE PODCZAS INSTALACJI LUB USUWANIA KOMPONENTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-08(01)[01]** | lista komponentów systemu jest aktualizowana przy instalacji komponentów; |
| | **CM-08(01)[02]** | lista komponentów systemu jest aktualizowana przy usuwaniu komponentów; |
| | **CM-08(01)[03]** | lista komponentów systemu jest aktualizowana przy aktualizacji systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-08(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; inwentaryzacja komponentów systemu; przeglądy inwentaryzacyjne i ich aktualizacje; zapisy dotyczące zabezpieczania zmian; zapisy instalacji składników; zapisy dotyczące usuwania składników; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-08(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za aktualizację listy komponentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-08(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie aktualizacji listy komponentów systemu; mechanizmy wspierające lub realizujące aktualizację listy komponentów systemu]. |

| | | |
|---|---|---|
| **CM-08(02)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| AUTOMATYCZNA KONSERWACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-08(02)_ODP[01]** | ***określono automatyczne mechanizmy służące do zapewnienia aktualności listy komponentów systemu;*** |
| | **CM-08(02)_ODP[02]** | ***określono automatyczne mechanizmy służące do zapewnienia kompletności listy komponentów systemu;*** |
| | **CM-08(02)_ODP[03]** | ***określono automatyczne mechanizmy służące do zapewnienia dokładności listy komponentów systemu;*** |
| | **CM-08(02)_ODP[04]** | ***określono automatyczne mechanizmy służące do zapewnienia dostępności listy komponentów systemu;*** |
| | **CM-08(02)[01]** | stosuje się ***<mechanizmy automatyczne CM-08(02)_ODP[01]>*** ***do*** zapewnienia aktualności listy komponentów systemu; |
| | **CM-08(02)[02]** | stosuje się ***<mechanizmy automatyczne CM-08(02)_ODP[02]>*** ***do*** zapewnienia kompletności listy komponentów systemu; |
| | **CM-08(02)[03]** | stosuje się ***<mechanizmy automatyczne CM-08(02)_ODP[03]>*** ***do*** zapewnienia dokładności listy komponentów systemu; |
| | **CM-08(02)[04]** | stosuje się ***<mechanizmy automatyczne CM-08(02)_ODP[04]>*** ***do*** zapewnienia dostępności listy komponentów systemu; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-08(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu; plan zarządzania konfiguracją; dokumentacja projektowa systemu;<br>plan bezpieczeństwa systemu; inwentaryzacja komponentów systemu; zapisy dotyczące zabezpieczania zmian; zapisy dotyczące utrzymania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| CM-08(02) | INWENTARYZACJA KOMPONENTÓW SYSTEMU \| AUTOMATYCZNA KONSERWACJA | |
|---|---|---|
| | **CM-08(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie inwentaryzacją komponentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **CM-08(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania inwentaryzacją komponentów systemu; mechanizmy automatyczne wspierające lub wdrażające inwentaryzację komponentów systemu]. |

| CM-08(03) | INWENTARYZACJA KOMPONENTÓW SYSTEMU \| AUTOMATYCZNE WYKRYWANIE NIEAUTORYZOWANYCH KOMPONENTÓW | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-08(03)_ODP[01]** | ***określono automatyczne mechanizmy służące do wykrywania obecności nieautoryzowanego sprzętu w systemie;*** |
| | **CM-08(03)_ODP[02]** | ***określono automatyczne mechanizmy służące do wykrywania obecności nieautoryzowanego oprogramowania w systemie;*** |
| | **CM-08(03)_ODP[03]** | ***określono automatyczne mechanizmy służące do wykrywania obecności nieautoryzowanego oprogramowania sprzętowego w systemie;*** |
| | **CM-08(03)_ODP[04]** | ***określono częstotliwość, z jaką stosowane są automatyczne mechanizmy do wykrywania obecności nieautoryzowanych komponentów w systemie;*** |
| | **CM-08(03)_ODP[05]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {zablokowanie nieautoryzowanym komponentom dostępu do sieci; izolacja nieautoryzowanych komponentów; powiadomienie <personelu lub ról CM-08(03)_ODP[06]>};*** |
| | **CM-08(03)_ODP[06]** | ***określono personel lub role, które mają być powiadamiane w przypadku wykrycia nieautoryzowanych komponentów (jeśli wybrano);*** |

| | | |
|---|---|---|
| **CM-08(03)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| AUTOMATYCZNE WYKRYWANIE NIEAUTORYZOWANYCH KOMPONENTÓW** | |
| | **CM-08(03)(a)[01]** | obecność nieautoryzowanego sprzętu w systemie jest wykrywana za pomocą ***<mechanizmów automatycznych CM-08(03)_ODP[01]> z <częstotliwością CM-08(03)_ODP[04]>***; |
| | **CM-08(03)(a)[02]** | obecność nieautoryzowanego oprogramowania w systemie jest wykrywana za pomocą ***<mechanizmów automatycznych CM-08(03)_ODP[02]> z <częstotliwością CM-08(03)_ODP[04]>***; |
| | **CM-08(03)(a)[03]** | obecność nieautoryzowanego oprogramowania sprzętowego w systemie jest wykrywana za pomocą ***<mechanizmów automatycznych CM-08(03)_ODP[03]> z <częstotliwością CM-08(03)_ODP[04]>***; |
| | **CM-08(03)(b)[01]** | ***<WYBRANA WARTOŚĆ PARAMETRU CM-08(03)_ODP[05]>*** ma zastosowanie, gdy wykryto nieautoryzowany sprzęt; |
| | **CM-08(03)(b)[02]** | ***<WYBRANA WARTOŚĆ PARAMETRU CM-08(03)_ODP[05]>*** ma zastosowanie, gdy wykryto nieautoryzowane oprogramowanie; |
| | **CM-08(03)(b)[03]** | ***<WYBRANA WARTOŚĆ PARAMETRU CM-08(03)_ODP[05]>*** ma zastosowanie, gdy wykryto nieautoryzowane oprogramowanie sprzętowe; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-08(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu; plan zarządzania konfiguracją; dokumentacja projektowa systemu;<br>plan bezpieczeństwa systemu; inwentaryzacja komponentów systemu; zapisy dotyczące zabezpieczania zmian; alerty/powiadomienia o nieautoryzowanych komponentach w systemie; zapisy dotyczące monitorowania systemu; zapisy dotyczące konserwacji systemu; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-08(03)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| AUTOMATYCZNE WYKRYWANIE NIEAUTORYZOWANYCH KOMPONENTÓW** | |
| | **CM-08(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie inwentaryzacją komponentów; personel organizacyjny odpowiedzialny za zarządzanie automatycznymi mechanizmami wykrywającymi nieautoryzowane komponenty w systemie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **CM-08(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania nieautoryzowanych komponentów w systemie; procesy organizacyjne dotyczące podejmowania działań w przypadku wykrycia nieautoryzowanych komponentów w systemie; automatyczne mechanizmy wspierające lub realizujące wykrywanie nieautoryzowanych komponentów w systemie; automatyczne mechanizmy wspierające lub realizujące działania podejmowane w przypadku wykrycia nieautoryzowanych komponentów w systemie]. |

| | | |
|---|---|---|
| **CM-08(04)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| INFORMACJE DOTYCZĄCE ODPOWIEDZIALNOŚCI I ROZLICZALNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-08(04)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {imię i nazwisko; stanowisko; rola};*** |
| | **CM-08(04)** | osoby odpowiedzialne i rozliczane za zarządzanie komponentami systemu są zidentyfikowane na liście komponentów systemu za pomocą ***<WYBRANA WARTOŚĆ PARAMETRU CM-08(04)_ODP>*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CM-08(04)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| INFORMACJE DOTYCZĄCE ODPOWIEDZIALNOŚCI I ROZLICZALNOŚCI** | |
| | **CM-08(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; inwentaryzacja komponentów systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-08(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie inwentaryzacją komponentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-08(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania inwentaryzacją komponentów systemu; mechanizmy wspierające lub wdrażające inwentaryzację komponentów systemu]. |

| | | |
|---|---|---|
| **CM-08(05)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| BRAK DUPLIKACJI KOMPONENTÓW** | |
| | [WYCOFANE: Włączone do CM-08]. | |

| | | |
|---|---|---|
| **CM-08(06)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| OCENA KONFIGURACJI I ZATWIERDZONE ODSTĘPSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-08(06)[01]** | oceniane konfiguracje komponentów są zawarte w inwentaryzacji komponentów systemu; |
| | **CM-08(06)[02]** | wszelkie zatwierdzone odstępstwa od aktualnych wdrożonych konfiguracji są uwzględniane w inwentaryzacji komponentów systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CM-08(06)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| OCENA KONFIGURACJI I ZATWIERDZONE ODSTĘPSTWA** | |
| | **CM-08(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; inwentaryzacja komponentów systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące zabezpieczania zmian; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-08(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za inwentaryzację komponentów systemu; personel organizacyjny odpowiedzialny za przeprowadzanie ocen; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-08(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania inwentaryzacją komponentów systemu; mechanizmy wspierające lub wdrażające inwentaryzację komponentów systemu]. |

| | | |
|---|---|---|
| **CM-08(07)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| SCENTRALIZOWANE REPOZYTORIUM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-08(07)** | do celów inwentaryzacji komponentów systemu zapewniane jest scentralizowane repozytorium. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CM-08(07)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| SCENTRALIZOWANE REPOZYTORIUM** | |
| | **CM-08(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; inwentaryzacja komponentów systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące zabezpieczania zmian; inne istotne dokumenty lub zapisy]. |
| | **CM-08(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie inwentaryzacją komponentów; personel organizacyjny odpowiedzialny za bezpieczeństwo]. |
| | **CM-08(07)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania inwentaryzacją komponentów systemu; mechanizmy wspierające lub wdrażające inwentaryzację komponentów systemu]. |

| | | |
|---|---|---|
| **CM-08(08)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| AUTOMATYCZNE ŚLEDZENIE LOKALIZACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-08(08)_ODP** | ***określono automatyczne mechanizmy śledzenia komponentów;*** |
| | **CM-08(08)** | stosuje się ***<mechanizmy automatyczne CM-08(08)_ODP> do*** wspierania śledzenia komponentów systemu według lokalizacji geograficznej. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CM-08(08)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| AUTOMATYCZNE ŚLEDZENIE LOKALIZACJI** | |
| | **CM-08(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu; plan zarządzania konfiguracją; dokumentacja projektowa systemu; inwentaryzacja komponentów systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CM-08(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie inwentaryzacją komponentów; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **CM-08(08)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania inwentaryzacją składników systemu; automatyczne mechanizmy wspomagające lub wdrażające inwentaryzację komponentów systemu; automatyczne mechanizmy wspomagające lub wdrażające śledzenie komponentów według lokalizacji geograficznej]. |

| | | |
|---|---|---|
| **CM-08(09)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-08(09)_ODP** | ***określono personel lub role, od których należy otrzymać potwierdzenie;*** |
| | **CM-08(09)(a)** | komponenty systemu są przypisane do systemu; |
| | **CM-08(09)(b)** | potwierdzenie przypisania komponentów otrzymuje się od ***<personelu lub ról CM-08(09)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CM-08(09)** | **INWENTARYZACJA KOMPONENTÓW SYSTEMU \| PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW** | |
| | **CM-08(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; inwentaryzacja komponentów systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące zabezpieczania zmian; potwierdzenie przypisania komponentów systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CM-08(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie inwentaryzacją komponentów; właściciel systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-08(09)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przypisania komponentów do systemów; procesy organizacyjne dotyczące potwierdzania przypisania komponentów do systemów; mechanizmy wdrażające przypisanie komponentów do systemu; mechanizmy wdrażające proces potwierdzania przypisania komponentów do systemów]. |

| | | |
|---|---|---|
| **CM-09** | **PLAN ZARZĄDZANIA KONFIGURACJĄ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-09_ODP** | ***określono personel lub role odpowiedzialne za przeglądanie i zatwierdzanie planu zarządzania konfiguracją;*** |
| | **CM-09[01]** | opracowano i udokumentowano plan zarządzania konfiguracją dla systemu; |
| | **CM-09[02]** | wdrożono plan zarządzania konfiguracją dla systemu; |

| CM-09 | PLAN ZARZĄDZANIA KONFIGURACJĄ | |
|---|---|---|
| | **CM-09a.[01]** | plan zarządzania konfiguracją odnosi się do ról; |
| | **CM-09a.[02]** | plan zarządzania konfiguracją odnosi się do obowiązków; |
| | **CM-09a.[03]** | plan zarządzania konfiguracją odnosi się do procesów i procedur zarządzania konfiguracją; |
| | **CM-09b.[01]** | plan zarządzania konfiguracją ustanawia proces identyfikacji elementów konfiguracji w całym cyklu rozwoju systemu; |
| | **CM-09b.[02]** | plan zarządzania konfiguracją ustanawia proces zarządzania konfiguracją elementów konfiguracyjnych; |
| | **CM-09c.[01]** | plan zarządzania konfiguracją definiuje elementy konfiguracji dla systemu; |
| | **CM-09c.[02]** | w ramach planu zarządzania konfiguracją elementy konfiguracji zostają objęte procesem zarządzania konfiguracją; |
| | **CM-09d.** | aktualny plan zarządzania konfiguracją jest przeglądany i aktualizowany przez ***<personel lub role CM-09_ODP>***; |
| | **CM-09e.[01]** | plan zarządzania konfiguracją jest chroniony przed nieautoryzowanym ujawnieniem; |
| | **CM-09e.[02]** | plan zarządzania konfiguracją jest chroniony przed nieautoryzowaną modyfikacją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące planowania procesu zarządzania konfiguracją; plan zarządzania konfiguracją; dokumentacja projektowa systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-09** | **PLAN ZARZĄDZANIA KONFIGURACJĄ** | |
| | **CM-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za opracowanie planu zarządzania konfiguracją; personel organizacyjny odpowiedzialny za wdrożenie i zarządzanie procesami określonymi w planie zarządzania konfiguracją; personel organizacyjny odpowiedzialny za ochronę planu zarządzania konfiguracją; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci]. |
| | **CM-09-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące opracowania i dokumentowania planu zarządzania konfiguracją; procesy organizacyjne dotyczące identyfikacji i zarządzania elementami konfiguracji;<br>procesy organizacyjne dotyczące ochrony planu zarządzania konfiguracją; mechanizmy wdrażające plan zarządzania konfiguracją; mechanizmy zarządzania elementami konfiguracji; mechanizmy ochrony planu zarządzania konfiguracją]. |

| | | |
|---|---|---|
| **CM-09(01)** | **PLAN ZARZĄDZANIA KONFIGURACJĄ \| PRZYPISANIE ODPOWIEDZIALNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-09(01)** | odpowiedzialność za rozwój procesu zarządzania konfiguracją jest przypisana do personelu organizacyjnego, który nie jest bezpośrednio zaangażowany w rozwój systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-09(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące odpowiedzialność za opracowanie procesu zarządzania konfiguracją; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-09(01)** | **PLAN ZARZĄDZANIA KONFIGURACJĄ \| PRZYPISANIE ODPOWIEDZIALNOŚCI** | |
| | **CM-09(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za opracowanie procesu zarządzania konfiguracją; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CM-10** | **OGRANICZENIA W UŻYCIU OPROGRAMOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-10a.** | oprogramowanie i związana z nim dokumentacja są wykorzystywane zgodnie z umowami i z poszanowaniem praw autorskich; |
| | **CM-10b.** | wykorzystanie oprogramowania chronionego licencjami ilościowymi wraz ze związaną z nim dokumentacją jest monitorowane w celu kontroli procesu kopiowania i dystrybucji takich treści; |
| | **CM-10c.** | wymiana plików w systemie „peer-to-peer” podlega kontroli i dokumentowaniu w celu zapewnienia, że nie służy ona do nieautoryzowanego rozpowszechniania, wyświetlania, wykonywania lub powielania treści chronionych prawem autorskim. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; ograniczenia w użytkowaniu oprogramowania; umowy dotyczące oprogramowania i praw autorskich; dokumentacja licencyjna witryny; lista ograniczeń w użytkowaniu oprogramowania; raporty ze śledzenia licencji na oprogramowanie; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-10** | **OGRANICZENIA W UŻYCIU OPROGRAMOWANIA** | |
| | **CM-10-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny obsługujący, eksploatujący lub utrzymujący system; personel organizacyjny odpowiedzialny za zarządzanie licencjami oprogramowania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-10-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie śledzenia wykorzystania oprogramowania chronionego licencjami ilościowymi; procesy organizacyjne w zakresie kontroli/dokumentowania wykorzystania wymiany plików w systemie „peer-to-peer"; mechanizmy wdrażające śledzenie licencji oprogramowania; mechanizmy wdrażające i kontrolujące wykorzystanie technologii wymiany plików peer-to-peer]. |

| | | |
|---|---|---|
| **CM-10(01)** | **OGRANICZENIA W UŻYCIU OPROGRAMOWANIA \| OPROGRAMOWANIE OTWARTE (OPEN-SOURCE)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-10(01)_ODP** | ***określono ograniczenia dotyczące korzystania z otwartego oprogramowania;*** |
| | **CM-10(01)** | ustanowiono ***<ograniczenia CM-10(01)_ODP> w*** zakresie korzystania z otwartego oprogramowania; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-10(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; ograniczenia w użytkowaniu oprogramowania; umowy dotyczące oprogramowania i praw autorskich; dokumentacja licencyjna witryny; lista ograniczeń w użytkowaniu oprogramowania; raporty ze śledzenia licencji na oprogramowanie; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-10(01)** | **OGRANICZENIA W UŻYCIU OPROGRAMOWANIA \| OPROGRAMOWANIE OTWARTE (OPEN-SOURCE)** | |
| | **CM-10(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny obsługujący, eksploatujący lub utrzymujący system; personel organizacyjny odpowiedzialny za zarządzanie licencjami oprogramowania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-10(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie śledzenia wykorzystania oprogramowania chronionego licencjami ilościowymi; procesy organizacyjne w zakresie kontroli/dokumentowania wykorzystania wymiany plików w systemie „peer-to-peer"; mechanizmy wdrażające śledzenie licencji oprogramowania; mechanizmy wdrażające i kontrolujące wykorzystanie technologii wymiany plików peer-to-peer]. |

| | | |
|---|---|---|
| **CM-11** | **OPROGRAMOWANIE ZAINSTALOWANE PRZEZ UŻYTKOWNIKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-11_ODP[01]** | ***zdefiniowano politykę dotyczącą instalacji oprogramowania przez użytkowników;*** |
| | **CM-11_ODP[02]** | ***zdefiniowano metody stosowane do egzekwowania zasad instalacji oprogramowania;*** |
| | **CM-11_ODP[03]** | ***zdefiniowano częstotliwość, z jaką należy monitorować zgodność z polityką;*** |
| | **CM-11a.** | Ustalono ***<politykę CM-11_ODP[01]>*** regulującą instalację oprogramowania przez użytkowników; |
| | **CM-11b.** | polityka instalacji oprogramowania jest egzekwowana za pomocą ***<metod CM-11_ODP[02]>***; |

| | | |
|---|---|---|
| **CM-11** | **OPROGRAMOWANIE ZAINSTALOWANE PRZEZ UŻYTKOWNIKA** | |
| | **CM-11c.** | zgodność z ***<polityką CM-11_ODP[01]>*** jest monitorowana z ***<częstotliwością CM-11_ODP[03]>*.** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-11-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące oprogramowania instalowanego przez użytkownika; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>lista zasad dotyczących oprogramowania instalowanego przez użytkownika; zapisy dotyczące monitorowania systemu; zapisy dotyczące audytu systemu; strategia ciągłego monitorowania; plan bezpieczeństwa systemu; inne stosowne dokumenty lub zapisy]. |
| | **CM-11-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie oprogramowaniem instalowanym przez użytkownika; personel organizacyjny obsługujący, eksploatujący lub utrzymujący system; personel organizacyjny monitorujący zgodność z polityką dotyczącą oprogramowania instalowanego przez użytkownika; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-11-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne regulujące oprogramowanie instalowane przez użytkownika w systemie; mechanizmy egzekwujące stosowanie polityki i metod regulujących instalację oprogramowania przez użytkowników; mechanizmy monitorujące zgodność z polityką]. |

| | | |
|---|---|---|
| **CM-11(01)** | **OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA \| OSTRZEGANIE O NIEAUTORYZOWANYCH INSTALACJACH** | |
| | [WYCOFANE: Włączone do CM-08(03)]. | |

| | | |
|---|---|---|
| **CM-11(02)** | **OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA \| ZABRONIONA INSTALACJA BEZ POSIADANIA STOSOWNYCH UPRAWNIEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-11(02)** | instalację oprogramowania mogą przeprowadzać jedynie użytkownicy, którym wyraźnie nadano status uprzywilejowany. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-11(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące oprogramowania instalowanego przez użytkownika; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>alerty/powiadomienia dotyczące instalacji nieautoryzowanego oprogramowania; strategia ciągłego monitorowania; plan bezpieczeństwa systemu; inne właściwe dokumenty lub zapisy]. |
| | **CM-11(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie oprogramowaniem instalowanym przez użytkownika; personel organizacyjny obsługujący, eksploatujący lub utrzymujący system; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-11(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne regulujące oprogramowanie instalowane przez użytkownika w systemie; mechanizmy zakazujące instalacji oprogramowania bez posiadania statusu uprzywilejowanego (np. kontrola dostępu)]. |

| | | |
|---|---|---|
| **CM-11(03)** | **OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA \| AUTOMATYCZNE EGZEKWOWANIE I MONITOROWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-11(03)_ODP[01]** | ***określono automatyczne mechanizmy służące do egzekwowania zasad zgodności;*** |
| | **CM-11(03)_ODP[02]** | ***określono automatyczne mechanizmy służące do monitorowania zgodności;*** |
| | **CM-11(03)[01]** | zgodność z zasadami instalacji oprogramowania jest egzekwowana przy użyciu ***<mechanizmów automatycznych CM-11(03)_ODP[01]>***; |
| | **CM-11(03)[02]** | zgodność z polityką instalacji oprogramowania jest egzekwowana przy użyciu<br>***<mechanizmów automatycznych CM-11(03)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-11(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące oprogramowania instalowanego przez użytkownika; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>lista zasad dotyczących oprogramowania instalowanego przez użytkownika; zapisy dotyczące monitorowania systemu; zapisy dotyczące audytu systemu; strategia ciągłego monitorowania; plan bezpieczeństwa systemu; inne stosowne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-11(03)** | **OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA \| AUTOMATYCZNE EGZEKWOWANIE I MONITOROWANIE** | |
| | **CM-11(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie oprogramowaniem instalowanym przez użytkownika; personel organizacyjny obsługujący, eksploatujący lub utrzymujący system; personel organizacyjny monitorujący zgodność z polityką dotyczącą oprogramowania instalowanego przez użytkownika; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CM-11(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące oprogramowania instalowanego przez użytkownika w systemie; automatyczne mechanizmy egzekwujące politykę dotyczącą instalacji oprogramowania przez użytkowników; automatyczne mechanizmy monitorujące zgodność z polityką]. |

| | | |
|---|---|---|
| **CM-12** | **POŁOŻENIE (LOKALIZACJA) INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-12_ODP** | ***definiuje się informacje, w przypadku których lokalizacja ma być identyfikowana i dokumentowana;*** |
| | **CM-12a.[01]** | lokalizacja ***<informacja CM-12_ODP >*** jest zidentyfikowana i udokumentowana; |
| | **CM-12a.[02]** | poszczególne komponenty systemu, w których przetwarzana jest ***<informacja CM-12_ODP >*** są identyfikowane i dokumentowane; |
| | **CM-12a.[03]** | poszczególne komponenty systemu, w których przechowywana jest ***<informacjaCM-12_ODP>*** są identyfikowane i dokumentowane; |

| | | |
|---|---|---|
| **CM-12** | **POŁOŻENIE (LOKALIZACJA) INFORMACJI** | |
| | **CM-12b.[01]** | użytkownicy, którzy mają dostęp do systemu i komponentów systemu, w których przetwarzana jest ***<informacja CM-12_ODP>***, są identyfikowani i dokumentowani; |
| | **CM-12b.[02]** | użytkownicy, którzy mają dostęp do systemu i komponentów systemu, w których przechowywana jest ***<informacja CM-12_ODP>***, są identyfikowani i dokumentowani; |
| | **CM-12c.[01]** | dokumentowane są zmiany w lokalizacji (tzn. w systemie lub komponentach systemu), w których przetwarzana jest ***<informacja CM-12_ODP>;*** |
| | **CM-12c.[02]** | dokumentowane są zmiany w lokalizacji (tzn. w systemie lub komponentach systemu), w których przechowywana jest ***<informacja CM-12_ODP>;*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-12-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące identyfikacji i dokumentowania lokalizacji informacji; plan zarządzania konfiguracją; dokumentacja projektowa systemu; dokumentacja architektury systemu; dokumentacja dotycząca wykazu danych identyfikacyjnych; dokumentacja dotycząca mapowania danych; zapisy z audytu; lista użytkowników mających dostęp do systemu i komponentów systemu; zapisy dotyczące zabezpieczania zmian; lista komponentów systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CM-12-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie lokalizacją informacji i dostępem użytkowników do informacji; personel organizacyjny obsługujący, eksploatujący lub utrzymujący system; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci; programiści systemu]. |

| | | |
|---|---|---|
| **CM-12** | **POŁOŻENIE (LOKALIZACJA) INFORMACJI** | |
| | **CM-12-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne regulujące lokalizację informacji; mechanizmy egzekwujące stosowanie polityki i metod regulowania lokalizacji informacji]. |

| | | |
|---|---|---|
| **CM-12(01)** | **POŁOŻENIE (LOKALIZACJA) INFORMACJI \| AUTOMATYCZNE NARZĘDZIA DO OBSŁUGI LOKACJI INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-12(01)_ODP[01]** | ***w przypadku informacji podlegających ochronie zdefiniowano typ takich informacji;*** |
| | **CM-12(01)_ODP[02]** | ***określono komponenty systemu, w których znajduje się informacja;*** |
| | **CM-12(01)** | stosuje automatyczne narzędzia do identyfikacji ***<informacji według typu informacji CM-12(01)_ODP[01]>*** w ***<komponentach systemu CM-12(01)_ODP[02]>***, aby zapewnić, że istnieją zabezpieczenia mające na celu ochronę informacji organizacji oraz prywatności osób. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-12(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące identyfikacji i dokumentowania lokalizacji informacji; plan zarządzania konfiguracją; dokumentacja projektowa systemu; dokumentacja dotycząca listy danych identyfikacyjnych; dokumentacja dotycząca mapowania danych; zapisy dotyczące zabezpieczania zmian; lista komponentów systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-12(01)** | **POŁOŻENIE (LOKALIZACJA) INFORMACJI \| AUTOMATYCZNE NARZĘDZIA DO OBSŁUGI LOKACJI INFORMACJI** | |
| | **CM-12(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie lokalizacją informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **CM-12(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne regulujące lokalizację informacji; automatyczne mechanizmy egzekwujące stosowanie polityki i metod regulowania lokalizacji informacji; automatyczne narzędzia stosowane do identyfikacji informacji o komponentach systemu]. |

| | | |
|---|---|---|
| **CM-13** | **MAPOWANIE DZIAŁAŃ NA DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-13** | opracowano i udokumentowano mapę działań dotyczących danych systemowych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CM-13-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące identyfikacji i dokumentowania lokalizacji informacji; procedury mapowania działań na danych; plan zarządzania konfiguracją; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja projektowa systemu; dokumentacja dotycząca listy danych identyfikacyjnych; dokumentacja dotycząca mapowania danych; zapisy dotyczące kontroli zmian; wykaz komponentów systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CM-13** | **MAPOWANIE DZIAŁAŃ NA DANYCH** | |
| | **CM-13-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie lokalizacją informacji; personel organizacyjny odpowiedzialny za mapowanie działań związanych z danymi; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci; programiści systemu]. |
| | **CM-13-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne regulujące lokalizację informacji; mechanizmy wspierające lub wdrażające mapowanie działań na danych]. |

| | | |
|---|---|---|
| **CM-14** | **PODPISYWANIE KOMPONENTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CM-14_ODP[01]** | ***określono komponenty oprogramowania wymagające weryfikacji podpisanego cyfrowo certyfikatu przed instalacją;*** |
| | **CM-14_ODP[02]** | ***określono komponenty oprogramowania sprzętowego wymagające weryfikacji podpisanego cyfrowo certyfikatu przed instalacją;*** |
| | **CM-14[01]** | instalacja ***<komponentów oprogramowania CM-14_ODP[01]>*** jest niemożliwa, chyba że zostanie zweryfikowane, że oprogramowanie to zostało podpisane cyfrowo przy użyciu certyfikatu uznanego i zatwierdzonego przez organizację; |
| | **CM-14[02]** | instalacja ***<komponentów oprogramowania sprzętowego CM-14_ODP[02]>*** jest niemożliwa, chyba że zostanie zweryfikowane, że oprogramowanie to zostało podpisane cyfrowo przy użyciu certyfikatu uznanego i zatwierdzonego przez organizację; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| CM-14 | PODPISYWANIE KOMPONENTÓW | |
|---|---|---|
| | **CM-14-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania konfiguracją; procedury dotyczące podpisanych cyfrowo certyfikatów dla komponentów oprogramowania i oprogramowania sprzętowego; plan zarządzania konfiguracją; plan bezpieczeństwa systemu;<br>dokumentacja projektowa systemu; zapisy dotyczące zabezpieczania zmian; lista komponentów systemu; plan bezpieczeństwa systemu; inne istotne dokumenty]. |
| | **CM-14-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację podpisanych cyfrowo certyfikatów do celów instalacji komponentów oprogramowania i oprogramowania sprzętowego;<br>personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **CM-14-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne regulujące lokalizację informacji; mechanizmy egzekwujące stosowanie polityki i metod regulowania lokalizacji informacji; automatyczne narzędzia wspierające lub wdrażające podpisy cyfrowe dla komponentów oprogramowania i oprogramowania sprzętowego; automatyczne narzędzia wspierające lub wdrażające weryfikację podpisów cyfrowych dla instalacji komponentów oprogramowania i oprogramowania sprzętowego]. |

## 4.6. KATEGORIA CP - PLANOWANIE AWARYJNE/CIĄGŁOŚĆ DZIAŁANIA

| | | |
|---|---|---|
| **CP-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-01_ODP[01]** | ***określono personel lub role, którym należy przekazać politykę planowania awaryjnego;*** |
| | **CP-01_ODP[02]** | ***określono personel lub role, którym należy przekazać procedury planowania awaryjnego;*** |
| | **CP-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **CP-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami planowania awaryjnego;*** |
| | **CP-01_ODP[05]** | ***określono częstotliwość, z jaką polityka planowania awaryjnego jest przeglądana i aktualizowana;*** |
| | **CP-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji polityki planowania awaryjnego;*** |
| | **CP-01_ODP[07]** | ***określono częstotliwość, z jaką aktualne procedury planowania awaryjnego są przeglądane i aktualizowane;*** |
| | **CP-01_ODP[08]** | ***określono zdarzenia skutkujące koniecznością przeprowadzenia przeglądu i aktualizacji procedur;*** |
| | **CP-01a.[01]** | opracowano i udokumentowano politykę planowania awaryjnego; |
| | **CP-01a.[02]** | polityka zarządzania awaryjnego jest rozpowszechniana wśród ***<personelu lub ról CP-01_ODP[01]>***; |

| CP-01 | POLITYKA I PROCEDURY | |
|---|---|---|
| | **CP-01a.[03]** | opracowano i udokumentowano procedury planowania awaryjnego ułatwiające realizację polityki planowania awaryjnego i związanych z nią zabezpieczeń w tym obszarze; |
| | **CP-01a.[04]** | procedury planowania awaryjnego są rozpowszechniane wśród ***<personelu lub ról CP-01_ODP[02]>***; |
| | **CP-01a.01(a)[01]** | ***<WYBRANA WARTOŚĆ PARAMETRU CP-01_ODP[03]>*** polityka planowania awaryjnego odnosi się do celu; |
| | **CP-01a.01(a)[02]** | ***<WYBRANA WARTOŚĆ PARAMETRU CP-01_ODP[03]>*** polityka planowania awaryjnego odnosi się do zakresu; |
| | **CP-01a.01(a)[03]** | ***<WYBRANA WARTOŚĆ PARAMETRU CP-01_ODP[03]>*** polityka planowania awaryjnego odnosi się do ról; |
| | **CP-01a.01(a)[04]** | ***<WYBRANA WARTOŚĆ PARAMETRU CP-01_ODP[03]>*** polityka planowania awaryjnego odnosi się do obowiązków; |
| | **CP-01a.01(a)[05]** | ***<WYBRANA WARTOŚĆ PARAMETRU CP-01_ODP[03]>*** polityka planowania awaryjnego odnosi się do zaangażowania kierownictwa; |
| | **CP-01a.01(a)[06]** | ***<WYBRANA WARTOŚĆ PARAMETRU CP-01_ODP[03]>*** polityka planowania awaryjnego odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **CP-01a.01(a)[07]** | ***<WYBRANA WARTOŚĆ PARAMETRU CP-01_ODP[03]>*** polityka planowania awaryjnego odnosi się do zgodności; |
| | **CP-01a.01(b)** | polityka planowania awaryjnego ***<WYBRANA WARTOŚĆ PARAMETRU CP-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **CP-01b.** | ***<urzędnik CP-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur planowania awaryjnego; |

| | | |
|---|---|---|
| **CP-01** | **POLITYKA I PROCEDURY** | |
| | **CP-01c.01[01]** | aktualna polityka planowania awaryjnego jest przeglądana i aktualizowana z ***<częstotliwością CP-01_ODP[05]>***; |
| | **CP-01c.01[02]** | aktualna polityka planowania awaryjnego jest przeglądana i aktualizowana po ***<zdarzeniach CP-01_ODP[06]>***; |
| | **CP-01c.02[01]** | aktualne procedury planowania awaryjnego są przeglądane i aktualizowane z ***<częstotliwością CP-01_ODP[07]>***; |
| | **CP-01c.02[02]** | aktualne procedury planowania awaryjnego są przeglądane i aktualizowane po ***<zdarzeniach CP-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury planowania awaryjnego; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CP-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie awaryjne; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **CP-02** | **PLAN CIĄGŁOŚCI DZIAŁANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-02_ODP[01]** | ***określono personel lub role, które mają dokonywać przeglądu planu awaryjnego;*** |
| | **CP-02_ODP[02]** | ***określono personel lub role odpowiedzialne za zatwierdzanie planu awaryjnego;*** |
| | **CP-02_ODP[03]** | ***określono kluczowy personel awaryjny (zidentyfikowany z imienia i nazwiska lub roli), któremu przekazuje się kopie planu awaryjnego;*** |

| CP-02 | PLAN CIĄGŁOŚCI DZIAŁANIA | |
|---|---|---|
| | **CP-02_ODP[04]** | ***określono kluczowe elementy organizacyjne, które otrzymują kopie planu awaryjnego;*** |
| | **CP-02_ODP[05]** | ***określono częstotliwość przeglądów planu awaryjnego;*** |
| | **CP-02_ODP[06]** | ***określono kluczowy personel awaryjny (określony z imienia i nazwiska lub roli), któremu należy przekazać zmiany;*** |
| | **CP-02_ODP[07]** | ***określono kluczowe elementy, organizacji, które należy informować przy wprowadzaniu zmian w planie awaryjnym;*** |
| | **CP-02a.01** | opracowano plan awaryjny dla systemu, który określa zasadnicze kwestie misji i działalności gospodarczej oraz związane z nimi wymagania dotyczące planowania awaryjnego; |
| | **CP-02a.02[01]** | plan awaryjny opracowany dla systemu określa cele w zakresie odzyskiwania; |
| | **CP-02a.02[02]** | plan awaryjny opracowany dla systemu określa priorytety przywracania; |
| | **CP-02a.02[03]** | plan awaryjny opracowany dla systemu określa metryki odbudowy; |
| | **CP-02a.03[01]** | plan awaryjny opracowany dla systemu określa role w sytuacjach awaryjnych; |
| | **CP-02a.03[02]** | plan awaryjny opracowany dla systemu określa obowiązki w sytuacjach awaryjnych; |
| | **CP-02a.03[03]** | plan awaryjny opracowany dla systemu obejmuje wyznaczone osoby wraz z informacjami kontaktowymi; |
| | **CP-02a.04** | plan awaryjny opracowany dla systemu zakłada utrzymanie podstawowych funkcji w zakresie misji i działalności gospodarczej pomimo wystąpienia zakłóceń, naruszeń bezpieczeństwa lub awarii systemu; |

| CP-02 | PLAN CIĄGŁOŚCI DZIAŁANIA | |
|---|---|---|
| | **CP-02a.05** | plan awaryjny opracowany dla systemu zakłada ostateczne przywrócenie pełnej sprawności systemu bez uszczerbku dla pierwotnie zaplanowanych i wdrożonych zabezpieczeń; |
| | **CP-02a.06** | plan awaryjny opracowany dla systemu uwzględnia wymianę informacji w sytuacjach kryzysowych; |
| | **CP-02a.07[01]** | plan awaryjny opracowany dla systemu jest opracowywany i przeglądany przez ***<personel lub role CP-02_ODP[01]>***. |
| | **CP-02a.07[02]** | plan awaryjny opracowany dla systemu jest zatwierdzany przez ***<personel lub role CP-02_ODP[02]>***. |
| | **CP-02b.[01]** | kopie planu awaryjnego są przekazywane ***<kluczowemu personelowi awaryjnemu CP-02_ODP[03]>***; |
| | **CP-02b.[02]** | kopie planu awaryjnego są przekazywane ***<kluczowym elementom organizacyjnym CP-02_ODP[04]>***; |
| | **CP-02c.** | działania związane z planowaniem awaryjnym są skoordynowane z działaniami związanymi z obsługą incydentów; |
| | **CP-02d.** | plan awaryjny dla systemu jest opracowywany i przeglądany z ***<częstotliwością CP-02_ODP[05]>***; |
| | **CP-02e.[01]** | plan awaryjny jest aktualizowany w celu uwzględnienia zmian w organizacji, systemie lub środowisku działania; |
| | **CP-02e.[02]** | plan awaryjny jest aktualizowany w celu uwzględnienia problemów napotkanych podczas jego wdrażania, realizacji lub testowania; |
| | **CP-02f.[01]** | zmiany w planie awaryjnym są przekazywane ***<kluczowemu personelowi awaryjnemu CP-02_ODP[06]>***; |
| | **CP-02f.[02]** | zmiany w planie awaryjnym są przekazywane ***<elementom organizacyjnym CP-02_ODP[07]>***; |

| | | |
|---|---|---|
| **CP-02** | **PLAN CIĄGŁOŚCI DZIAŁANIA** | |
| | **CP-02g.[01]** | wnioski wyciągnięte z testowania planu awaryjnego lub rzeczywistych działań w sytuacjach awaryjnych są włączane do testów planu awaryjnego; |
| | **CP-02g.[02]** | wnioski wyciągnięte ze szkolenia w zakresie planu awaryjnego lub rzeczywistych działań w sytuacjach awaryjnych są włączane do testów i szkoleń dotyczących planowania awaryjnego; |
| | **CP-02h.[01]** | plan awaryjny jest chroniony przed nieuprawnionym ujawnieniem; |
| | **CP-02h.[02]** | plan awaryjny jest chroniony przed nieuprawnioną modyfikacją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące działań awaryjnych dla systemu; plan awaryjny; dowody przeglądów i aktualizacji planu awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sporządzanie i wdrażanie planu awaryjnego; personel organizacyjny odpowiedzialny za obsługę incydentów; personel organizacyjny ze znajomością wymagań dotyczących misji i funkcji biznesowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące opracowania, przeglądu, aktualizacji i ochrony planu awaryjnego; mechanizmy opracowania, przeglądu, aktualizacji lub ochrony planu awaryjnego]. |

| CP-02(01) | PLAN CIĄGŁOŚCI DZIAŁANIA \| KOORDYNACJA Z POWIĄZANYMI PLANAMI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-02(01)** | opracowywanie planu awaryjnego jest koordynowane z elementami organizacyjnymi odpowiedzialnymi za powiązane plany. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-02(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące działań awaryjnych dla systemu; plan awaryjny; plany awaryjne dotyczące działalności; plany odzyskiwania danych po awarii; plany dotyczące ciągłości działania; plany dotyczące komunikacji kryzysowej; plany dotyczące infrastruktury krytycznej; plan reagowania na incydenty cybernetyczne; plany dotyczące reagowania na zagrożenia wewnętrzne; plany awaryjne dla mieszkańców; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-02(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sporządzanie i wdrażanie planów awaryjnych oraz szkolenie w zakresie planowania awaryjnego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel odpowiedzialny za powiązane plany]. |

| CP-02(02) | PLAN CIĄGŁOŚCI DZIAŁANIA \| PLANOWANIE ZDOLNOŚCI DO FUNKCJONOWANIA | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-02(02)[01]** | Planowanie zdolności do funkcjonowania prowadzi się tak, aby podczas działań w sytuacji awaryjnej istniała możliwość podjęcia odpowiednich działań; |

| | | |
|---|---|---|
| **CP-02(02)** | **PLAN CIĄGŁOŚCI DZIAŁANIA \| PLANOWANIE ZDOLNOŚCI DO FUNKCJONOWANIA** | |
| | **CP-02(02)[02]** | Planowanie zdolności do funkcjonowania prowadzi się tak, aby w sytuacji awaryjnej dotyczącej rozwiązań telekomunikacyjnych istniała możliwość podjęcia odpowiednich działań; |
| | **CP-02(02)[03]** | Planowanie zdolności do funkcjonowania prowadzi się tak, aby w sytuacji awaryjnej istniała możliwość podjęcia odpowiednich działań w zakresie utrzymania warunków środowiskowych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące działań awaryjnych dla systemu; plan awaryjny; dokumentacja dotycząca planowania zdolności do funkcjonowania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sporządzanie i wdrażanie planu awaryjnego; personel organizacyjny odpowiedzialny za planowanie zdolności do funkcjonowania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-02(03)** | **PLAN CIĄGŁOŚCI DZIAŁANIA \| WZNAWIANIE PODSTAWOWYCH DZIAŁAŃ I FUNKCJI BIZNESOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-02(03)_ODP[01]** | ***wybrano jedną z następujących WARTOŚCI PARAMETRÓW: {wszystkie; kluczowe};*** |
| | **CP-02(03)_ODP[02]** | ***określono okres uruchomienia planu awaryjnego, w którym należy wznowić działalność w zakresie misji i funkcji biznesowych;*** |

| | | |
|---|---|---|
| **CP-02(03)** | **PLAN CIĄGŁOŚCI DZIAŁANIA \| WZNAWIANIE PODSTAWOWYCH DZIAŁAŃ I FUNKCJI BIZNESOWYCH** | |
| | **CP-02(03)** | planowe wznowienie***<WYBRANA WARTOŚĆ PARAMETRU CP-02(03)_ODP[01]>*** działalności w zakresie misji i funkcji biznesowych odbywa się w ***<okresie CP-02(03)_ODP[02]> od*** uruchomienia planu awaryjnego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-02(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące działań awaryjnych dla systemu; plan awaryjny; ocena wpływu na działalność; plan bezpieczeństwa systemu; plan ochrony prywatności; inne powiązane plany; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-02(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sporządzanie i wdrażanie planu awaryjnego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny posiadający wiedzę na temat wymagań dotyczących misji i funkcji biznesowych]. |
| | **CP-02(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wznawiania działalności w zakresie misji i funkcji biznesowych]. |

| | |
|---|---|
| **CP-02(04)** | **PLAN CIĄGŁOŚCI DZIAŁANIA \| PRZYWRÓCENIE DZIAŁANIA WSZYSTKICH FUNKCJI BIZNESOWYCH** |
| | [WYCOFANE: Włączone do CP-02(03)]. |

| | | |
|---|---|---|
| **CP-02(05)** | **PLAN CIĄGŁOŚCI DZIAŁANIA \| KONTYNUACJA NIEZBĘDNYCH DZIAŁAŃ I FUNKCJI BIZNESOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-02(05)_ODP** | ***wybrano jedną z następujących WARTOŚCI PARAMETRÓW: {wszystkie; kluczowe};*** |
| | **CP-02(05)[01]** | planuje się kontynuowanie działalności w zakresie misji i funkcji biznesowych ***<WYBRANA WARTOŚC PARAMETRU CP-02(05)_ODP>*** przy minimalnej utracie ciągłości działalności lub bez jej utraty; |
| | **CP-02(05)[02]** | ciągłość działania zapewniana jest do czasu pełnego przywrócenia pierwotnego funkcjonowania systemu w głównych miejscach przetwarzania lub przechowywania danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-02(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące działań awaryjnych dla systemu; plan awaryjny; ocena wpływu na działalność; umowy dotyczące głównego miejsca przetwarzania; umowy dotyczące głównego miejsca przechowywania; umowy dotyczące zapasowego miejsca przetwarzania; umowy dotyczące zapasowego miejsca przechowywania; dokumentacja testów planu awaryjnego; wyniki testów planu awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-02(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za tworzenie i wdrażanie planów awaryjnych; personel organizacyjny znający wymagania dotyczące działalności biznesowej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-02(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wznawiania działalności w zakresie misji i funkcji biznesowych]. |

| | | |
|---|---|---|
| **CP-02(06)** | **PLAN CIĄGŁOŚCI DZIAŁANIA \| ZAPASOWE MIEJSCA PRZETWARZANIA I PRZECHOWYWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-02(06)_ODP** | ***wybrano jedną z następujących WARTOŚCI PARAMETRÓW: {wszystkie; kluczowe};*** |
| | **CP-02(06)[01]** | zaplanowano przeniesienie ***<WYBRANA WARTOŚĆ PARAMETRU CP-02(06)_ODP>*** działalności w zakresie misji i funkcji biznesowych do zapasowych miejsc przetwarzania lub przechowywania przy minimalnej lub żadnej utracie ciągłości działania; |
| | **CP-02(06)[02]** | ciągłość działania zapewniana jest do czasu pełnego przywrócenia pierwotnego funkcjonowania systemu w głównych miejscach przetwarzania lub przechowywania danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-02(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące działań awaryjnych dla systemu; plan awaryjny; ocena wpływu na działalność; umowy dotyczące zapasowego miejsca przetwarzania; umowy dotyczące zapasowego miejsca przechowywania; dokumentacja testowa planu awaryjnego; wyniki testów planu awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-02(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za tworzenie i wdrażanie planów awaryjnych; personel organizacyjny znający wymagania dotyczące działalności biznesowej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-02(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przeniesienia głównej działalności w zakresie misji i funkcji biznesowych do zapasowych miejsc przetwarzania/magazynowania]. |

| | | |
|---|---|---|
| **CP-02(07)** | **PLAN CIĄGŁOŚCI DZIAŁANIA \| KOORDYNACJA Z USŁUGODAWCAMI ZEWNĘTRZNYMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-02(07)** | plan awaryjny jest skoordynowany z planami awaryjnymi zewnętrznych dostawców usług, aby zapewnić możliwość spełnienia wymagań dotyczących planowania awaryjnego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-02(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące działań awaryjnych dla systemu; plan awaryjny; plany awaryjne zewnętrznych dostawców usług; umowy o poziomie usług; wymagania dotyczące planu awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-02(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sporządzanie i wdrażanie planu awaryjnego; zewnętrzni dostawcy usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-02(08)** | **PLAN CIĄGŁOŚCI DZIAŁANIA \| IDENTYFIKACJA ZASOBÓW KRYTYCZNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-02(08)_ODP** | ***wybrano jedną z następujących WARTOŚCI PARAMETRÓW: {wszystkie; kluczowe};*** |
| | **CP-02(08)** | określono krytyczne zasoby systemu wspierające ***<WYBRANA WARTOŚĆ PARAMETRU CP-02(08)_ODP>***<br>działalność w zakresie misji i funkcji biznesowych. |

| | | |
|---|---|---|
| **CP-02(08)** | **PLAN CIĄGŁOŚCI DZIAŁANIA \| IDENTYFIKACJA ZASOBÓW KRYTYCZNYCH** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-02(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące działań awaryjnych dla systemu; plan awaryjny; ocena wpływu na działalność; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-02(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za tworzenie i wdrażanie planów awaryjnych; personel organizacyjny znający wymagania dotyczące działalności biznesowej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-03** | **SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-03_ODP[01]** | ***określono okres, w którym należy przeprowadzić szkolenie dot. planowania awaryjnego dla użytkowników obejmujących rolę lub obowiązki, które obejmują sytuacje awaryjne;*** |
| | **CP-03_ODP[02]** | ***określono częstotliwość, z jaką należy przeprowadzać szkolenia dla użytkowników systemu, których rola lub obowiązki dotyczą planowania awaryjnego;*** |
| | **CP-03_ODP[03]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji treści szkolenia dot. planowania awaryjnego;*** |
| | **CP-03_ODP[04]** | ***określono zdarzenia wymagające przeglądu i aktualizacji szkolenia dot. planowania awaryjnego;*** |

| | | |
|---|---|---|
| **CP-03** | **SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA** | |
| | **CP-03a.01** | szkolenie dot. planowania awaryjnego jest zapewniane użytkownikom systemu zgodnie z przypisanymi rolami i obowiązkami w ***<okresie CP-03_ODP[01]>*** od objęcia roli lub zakresu odpowiedzialności, które dotyczą planowania awaryjnego. |
| | **CP-03a.02** | jeśli wymagają tego zmiany w systemie, przeprowadza się szkolenie dot. planowania awaryjnego zgodnie z przypisanymi rolami i obowiązkami; |
| | **CP-03a.03** | szkolenie dot. planowania awaryjnego jest następnie zapewniane użytkownikom systemu zgodnie z przypisanymi rolami i obowiązkami z ***<częstotliwością CP-03_ODP[02]>***; |
| | **CP-03b.[01]** | treść szkolenia dot. planowania awaryjnego jest przeglądana i aktualizowana z ***<częstotliwością CP-03_ODP[03]>***; |
| | **CP-03b.[02]** | treść szkolenia dot. planowania awaryjnego jest weryfikowana i aktualizowana po ***<zdarzeniach CP-03_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące szkolenia dot. sytuacjach awaryjnych; plan awaryjny; program szkolenia w sytuacjach awaryjnych; materiały szkoleniowe w sytuacjach awaryjnych; zapisy szkolenia w sytuacjach awaryjnych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za tworzenie i wdrażanie planów awaryjnych oraz szkolenie w tym zakresie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CP-03-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie szkolenia dot. planowania awaryjnego]. |

| | | |
|---|---|---|
| **CP-03(01)** | **SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA \| ZDARZENIA SYMULOWANE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-03(01)** | do szkolenia awaryjnego włącza się zdarzenia symulowane, aby ułatwić personelowi skuteczne reagowanie w sytuacjach kryzysowych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury w zakresie szkolenia dot. planowania awaryjnego; plan awaryjny; program szkolenia dot. planowania awaryjnego; materiały do szkoleń dot. planowania awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za tworzenie i wdrażanie planów awaryjnych oraz szkolenie w tym zakresie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CP-03(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie szkoleń dot. planowania awaryjnego; mechanizmy symulacji zdarzeń awaryjnych]. |

| | | |
|---|---|---|
| **CP-03(02)** | **SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA \| ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-03(02)** | mechanizmy stosowane w działalności są wykorzystywane w celu zapewnienia bardziej szczegółowego i realistycznego środowiska do szkolenia w zakresie planowania awaryjnego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CP-03(02)** | **SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA \| ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE** | |
| | **CP-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury w zakresie szkolenia dot. planowania awaryjnego; plan awaryjny; program szkolenia dot. planowania awaryjnego; materiały do szkoleń dot. planowania awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za tworzenie i wdrażanie planów awaryjnych oraz szkolenie w tym zakresie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **CP-03(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie szkolenia dot. planowania awaryjnego; mechanizmy zapewnienia środowiska szkolenia dot. planowania awaryjnego]. |

| | | |
|---|---|---|
| **CP-04** | **TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-04_ODP[01]** | ***określono częstotliwość testowania planu awaryjnego systemu;*** |
| | **CP-04_ODP[02]** | ***określono testy służące do weryfikacji skuteczności planu awaryjnego;*** |
| | **CP-04_ODP[03]** | ***określono testy wskazujące na gotowość do realizacji planu awaryjnego;*** |
| | **CP-04a.[01]** | plan awaryjny dla systemu jest testowany z ***<częstotliwością CP-04_ODP[01]>***; |
| | **CP-04a.[02]** | do określenia skuteczności planu wykorzystuje się ***<testy <CP-04_ODP[02]>***; |
| | **CP-04a.[03]** | do określenia gotowości do realizacji planu stosuje się ***<testy CP-04_ODP[03]>***; |

| | | |
|---|---|---|
| **CP-04** | **TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA** | |
| | **CP-04b.** | dokonuje się przeglądu wyników testów planu awaryjnego; |
| | **CP-04c.** | w razie potrzeby rozpoczyna się działania naprawcze. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące testowania planu awaryjnego; plan awaryjny; dokumentacja z testów planu awaryjnego; wyniki testów planu awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za testowanie lub przegląd planów awaryjnych, bądź reagowanie na ich testy; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-04-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące testowania planu awaryjnego; mechanizmy wspierające plan awaryjny lub testowanie planu awaryjnego]. |

| | | |
|---|---|---|
| **CP-04(01)** | **TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA \| KOORDYNACJA Z POWIĄZANYMI PLANAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-04(01)** | testowanie planów awaryjnych jest koordynowane z elementami organizacyjnymi odpowiedzialnymi za plany powiązane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CP-04(01)** | **TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA \| KOORDYNACJA Z POWIĄZANYMI PLANAMI** | |
| | **CP-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; polityka reagowania na incydenty; procedury dotyczące testowania planu awaryjnego; dokumentacja testowania planu awaryjnego; plan awaryjny; plany ciągłości działania; plany odzyskiwania danych po awarii; plany komunikacji kryzysowej; plany infrastruktury krytycznej; plany reagowania na incydenty cybernetyczne; plany awaryjne dla mieszkańców; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za testowanie planów awaryjnych; personel odpowiedzialny za plany powiązane; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-04(02)** | **TESTOWANIE PLANU AWARYJNEGO \|ZAPASOWE MIEJSCE PRZETWARZANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-04(02)(a)** | plan awaryjny jest testowany w zapasowym miejscu przetwarzania w celu zapoznania personelu awaryjnego z obiektem i dostępnymi zasobami; |
| | **CP-04(02)(b)** | plan awaryjny jest testowany w zapasowym miejscu przetwarzania w celu oceny zdolności tegoż miejsca do wspierania działalności w sytuacjach awaryjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| CP-04(02) | TESTOWANIE PLANU AWARYJNEGO \|ZAPASOWE MIEJSCE PRZETWARZANIA | |
|---|---|---|
| | **CP-04(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące testowania planu awaryjnego; plan awaryjny; dokumentacja testowa planu awaryjnego; wyniki testów planu awaryjnego; umowy dotyczące zapasowego miejsca przetwarzania; umowy o poziomie usług; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-04(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie awaryjne i realizację planu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-04(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące testowania planu awaryjnego; mechanizmy wspierające plan awaryjny lub testowanie planu awaryjnego]. |

| CP-04(03) | TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA \| TESTOWANIE AUTOMATYCZNE | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-04(03)_ODP** | ***określono automatyczne mechanizmy testowania planów awaryjnych;*** |
| | **CP-04(03)** | plan awaryjny testowany jest przy użyciu ***<mechanizmów automatycznych CP-O4(03)_ODP>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-04(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące testowanie planu awaryjnego; plan awaryjny; automatyczne mechanizmy wspierające testowanie planu awaryjnego; dokumentacja z testu planu awaryjnego; wyniki testu planu awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| CP-04(03) | TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA \| TESTOWANIE AUTOMATYCZNE | |
|---|---|---|
| | **CP-04(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za testowanie planów awaryjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-04(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące testowania planu awaryjnego; automatyczne mechanizmy wspierające testowanie planów awaryjnych]. |

| CP-04(04) | TESTOWANIE PLANU AWARYJNEGO \| PEŁNE ODZYSKIWANIE I ODTWARZANIE | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-04(04)[01]** | elementem planu testowania w sytuacjach awaryjnych jest pełne odzyskanie systemu i przywrócenie go do znanego stanu; |
| | **CP-04(04)[02]** | elementem planu testowania w sytuacjach awaryjnych jest pełne odtworzenie systemu i przywrócenie go do znanego stanu; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-04(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące odzyskiwania i przywracania systemu; plan awaryjny; dokumentacja testów planu awaryjnego; wyniki testów planu awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-04(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za testowanie planu awaryjnego; personel organizacyjny odpowiedzialny za odzyskiwanie i odtwarzanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| **CP-04(04)** | **TESTOWANIE PLANU AWARYJNEGO \| PEŁNE ODZYSKIWANIE I ODTWARZANIE** | |
|---|---|---|
| | **CP-04(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne testowania planu awaryjnego; mechanizmy wspierające testowanie planu awaryjnego; mechanizmy wspierające odzyskiwanie i odtwarzanie systemu]. |

| **CP-04(05)** | **TESTOWANIE PLANU AWARYJNEGO \|PRÓBNE AWARIE** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-04(05)_ODP[01]** | ***określono mechanizmy stosowane w celu zakłócenia systemu bądź jego komponentów lub wywarcia na nie innego negatywnego wpływu;*** |
| | **CP-04(05)_ODP[02]** | ***określono systemu lub komponentu systemu, w którym mają być zastosowane mechanizmy zakłócające;*** |
| | **CP-04(05)** | stosuje się ***<mechanizmy CP-04(05)_ODP[01]> w*** celu zakłócenia i wywarcia negatywnego wpływu na ***<system lub komponent systemu CP-04(05)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-04(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące odzyskiwania i przywracania systemu; plan awaryjny; dokumentacja testów planu awaryjnego; wyniki testów planu awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-04(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za testowanie planu awaryjnego; personel organizacyjny odpowiedzialny za odzyskiwanie i odtwarzanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-04(05)** | **TESTOWANIE PLANU AWARYJNEGO \|PRÓBNE AWARIE** | |
| | **CP-04(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne testowania planów awaryjnych; mechanizmy wspierające testowanie planów awaryjnych]. |

| | |
|---|---|
| **CP-05** | **AKTUALIZACJA PLANU CIĄGŁOŚCI DZIAŁANIA** |
| | [WYCOFANE: Włączone do CP-02]. |

| | | |
|---|---|---|
| **CP-06** | **ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-06a.[01]** | ustanowiono zapasowe miejsce przechowywania; |
| | **CP-06a.[02]** | czynności w zakresie ustanowienia zapasowego miejsca przechowywania obejmowały niezbędne umowy umożliwiające przechowywanie i pobieranie kopii zapasowych informacji systemowych; |
| | **CP-06b.** | zapasowe miejsce przechowywania zapewnia zabezpieczenia równoważne do tych w miejscu podstawowym. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące zapasowych miejsc przechowywania; plan awaryjny; umowy dotyczące zapasowych miejsc przechowywania; umowy dotyczące głównego miejsca przechowywania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CP-06** | **ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII** | |
| | **CP-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zapasowe miejsce przechowywania kopii w ramach planu awaryjnego; personel organizacyjny odpowiedzialny za odzyskiwanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przechowywania i pobierania informacji o kopii zapasowej systemu w zapasowym miejscu przechowywania; mechanizmy wspierające lub wdrażające przechowywanie i pobieranie informacji o kopii zapasowej systemu w zapasowym miejscu przechowywania]. |

| | | |
|---|---|---|
| **CP-06(01)** | **ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII \| ODDZIELENIE OD LOKALIZACJI GŁÓWNEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-06(01)** | określono zapasowe miejsce przechowywania, które jest oddzielone od głównego miejsca przechowywania w stopniu wystarczającym do zmniejszenia podatności na te same zagrożenia. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-06(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące zapasowych miejsc przechowywania; plan awaryjny; zapasowe miejsce przechowywania; umowy dotyczące alternatywnego miejsca przechowywania; umowy dotyczące głównego miejsca przechowywania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CP-06(01)** | **ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII \| ODDZIELENIE OD LOKALIZACJI GŁÓWNEJ** | |
| | **CP-06(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zapasowe miejsce przechowywania kopii w ramach planu awaryjnego; personel organizacyjny odpowiedzialny za odzyskiwanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-06(02)** | **ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII \| CZAS ODZYSKIWANIA I PUNKT ODTWORZENIA DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-06(02)[01]** | zapasowe miejsce przechowywania jest skonfigurowane tak, aby ułatwić przeprowadzenie operacji odzyskiwania zgodnie z celami dotyczącymi czasu odzyskiwania; |
| | **CP-06(02)[02]** | zapasowe miejsce przechowywania jest skonfigurowane tak, aby ułatwić przeprowadzenie operacji odzyskiwania zgodnie z celami dotyczącymi punktu odzyskiwania; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-06(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące zapasowych miejsc przechowywania; plan awaryjny; zapasowe miejsce przechowywania; umowy dotyczące zapasowego miejsca przechowywania; konfiguracje zapasowego miejsca przechowywania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-06(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za testowanie planów awaryjnych; personel organizacyjny odpowiedzialny za testowanie planów powiązanych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-06(02)** | **ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII \| CZAS ODZYSKIWANIA I PUNKT ODTWORZENIA DANYCH** | |
| | **CP-06(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne testowania planów awaryjnych; mechanizmy wspierające kwestie związane z czasem odzyskiwania i punktem odtworzenia danych]. |

| | | |
|---|---|---|
| **CP-06(03)** | **ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII \| DOSTĘPNOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-06(03)[01]** | określono potencjalne problemy z dostępnością do zapasowego miejsca przechowywania w przypadku zakłóceń lub katastrofy na skalę regionalną; |
| | **CP-06(03)[02]** | przedstawiono wyraźne działania łagodzące w celu rozwiązania zidentyfikowanych problemów z dostępnością. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-06(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące zapasowych miejsc przechowywania; plan awaryjny; zapasowe miejsce przechowywania; wykaz potencjalnych problemów z dostępnością do zapasowego miejsca przechowywania; działania łagodzące problemy z dostępnością do zapasowego miejsca przechowywania; oceny ryzyka dla organizacji; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-06(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zapasowe miejsce przechowywania kopii w ramach planu awaryjnego; personel organizacyjny odpowiedzialny za odzyskiwanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-07** | **ZAPASOWE MIEJSCE PRZETWARZANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-07_ODP[01]** | ***określono operacje systemowe dla podstawowych funkcji w zakresie misji i działalności biznesowej;*** |
| | **CP-07_ODP[02]** | ***określono okres zgodny z celami dot. czasu i punktu odzyskiwania;*** |
| | **CP-07a.** | zapasowe miejsce przetwarzania, wraz z niezbędnymi umowami umożliwiającymi przeniesienie i wznowienie ***<CP-07_ODP[01] operacji systemowych>*** obejmujących istotne funkcje w zakresie misji i działalności biznesowej, zostaje ustanowione w ciągu ***<okres CP-07_ODP[02]>***, jeżeli podstawowe zdolności do przetwarzania są niedostępne; |
| | **CP-07b.[01]** | sprzęt i materiały wymagane do przeniesienia operacji są dostępne w zapasowym miejscu przetwarzania bądź też zawarto umowy ws. wsparcia realizacji dostaw do tego miejsca w ciągu ***<okres CP-07_ODP[02]>*** w celu dokonania takiego przeniesienia; |
| | **CP-07b.[02]** | sprzęt i materiały wymagane do wznowienia operacji są dostępne w zapasowym miejscu przetwarzania bądź też zawarto umowy ws. wsparcia realizacji dostaw do tego miejsca w ciągu ***<okres CP-07_ODP[02]>*** w celu dokonania takiego przeniesienia; |
| | **CP-07c.** | zabezpieczenia zapewnione w zapasowym miejscu przetwarzania są równoważne z tymi dostępnymi w miejscu podstawowym. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CP-07** | **ZAPASOWE MIEJSCE PRZETWARZANIA** | |
| | **CP-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące zapasowych miejsc przetwarzania; plan awaryjny; umowy dotyczące zapasowego miejsca przetwarzania; umowy dotyczące głównego miejsca przetwarzania; lista zapasowego sprzętu i materiałów w zapasowym miejscu przetwarzania; umowy dotyczące sprzętu i dostaw; umowy o poziomie usług; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie awaryjne lub zapewnienie zapasowego miejsca przechowywania/przetwarzania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-07-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące odzyskiwania danych w zapasowym miejscu przetwarzania; mechanizmy wspierające lub wdrażające odzyskiwanie danych w zapasowym miejscu przetwarzania]. |

| | | |
|---|---|---|
| **CP-07(01)** | **ZAPASOWE MIEJSCE PRZETWARZANIA \| ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-07(01)** | określono zapasowe miejsce przetwarzania, które jest wystarczająco oddzielone od podstawowej lokalizacji przetwarzania, aby zmniejszyć podatność na te same zagrożenia. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CP-07(01)** | **ZAPASOWE MIEJSCE PRZETWARZANIA \| ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ** | |
| | **CP-07(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące zapasowych miejsc przetwarzania; plan awaryjny; zapasowe miejsce przetwarzania; umowy dotyczące zapasowych miejsc przetwarzania; umowy dotyczące głównego miejsca przetwarzania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-07(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zapasowe miejsca przetwarzania w ramach planu awaryjnego; personel organizacyjny odpowiedzialny za odzyskiwanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-07(02)** | **ZAPASOWE MIEJSCE PRZETWARZANIA \| DOSTĘPNOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-07(02)[01]** | określono potencjalne problemy z dostępnością do zapasowych miejsc przetwarzania w przypadku zakłóceń lub katastrofy na skalę regionalną; |
| | **CP-07(02)[02]** | przedstawiono wyraźne działania łagodzące w celu rozwiązania zidentyfikowanych problemów z dostępnością. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-07(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące zapasowych miejsc przetwarzania; plan awaryjny; zapasowe miejsce przetwarzania; umowy dotyczące zapasowych miejsc przetwarzania; umowy dotyczące głównego miejsca przetwarzania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **CP-07(02)** | **ZAPASOWE MIEJSCE PRZETWARZANIA \| DOSTĘPNOŚĆ** | |
| | **CP-07(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zapasowe miejsca przetwarzania w ramach planu awaryjnego; personel organizacyjny odpowiedzialny za odzyskiwanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-07(03)** | **ZAPASOWE MIEJSCE PRZETWARZANIA \| PRIORYTET USŁUG** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-07(03)** | sporządzono umowy dotyczące zapasowych miejsc przetwarzania, które zawierają postanowienia dotyczące pierwszeństwa obsługi, zgodnie z wymogami dostępności (w tym cele dotyczące czasu odzyskiwania). |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-07(03)-Badanie** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie awaryjne w zapasowym miejscu przetwarzania; personel organizacyjny odpowiedzialny za odzyskiwanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zakupy/umowy]. |
| | **CP-07(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za plan awaryjny w zapasowym miejscu przetwarzania; personel organizacyjny odpowiedzialny za odzyskiwanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zakupy/umowy]. |

| | | |
|---|---|---|
| **CP-07(04)** | **ZAPASOWE MIEJSCE PRZETWARZANIA \| GOTOWOŚĆ DO UŻYCIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-07(04)** | zastępcze miejsce przetwarzania jest przygotowane tak, by mogło służyć jako miejsce operacyjne wspierające podstawowe funkcje w zakresie misji i działalności biznesowej. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-07(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące zapasowych miejsc przetwarzania; plan awaryjny; zapasowe miejsce przetwarzania; umowy dotyczące zapasowego miejsca przetwarzania; konfiguracja zapasowego miejsca przetwarzania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-07(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zapasowe miejsca przetwarzania w ramach planu awaryjnego; personel organizacyjny odpowiedzialny za odzyskiwanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-07(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające odzyskiwanie systemu w zapasowym miejscu przetwarzania]. |

| | | |
|---|---|---|
| **CP-07(05)** | **ZAPASOWE MIEJSCE PRZETWARZANIA \| ZASTĘPCZE ŚRODKI BEZPIECZEŃSTWA** | |
| | [WYCOFANE: Włączone do CP-07]. | |

| | | |
|---|---|---|
| **CP-07(06)** | **ZAPASOWE MIEJSCE PRZETWARZANIA \| BRAK MOŻLIWOŚCI POWROTU DO LOKALIZACJI PODSTAWOWEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-07(06)[01]** | w planowaniu uwzględniono okoliczności uniemożliwiające powrót do podstawowego miejsca przetwarzania; |
| | **CP-07(06)[02]** | w ramach przygotowań uwzględniono okoliczności uniemożliwiające powrót do podstawowego miejsca przetwarzania; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-07(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące zapasowych miejsc przetwarzania; plan awaryjny; zapasowe miejsce przetwarzania; umowy dotyczące zapasowego miejsca przetwarzania; konfiguracja zapasowego miejsca przetwarzania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-07(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za odtworzenie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-08** | **USŁUGI TELEKOMUNIKACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-08_ODP[01]** | ***określono operacje systemowe, które mają być wznowione w celu przywrócenia podstawowych funkcji w zakresie misji i działalności biznesowej;*** |
| | **CP-08_ODP[02]** | ***określono okres, w którym należy wznowić zasadnicze funkcje w zakresie misji i działalności, gdy podstawowe możliwości telekomunikacyjne są niedostępne;*** |

| | | |
|---|---|---|
| **CP-08** | **USŁUGI TELEKOMUNIKACYJNE** | |
| | **CP-08** | zapewniono alternatywne usługi telekomunikacyjne, w tym umowy niezbędne do umożliwienia wznowienia ***<operacji systemowych CP-08_ODP[01]>*** do celów realizacji podstawowych funkcji w zakresie misji i działalności biznesowej w ***<CP-08_ODP[02] okresie>***, jeśli podstawowe usługi telekomunikacyjne są niedostępne w głównych lub zapasowych miejscach przetwarzania lub przechowywania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące alternatywnych usług telekomunikacyjnych; plan awaryjny; umowy dotyczące podstawowych i alternatywnych usług telekomunikacyjnych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za telekomunikacyjny plan awaryjny; personel organizacyjny odpowiedzialny za odzyskiwanie systemu; personel organizacyjny znający wymagania dotyczące misji i funkcji biznesowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zakupy/umowy]. |
| | **CP-08-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające telekomunikację]. |

| | | |
|---|---|---|
| **CP-08(01)** | **USŁUGI TELEKOMUNIKACYJNE \| PRIORYTETY ŚWIADCZENIA USŁUG** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-08(01)(a)[01]** | sporządzono podstawowe umowy o świadczenie usług telekomunikacyjnych, które zawierają postanowienia dotyczące priorytetów świadczenia usług zgodnie z wymogami dostępności (w tym cele dotyczące czasu odzyskiwania); |

| | | |
|---|---|---|
| **CP-08(01)** | **USŁUGI TELEKOMUNIKACYJNE \| PRIORYTETY ŚWIADCZENIA USŁUG** | |
| | **CP-08(01)(a)[02]** | sporządzono dodatkowe umowy o świadczenie usług telekomunikacyjnych, które zawierają postanowienia dotyczące priorytetów świadczenia usług zgodnie z wymogami dostępności (w tym cele dotyczące czasu odzyskiwania); |
| | **CP-08(01)(b)** | Wymagany jest priorytet świadczenia usług w przypadku wszystkich usług telekomunikacyjnych wykorzystywanych w ramach przygotowań na wypadek zagrożenia bezpieczeństwa narodowego, jeżeli podstawowe lub alternatywne usługi telekomunikacyjne są świadczone przez publicznego dostawcę usług telekomunikacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-08(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące podstawowych i alternatywnych usług telekomunikacyjnych; plan awaryjny; umowy dotyczące podstawowych i alternatywnych usług telekomunikacyjnych; dokumentacja dotycząca priorytetów usług telekomunikacyjnych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-08(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za telekomunikacyjny plan awaryjny; personel organizacyjny odpowiedzialny za odzyskiwanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zakupy/umowy]. |
| | **CP-08(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające telekomunikację]. |

| | | |
|---|---|---|
| **CP-08(02)** | **USŁUGI TELEKOMUNIKACYJNE \| POJEDYNCZE PUNKTY AWARII** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-08(02)** | pozyskano alternatywne usługi telekomunikacyjne, zmniejszające prawdopodobieństwo współdzielenia pojedynczego punktu podatności na awarię z podstawowymi usługami telekomunikacyjnymi. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-08(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące podstawowych i alternatywnych usług telekomunikacyjnych; plan awaryjny; umowy dotyczące podstawowych i alternatywnych usług telekomunikacyjnych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-08(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za plan awaryjny w zakresie telekomunikacji; personel organizacyjny odpowiedzialny za odtwarzanie systemu; główni i alternatywni dostawcy usług telekomunikacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-08(03)** | **USŁUGI TELEKOMUNIKACYJNE \| ROZDZIELENIE DOSTAWCÓW PODSTAWOWYCH I ALTERNATYWNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-08(03)** | w celu zmniejszenia podatności na te same zagrożenia pozyskano zastępcze usługi telekomunikacyjne od dostawców innych niż dostawcy usług podstawowych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **CP-08(03)** | **USŁUGI TELEKOMUNIKACYJNE \| ROZDZIELENIE DOSTAWCÓW PODSTAWOWYCH I ALTERNATYWNYCH** | |
| | **CP-08(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące podstawowych i alternatywnych usług telekomunikacyjnych; plan awaryjny; umowy dotyczące podstawowych i alternatywnych usług telekomunikacyjnych; siedziba alternatywnego dostawcy usług telekomunikacyjnych; siedziba podstawowego dostawcy usług telekomunikacyjnych; inne istotne dokumenty lub zapisy]. |
| | **CP-08(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za plan awaryjny w zakresie telekomunikacji; personel organizacyjny odpowiedzialny za odtwarzanie systemu; główni i alternatywni dostawcy usług telekomunikacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-08(04)** | **USŁUGI TELEKOMUNIKACYJNE \| PLAN AWARYJNY DOSTAWCY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-08(04)_ODP[01]** | ***określono częstotliwość, z jaką należy uzyskiwać dowody realizacji testów dot. planowania awaryjnego przez świadczeniodawców;*** |
| | **CP-08(04)_ODP[02]** | ***określono częstotliwość, z jaką należy uzyskiwać od dostawców dowody na odbycie przez usługodawcę szkolenia dot. planowania awaryjnego;*** |
| | **CP-08(04)(a)[01]** | dostawcy podstawowych usług telekomunikacyjnych są zobowiązani do posiadania planów awaryjnych; |
| | **CP-08(04)(a)[02]** | dostawcy zapasowych usług telekomunikacyjnych są zobowiązani do posiadania planów awaryjnych; |
| | **CP-08(04)(b)** | plany awaryjne dostawców są poddawane przeglądowi w celu zapewnienia, że plany te spełniają wymogi organizacji w zakresie planowania awaryjnego; |

| | | |
|---|---|---|
| **CP-08(04)** | **USŁUGI TELEKOMUNIKACYJNE \| PLAN AWARYJNY DOSTAWCY** | |
| | **CP-08(04)(c)[01]** | dowody na przeprowadzanie testów dot. planowania awaryjnego przez usługodawców uzyskuje się z ***<częstotliwościąCP-08(04)_ODP[01]***>. |
| | **CP-08(04)(c)[02]** | dowody na przeprowadzanie szkolenia dot. planowania awaryjnego przez usługodawców uzyskuje się z ***<częstotliwością CP-08(04)_ODP[01]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-08(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie planowania awaryjnego; procedury dotyczące podstawowych i alternatywnych usług telekomunikacyjnych; plan awaryjny; plany awaryjne dostawców; dowody testów/szkoleń prowadzonych przez dostawców w zakresie planowania awaryjnego; umowy dotyczące podstawowych i alternatywnych usług telekomunikacyjnych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-08(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie awaryjne, wdrażanie planu i testowanie; główni i alternatywni dostawcy usług telekomunikacyjnych;<br>dostawcy usług telekomunikacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zakupy/umowy]. |

| | | |
|---|---|---|
| **CP-08(05)** | **USŁUGI TELEKOMUNIKACYJNE \| TESTOWANIE ALTERNATYWNYCH USŁUG TELEKOMUNIKACYJNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-08(05)_ODP** | ***określono częstotliwość, z jaką testowane są alternatywne usługi telekomunikacyjne;*** |

| | | |
|---|---|---|
| **CP-08(05)** | **USŁUGI TELEKOMUNIKACYJNE \| TESTOWANIE ALTERNATYWNYCH USŁUG TELEKOMUNIKACYJNYCH** | |
| | **CP-08(05)** | alternatywne usługi telekomunikacyjne testowane są z***<częstotliwością CP-08(05)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-08(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące alternatywnych usług telekomunikacyjnych; plan awaryjny; dowody testowania alternatywnych usług telekomunikacyjnych; umowy dotyczące alternatywnych usług telekomunikacyjnych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-08(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie awaryjne, wdrażanie planu i testowanie; alternatywni dostawcy usług telekomunikacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji. |
| | **CP-08(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające testowanie alternatywnych usług telekomunikacyjnych]. |

| | | |
|---|---|---|
| **CP-09** | **KOPIA ZAPASOWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-09_ODP[01]** | ***określono komponenty systemu, w przypadku których sporządza się kopie zapasowe informacji na poziomie użytkownika;*** |
| | **CP-09_ODP[02]** | ***określono częstotliwość, z jaką należy wykonywać kopie zapasowe informacji na poziomie użytkownika, zgodnie z celami dotyczącymi czasu i punktu odzyskiwania;*** |

| | | |
|---|---|---|
| **CP-09** | **KOPIA ZAPASOWA** | |
| | **CP-09_ODP[03]** | ***określono częstotliwość, z jaką należy wykonywać kopie zapasowe informacji na poziomie systemu, zgodnie z celami dotyczącymi czasu i punktu odzyskiwania;*** |
| | **CP-09_ODP[04]** | ***określono częstotliwość wykonywania kopii zapasowych dokumentacji systemowej która jest zgodna z celami dotyczącymi czasu i punktu odzyskiwania;*** |
| | **CP-09a.** | kopie zapasowe informacji na poziomie użytkownika zawartych w ***<CP-09_ODP[01] elementach systemu>*** są wykonywane z ***<częstotliwością CP-09_ODP[02]*** >; |
| | **CP-09b.** | sporządza się kopie zapasowe informacji na poziomie systemu z ***<częstotliwością CP-09_ODP[03]>***; |
| | **CP-09c.** | sporządza się kopie zapasowe dokumentacji systemowej, w tym dokumentacji związanej z bezpieczeństwem i prywatnością, z ***<częstotliwością CP-09_ODP[04]>***; |
| | **CP-09d.[01]** | poufność informacji zawartych w kopii zapasowej jest chroniona; |
| | **CP-09d.[02]** | integralność kopii zapasowej informacji jest chroniona; |
| | **CP-09d.[03]** | dostępność kopii zapasowej informacji jest chroniona. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu; plan awaryjny; miejsce/miejsca przechowywania kopii zapasowych; dzienniki lub zapisy kopii zapasowych systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **CP-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kopie zapasowe systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **CP-09** | **KOPIA ZAPASOWA** | |
| | **CP-09-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące prowadzenia kopii zapasowych systemu; mechanizmy wspierające lub wdrażające kopie zapasowe systemu]. |

| | | |
|---|---|---|
| **CP-09(01)** | **KOPIA ZAPASOWA \| BADANIE NIEZAWODNOŚCI NOŚNIKÓW/INTEGRALNOŚCI INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-09(01)_ODP[01]** | ***określono częstotliwość, z jaką należy testować informacje z kopii zapasowych pod kątem niezawodności nośnika;*** |
| | **CP-09(01)_ODP[02]** | ***określono częstotliwość, z jaką należy testować informacje z kopii zapasowych pod kątem integralności informacji;*** |
| | **CP-09(01)[01]** | informacje z kopii zapasowych są testowane z ***<częstotliwością CP-09(01)_ODP[01]> w*** celu potwierdzenia niezawodności mediów; |
| | **CP-09(01)[02]** | informacje z kopii zapasowych są testowane z ***<częstotliwością CP-09(01)_ODP[02]> w*** celu potwierdzenia integralności informacji; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-09(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu; plan awaryjny; wyniki testów tworzenia kopii zapasowych systemu; dokumentacja testów planu awaryjnego; wyniki testów planu awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-09(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kopiami zapasowymi systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-09(01)** | **KOPIA ZAPASOWA \| BADANIE NIEZAWODNOŚCI NOŚNIKÓW/INTEGRALNOŚCI INFORMACJI** | |
| | **CP-09(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące prowadzenia kopii zapasowych systemu; mechanizmy wspierające lub wdrażające kopie zapasowe systemu]. |

| | | |
|---|---|---|
| **CP-09(02)** | **KOPIA ZAPASOWA \| TESTY ODTWORZENIOWE Z WYKORZYSTANIEM PRÓBEK DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-09(02)** | w ramach testowania planu awaryjnego wykorzystuje się próbkę informacji z kopii zapasowych do odtworzenia wybranych funkcji systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-09(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu; plan awaryjny; wyniki testów tworzenia kopii zapasowych systemu; dokumentacja testów planu awaryjnego; wyniki testów planu awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-09(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kopie zapasowe systemu; personel organizacyjny odpowiedzialny za planowanie awaryjne/testowanie planu awaryjnego;<br>personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-09(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące prowadzenia kopii zapasowych systemu; mechanizmy wspierające lub wdrażające kopie zapasowe systemu]. |

| | | |
|---|---|---|
| **CP-09(03)** | **KOPIA ZAPASOWA \| SEPARACJA PRZECHOWYWANIA INFORMACJI KRYTYCZNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-09(03)_ODP** | ***określono kopie zapasowe krytycznego oprogramowania systemowego i innych informacji związanych z bezpieczeństwem, które mają być przechowywane w oddzielnym obiekcie;*** |
| | **CP-09(03)** | kopie zapasowe ***<krytycznego oprogramowania i innych informacji związanych z bezpieczeństwem CP-09(03)_ODP>*** są przechowywane w oddzielnym obiekcie lub w ognioodpornym pojemniku, który nie jest połączony z systemem operacyjnym. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-09(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu; plan awaryjny; miejsce lub miejsca przechowywania kopii zapasowych; konfiguracje kopii zapasowych systemu i związana z nimi dokumentacja; dzienniki lub zapisy dotyczące kopii zapasowych systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-09(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie awaryjne i realizację planu; personel organizacyjny odpowiedzialny za tworzenie kopii zapasowych systemów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | |
|---|---|
| **CP-09(04)** | **KOPIA ZAPASOWA \| OCHRONA PRZED NIEAUTORYZOWANĄ MODYFIKACJĄ** |
| | [WYCOFANE: Włączone do CP-09]. |

| CP-09(05) | KOPIA ZAPASOWA \| PRZEKAZANIE KOPII DO ALTERNATYWNEJ LOKALIZACJI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-09(05)_ODP[01]** | ***określono okres zgodny z celami dot. czasu i punktu odzyskiwania;*** |
| | **CP-09(05)_ODP[02]** | ***określono szybkość przesyłania danych zgodną z celami dot. czasu i punktu odzyskiwania;*** |
| | **CP-09(05)[01]** | kopia zapasowa informacji systemowych jest przekazywana do zapasowego miejsca przechowywania na ***<okres CP-09(05)_ODP[01]>***; |
| | **CP-09(05)[02]** | kopia zapasowa informacji systemowych jest przekazywana do zapasowego miejsca przechowywania z zastosowaniem ***<szybkości przesyłania CP-09(05)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-09(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu; plan awaryjny; dzienniki lub rejestry kopii zapasowych systemu; dowody przekazania informacji o kopii zapasowej systemu do zapasowego miejsca przechowywania; umowy dotyczące zapasowego miejsca przechowywania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-09(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kopiami zapasowymi systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **CP-09(05)** | **KOPIA ZAPASOWA \| PRZEKAZANIE KOPII DO ALTERNATYWNEJ LOKALIZACJI** | |
| | **CP-09(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przekazywania kopii zapasowych systemu do zapasowego miejsca przechowywania danych; mechanizmy wspierające lub wdrażające tworzenie kopii zapasowych systemu; mechanizmy wspierające lub wdrażające przekazywanie informacji do zapasowego miejsca przechowywania]. |

| | | |
|---|---|---|
| **CP-09(06)** | **KOPIA ZAPASOWA \| REDUNDANCJA (NADMIAROWOŚĆ) SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-09(06)[01]** | kopię zapasową systemu zapewnia się poprzez utrzymywanie redundantnego systemu dodatkowego, który nie jest kolokowany z systemem podstawowym; |
| | **CP-09(06)[02]** | kopię zapasową systemu zapewnia się poprzez utrzymywanie redundantnego systemu dodatkowego, który może być aktywowany bez utraty informacji lub zakłóceń operacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-09(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu; plan awaryjny; wyniki testów tworzenia kopii zapasowych systemu; wyniki testów planu awaryjnego; dokumentacja testów planu awaryjnego; nadmiarowy system do tworzenia kopii zapasowych systemu; lokalizacja nadmiarowego systemu do tworzenia kopii zapasowych (lub lokalizacje, jeśli takich systemów jest więcej); plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-09(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kopie zapasowe systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za redundantny system dodatkowy]. |

| | | |
|---|---|---|
| **CP-09(06)** | **KOPIA ZAPASOWA \| REDUNDANCJA (NADMIAROWOŚĆ) SYSTEMU** | |
| | **CP-09(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące utrzymania redundantnych systemów dodatkowych; mechanizmy wspierające lub wdrażające tworzenie kopii zapasowych systemu; mechanizmy wspierające lub wdrażające przekazywanie informacji do redundantnego systemu dodatkowego]. |

| | | |
|---|---|---|
| **CP-09(07)** | **KOPIA ZAPASOWA \| PODWÓJNA AUTORYZACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-09(07)_ODP** | ***określono informacje z kopii zapasowych, których usunięcie lub zniszczenie musi wymagać podwójnej autoryzacji;*** |
| | **CP-09(07)** | egzekwuje się stosowanie podwójnej autoryzacji w przypadku usuwania lub niszczenia ***<informacji o kopiach zapasowych CP-09(07)_ODP>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-09(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu; plan awaryjny; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wygenerowana przez system lista poświadczeń lub zasad podwójnej autoryzacji; dzienniki lub zapisy dotyczące usuwania lub niszczenia informacji z kopii zapasowych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-09(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kopiami zapasowymi systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-09(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające podwójną autoryzację; mechanizmy wspierające lub wdrażające procedurę usuwania/niszczenie informacji o kopiach zapasowych]. |

| | | |
|---|---|---|
| **CP-09(08)** | **KOPIA ZAPASOWA \| OCHRONA KRYPTOGRAFICZNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-09(08)_ODP** | ***zdefiniowano informacje z kopii zapasowych w celu ich ochrony przed nieuprawnionym ujawnieniem i modyfikacją;*** |
| | **CP-09(08)** | wdrożono mechanizmy kryptograficzne, aby zapobiec nieautoryzowanemu ujawnieniu i modyfikacji ***<informacji z kopii zapasowych CP-09(08)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-09(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu; plan awaryjny; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-09(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie kopiami zapasowymi systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-09(08)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające kryptograficzną ochronę informacji z kopii zapasowych]. |

| | | |
|---|---|---|
| **CP-10** | **ODZYSKIWANIE I ODTWARZANIE SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-10_ODP[01]** | ***określono okres zgodny z celami dotyczącymi czasu i punktu odzyskiwania dla procesu odzyskiwania systemu;*** |

| | | |
|---|---|---|
| **CP-10** | **ODZYSKIWANIE I ODTWARZANIE SYSTEMU** | |
| | **CP-10_ODP[02]** | ***określono okres zgodny z celami dotyczącymi czasu i punktu odzyskiwania dla procesu odzyskiwania systemu;*** |
| | **CP-10[01]** | przewiduje się przywrócenie systemu do znanego stanu w ciągu ***<okresu CP-10_ODP[01]>*** po wystąpieniu zakłócenia, naruszenia bezpieczeństwa lub awarii; |
| | **CP-10[02]** | przewiduje się odtworzenie systemu do znanego stanu w ciągu ***<okresu CP-10_ODP[02]>*** po wystąpieniu zakłócenia, naruszenia bezpieczeństwa lub awarii. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu; plan awaryjny; wyniki testów tworzenia kopii zapasowych systemu; wyniki testów planu awaryjnego; dokumentacja testów planu awaryjnego; nadmiarowy system do tworzenia kopii zapasowych systemu; lokalizacja nadmiarowego systemu do tworzenia kopii zapasowych (lub lokalizacje, jeśli takich systemów jest więcej); plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-10-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie awaryjne, odzyskiwanie lub odtwarzanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-10-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne wdrażające operacje odzyskiwania i odtwarzania systemu; mechanizmy wspierające lub wdrażające operacje odzyskiwania i odtwarzania systemu]. |

| | |
|---|---|
| **CP-10(01)** | **ODZYSKIWANIE I ODTWARZANIE SYSTEMU \| TESTOWANIE PLANU AWARYJNEGO** |
| | [WYCOFANE: Włączone do CP-04]. |

| | | |
|---|---|---|
| **CP-10(02)** | **ODZYSKIWANIE I ODTWARZANIE SYSTEMU \| ODTWARZANIE TRANSAKCJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-10(02)** | odzyskiwanie transakcji stosuje się w przypadku systemów opartych na transakcjach. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-10(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące przywracania i odtwarzania systemu; plan awaryjny; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja testowa planu awaryjnego; wyniki testów planu awaryjnego; zapisy dotyczące odtwarzania transakcji systemowych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-10(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za odzyskiwanie transakcji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-10(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie odzyskiwania transakcji]. |

| | |
|---|---|
| **CP-10(03)** | **ODZYSKIWANIE I ODTWARZANIE SYSTEMU \| KOMPENSACYJNE ŚRODKI BEZPIECZEŃSTWA** |
| | [WYCOFANE. Problem rozwiązany w drodze dopasowania zakresu obowiązków]. |

| | | |
|---|---|---|
| **CP-10(04)** | **ODZYSKIWANIE I ODTWARZANIE SYSTEMU \| PRZYWRACANIE W WYZNACZONYM TERMINIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-10(04)_ODP** | ***określono okres przywracania, w którym należy przywrócić komponenty systemu do znanego, operacyjnego stanu;*** |
| | **CP-10(04)** | zapewniona jest możliwość przywrócenia komponentów systemu w trakcie***<okresu przywracania CP-10(04)_ODP>*** na podstawie komponentów operacyjnych kontrolowanych pod względem konfiguracji i chronionych pod względem integralności, które reprezentują znany, operacyjny stan komponentów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-10(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące przywracania i odtwarzania systemu; plan awaryjny; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja testowa planu awaryjnego; wyniki testów planu awaryjnego; dowody operacji przywracania i odtwarzania systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-10(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za odzyskiwanie i odtwarzanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-10(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające odzyskiwanie/odtwarzanie informacji systemowych]. |

| | |
|---|---|
| **CP-10(05)** | **ODZYSKIWANIE I ODTWARZANIE SYSTEMU \|PRACE AWARYJNE** |
| | [WYCOFANE: Włączone do SI-13]. |

| CP-10(06) | ODZYSKIWANIE I ODTWARZANIE SYSTEMU \| OCHRONA KOMPONENTÓW | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-10(06)** | komponenty systemu używane do przywracania i odzyskiwania są chronione. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-10(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące przywracania i odtwarzania systemu; plan awaryjny; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dane uwierzytelniające dotyczące dostępu logicznego; dane uwierzytelniające dotyczące dostępu fizycznego; zapisy dotyczące autoryzacji dostępu logicznego; zapisy dotyczące autoryzacji dostępu fizycznego; plan bezpieczeństwa systemu; inne stosowne dokumenty lub zapisy]. |
| | **CP-10(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za odzyskiwanie i odtwarzanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **CP-10(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ochrony kopii zapasowych i kopii odtwarzania dla sprzętu, oprogramowania oraz oprogramowania sprzętowego; mechanizmy wspierające lub wdrażające ochronę kopii zapasowych i kopii odtwarzania dla sprzętu, oprogramowania i oprogramowania sprzętowego]. |

| CP-11 | ALTERNATYWNE PROTOKOŁY KOMUNIKACJI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-11_ODP** | ***określono alternatywne protokoły komunikacyjne wspierające utrzymanie ciągłości operacji;*** |

| | | |
|---|---|---|
| **CP-11** | **ALTERNATYWNE PROTOKOŁY KOMUNIKACJI** | |
| | **CP-11** | zapewniono zdolność do stosowania **<alternatywnych protokołów komunikacji *CP-11_ODP*> *w*** celu wsparcia utrzymania ciągłości operacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-11-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące alternatywnych protokołów komunikacji; plan awaryjny; plan ciągłości operacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista alternatywnych protokołów komunikacyjnych wspierających ciągłość operacji; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-11-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i wdrażanie planów awaryjnych; personel organizacyjny odpowiedzialny za planowanie i wdrażanie działań dotyczących ciągłości operacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **CP-11-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wykorzystujące alternatywne protokoły komunikacji]. |

| | | |
|---|---|---|
| **CP-12** | **TRYB BEZPIECZNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-12_ODP[01]** | ***określono ograniczenia dotyczące trybu bezpiecznego;*** |
| | **CP-12_ODP[02]** | ***określono warunki, które muszą zostać wykryte, by przejść w tryb bezpieczny;*** |

| | | |
|---|---|---|
| **CP-12** | **TRYB BEZPIECZNY** | |
| | **CP-12** | tryb bezpieczny zostaje uruchomiony za pomocą ***<ograniczeń CP-12_ODP[01]>***, gdy zostaną wykryte ***<warunki CP-12_ODP[02]>*.** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-12-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące trybu bezpiecznego dla systemu; plan awaryjny; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; podręczniki administrowania systemem; podręczniki obsługi systemu; podręczniki instalacji systemu; zapisy z testów planu awaryjnego; zapisy dot. obsługi incydentów; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-12-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za eksploatację systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **CP-12-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające bezpieczny tryb pracy]. |

| | | |
|---|---|---|
| **CP-13** | **ALTERNATYWNE MECHANIZMY BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **CP-13_ODP[01]** | ***określono alternatywne lub dodatkowe mechanizmy bezpieczeństwa;*** |
| | **CP-13_ODP[02]** | ***określono funkcje bezpieczeństwa;*** |

| | | |
|---|---|---|
| **CP-13** | **ALTERNATYWNE MECHANIZMY BEZPIECZEŃSTWA** | |
| | **CP-13** | stosuje się ***<alternatywne lub dodatkowe mechanizmy bezpieczeństwa CP-13_ODP[01]> w*** celu zapewnienia funkcjonowania***<zabezpieczeń CP-13_ODP[02]>***, jeżeli podstawowe środki wdrażające funkcje zabezpieczeń są niedostępne lub jeśli naruszono bezpieczeństwo takich środków. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **CP-13-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania awaryjnego; procedury dotyczące alternatywnych mechanizmów bezpieczeństwa; plan awaryjny; plan ciągłości działania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy testów planu awaryjnego; wyniki testów planu awaryjnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **CP-13-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za eksploatację systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji. |
| | **CP-13-Test** | [WYBÓR SPOŚRÓD: możliwości systemu, wdrażające alternatywne mechanizmy bezpieczeństwa]. |

## 4.7. KATEGORIA IA - IDENTYFIKACJA I UWIERZYTELNIANIE

| | | |
|---|---|---|
| **IA-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-01_ODP[01]** | ***określono osoby lub role, którym należy przekazać politykę identyfikacji i uwierzytelniania;*** |
| | **IA-01_ODP[02]** | ***określono osoby lub role, którym należy przekazać procedury identyfikacji i uwierzytelniania;*** |
| | **IA-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **IA-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami identyfikacji i uwierzytelniania;*** |
| | **IA-01_ODP[05]** | ***określono częstotliwość, z jaką polityka identyfikacji i uwierzytelniania jest przeglądana i aktualizowana;*** |
| | **IA-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji polityki identyfikacji i uwierzytelniania;*** |
| | **IA-01_ODP[07]** | ***określono częstotliwość, z jaką aktualne procedury identyfikacji i uwierzytelniania są przeglądane i aktualizowane;*** |
| | **IA-01_ODP[08]** | ***określono zdarzenia skutkujące koniecznością przeprowadzenia przeglądu i aktualizacji procedur identyfikacji i uwierzytelniania;*** |
| | **IA-01a.[01]** | opracowano i udokumentowano politykę identyfikacji i uwierzytelniania; |
| | **IA-01a.[02]** | polityka identyfikacji i uwierzytelniania jest rozpowszechniana wśród ***<personelu lub ról IA-01_ODP[01]>***; |

| **IA-01** | **POLITYKA I PROCEDURY** | |
|---|---|---|
| | **IA-01a.[03]** | opracowano i udokumentowano procedury identyfikacji i uwierzytelniania ułatwiające wdrożenie polityki identyfikacji i uwierzytelniania oraz związanych z nią zabezpieczeń w tym obszarze; |
| | **IA-01a.[04]** | procedury identyfikacji i uwierzytelniania są rozpowszechniane wśród ***<personelu lub ról IA-01_ODP[02]>***; |
| | **IA-01a.01(a)[01]** | ***<WYBRANA WARTOŚĆ PARAMETRU IA-01_ODP[03]>*** polityka identyfikacji i uwierzytelniania odnosi się do celu; |
| | **IA-01a.01(a)[02]** | ***<WYBRANA WARTOŚĆ PARAMETRU IA-01_ODP[03]>*** polityka identyfikacji i uwierzytelniania odnosi się do zakresu; |
| | **IA-01a.01(a)[03]** | ***<WYBRANA WARTOŚĆ PARAMETRU IA-01_ODP[03]>*** polityka identyfikacji i uwierzytelniania odnosi się do ról; |
| | **IA-01a.01(a)[04]** | ***<WYBRANA WARTOŚĆ PARAMETRU IA-01_ODP[03]>*** polityka identyfikacji i uwierzytelniania odnosi się do obowiązków; |
| | **IA-01a.01(a)[05]** | ***<WYBRANA WARTOŚĆ PARAMETRU IA-01_ODP[03]>*** polityka identyfikacji i uwierzytelniania odnosi się do zaangażowania kierownictwa; |
| | **IA-01a.01(a)[06]** | ***<WYBRANA WARTOŚĆ PARAMETRU IA-01_ODP[03]>*** polityka identyfikacji i uwierzytelniania odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **IA-01a.01(a)[07]** | ***<WYBRANA WARTOŚĆ PARAMETRU IA-01_ODP[03]>*** polityka identyfikacji i uwierzytelniania odnosi się do zgodności; |
| | **IA-01a.01(b)** | ***<IA-01_ODP[03] WYBRANA WARTOŚĆ PARAMETRU>*** polityka identyfikacji i uwierzytelniania jest zgodna z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |

| | | |
|---|---|---|
| **IA-01** | **POLITYKA I PROCEDURY** | |
| | **IA-01b.** | ***<urzędnik CA-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur planowania awaryjnego; |
| | **IA-01c.01[01]** | aktualna polityka identyfikacji i uwierzytelniania jest poddawana przeglądowi i aktualizacji z ***<częstotliwością IA-01_ODP[05]>***; |
| | **IA-01c.01[02]** | aktualna polityka identyfikacji i uwierzytelniania jest poddawana przeglądowi i aktualizacji po ***<zdarzeniach IA-01_ODP[06]***>; |
| | **IA-01c.02[01]** | aktualne procedury identyfikacji i uwierzytelniania są przeglądane i aktualizowane z ***<częstotliwością IA-01_ODP[07]>***; |
| | **IA-01c.02[02]** | aktualne procedury identyfikacji i uwierzytelniania są przeglądane i aktualizowane po ***<zdarzeniach IA-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja strategii zarządzania ryzykiem; lista zdarzeń wymagających przeglądu i aktualizacji procedur identyfikacji i uwierzytelniania (np. ustalenia z audytu); inne istotne dokumenty lub zapisy]. |
| | **IA-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za identyfikację i uwierzytelnianie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **IA-02** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-02[01]** | Użytkownicy organizacyjni są jednoznacznie identyfikowani i uwierzytelniani; |
| | **IA-02[02]** | unikalna identyfikacja uwierzytelnionych użytkowników organizacyjnych jest związana z procesami działającymi w imieniu tych użytkowników. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; plan bezpieczeństwa systemu, dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; lista kont systemowych; inne istotne dokumenty lub zapisy]. |
| | **IA-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za zarządzanie kontami; programiści systemu]. |
| | **IA-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne służące jednoznacznej identyfikacji i uwierzytelnianiu użytkowników; mechanizmy wspierające lub wdrażające możliwości identyfikacji i uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-02(01)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT UPRZYWILEJOWANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-02(01)** | dostęp do kont uprzywilejowanych jest zabezpieczony uwierzytelnianiem wieloskładnikowym. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-02(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; plan bezpieczeństwa systemu, dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; lista kont systemowych; inne istotne dokumenty lub zapisy]. |
| | **IA-02(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-02(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności uwierzytelniania wieloskładnikowego]. |

| | | |
|---|---|---|
| **IA-02(02)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT NIEUPRZYWILEJOWANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-02(02)** | Dostęp do kont nieuprzywilejowanych jest zabezpieczony uwierzytelnianiem wieloskładnikowym. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; lista kont systemowych; inne istotne dokumenty lub zapisy]. |
| | **IA-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-02(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności uwierzytelniania wieloskładnikowego]. |

| | |
|---|---|
| **IA-02(03)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| DOSTĘP LOKALNY DO KONT UPRZYWILEJOWANYCH** |
| | [WYCOFANE: Włączone do IA-02(01)]. |

| | |
|---|---|
| **IA-02(04)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| DOSTĘP LOKALNY DO KONT NIEUPRZYWILEJOWANYCH** |
| | [WYCOFANE: Włączone do IA-02(02)]. |

| | | |
|---|---|---|
| **IA-02(05)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| UWIERZYTELNIANIE INDYWIDUALNE PRZED UWIERZYTELNIANIEM GRUPOWYM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-02(05)** | w przypadku stosowania współdzielonych kont lub środków uwierzytelniania użytkownicy muszą zostać indywidualnie uwierzytelnieni przed przyznaniem dostępu do współdzielonych kont lub zasobów; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-02(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; lista kont systemowych; inne istotne dokumenty lub zapisy]. |
| | **IA-02(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-02(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwości uwierzytelniania dla kont grupowych]. |

| | | |
|---|---|---|
| **IA-02(06)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| DOSTĘP DO KONT — ODSEPAROWANE URZĄDZENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-02(06)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {lokalne; sieciowe; zdalne};*** |
| | **IA-02(06)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {konta uprzywilejowane; konta nieuprzywilejowane};*** |
| | **IA-02(06)_ODP[03]** | ***dla mechanizmu określono zakres wymagań, których stosowanie ma być egzekwowane przez urządzenie odrębne od systemu uzyskującego dostęp do kont;*** |
| | **IA-02(06)(a)** | w przypadku dostępu ***<WYBRANA WARTOŚĆ PARAMETRU IA-02(06)_ODP[01]>*** do ***<WYBRANA WARTOŚĆ PARAMETRU IA-02(06)_ODP[02]>*** wdrożono uwierzytelnianie wieloskładnikowe w taki sposób, że jeden ze składników jest dostarczany przez urządzenie odrębne od systemu uzyskującego dostęp; |
| | **IA-02(06)(b)** | w przypadku dostępu ***<WYBRANA WARTOŚĆ PARAMETRU IA-02(06)_ODP[01]>*** do ***<WYBRANA WARTOŚĆ PARAMETRU IA-02(06)_ODP[02]>*** wdrożono uwierzytelnianie wieloskładnikowe w taki sposób, że urządzenie spełnia ***<wymagania dotyczące wytrzymałości mechanizmu IA-02(06)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-02(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; lista kont systemowych; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IA-02(06)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| DOSTĘP DO KONT — ODSEPAROWANE URZĄDZENIE** | |
| | **IA-02(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-02(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność do uwierzytelniania wieloskładnikowego]. |

| | |
|---|---|
| **IA-02(07)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| DOSTĘP SIECIOWY DO NIEUPRZYWILEJOWANYCH KONT — ODSEPAROWANE URZĄDZENIE** |
| | [WYCOFANE: Włączone do IA-02(06)]. |

| | | |
|---|---|---|
| **IA-02(08)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| DOSTĘP DO KONT — ODPORNOŚĆ NA ATAK POWTÓRZENIOWY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-02(08)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {konta uprzywilejowane; konta nieuprzywilejowane};*** |
| | **IA-02(08)** | wdrożono mechanizmy dostępu do ***<WYBRANA WARTOŚĆ PARAMETRU IA-02(08)_ODP>***, które są odporne na atak metodą powtórzenia. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IA-02(08)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| DOSTĘP DO KONT — ODPORNOŚĆ NA ATAK POWTÓRZENIOWY** | |
| | **IA-02(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; lista uprzywilejowanych kont systemowych; inne istotne dokumenty lub zapisy]. |
| | **IA-02(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-02(08)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |

| | |
|---|---|
| **IA-02(09)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| DOSTĘP DO KONT – ODPONOŚĆ NA POWTARZANIE** |
| | [WYCOFANE: Włączone do IA-02(08)]. |

| | | |
|---|---|---|
| **IA-02(10)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| LOGOWANIE POJEDYNCZE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-02(10)_ODP** | ***określono konta systemowe i usługi, dla których musi być zapewniona możliwość pojedynczego logowania;*** |
| | **IA-02(10)** | zapewniono możliwość pojedynczego logowania do ***<kont i usług systemowych IA-02(10)_ODP***>. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-02(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące możliwości pojedynczego logowania do kont i usług systemowych; procedury dotyczące identyfikacji i uwierzytelniania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>dokumentacja z audytu systemu; lista kont i usług systemowych wymagających możliwości pojedynczego logowania; inne stosowne dokumenty lub zapisy]. |
| | **IA-02(10)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-02(10)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające funkcje identyfikacji i uwierzytelniania; mechanizmy wspomagające lub realizujące funkcje pojedynczego logowania do kont i usług systemowych]. |

| | |
|---|---|
| **IA-02(11)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| ZDALNY DOSTĘP — ODSEPAROWANE URZĄDZENIE** |
| | [WYCOFANE: Włączone do IA-02(06)]. |

| | | |
|---|---|---|
| **IA-02(12)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| AUTORYZACJA DANYCH DOSTĘPOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-02(12)** | Poświadczenia zgodne ze standardem Personal Identity Verification (PIV) są akceptowane i weryfikowane elektronicznie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-02(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; zapisy z weryfikacji karty PIV; dowody posiadania poświadczeń PIV; autoryzacje dla poświadczeń PIV; inne istotne dokumenty lub zapisy]. |
| | **IA-02(12)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-02(12)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające akceptację i weryfikację identyfikatorów PIV]. |

| | | |
|---|---|---|
| **IA-02(13)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) \| UWIERZYTELNIANIE „POZA PASMEM" (Z WYKORZYSTANIEM DWÓCH ODDZIELNYCH ŚCIEŻEK)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-02(13)_ODP[01]** | ***określono mechanizmy uwierzytelniania „poza pasmem", które mają być zaimplementowane;*** |
| | **IA-02(13)_ODP[02]** | ***określono warunki, w jakich ma być stosowane uwierzytelnianie „poza pasmem";*** |
| | **IA-02(13)** | wdrożono mechanizmy ***<uwierzytelniania „poza pasmem" IA-02(13)_ODP[01]>*** zgodnie z ***<warunkami IA-02(13)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-02(13)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; wygenerowana przez system lista ścieżek uwierzytelniania „poza pasmem"; inne istotne dokumenty lub zapisy]. |
| | **IA-02(13)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-02(13)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność uwierzytelniania „poza pasmem"]. |

| | | |
|---|---|---|
| **IA-03** | **IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-03_ODP[01]** | ***określono urządzenia lub typy urządzeń, które mają być jednoznacznie zidentyfikowane i uwierzytelnione przed nawiązaniem połączenia;*** |
| | **IA-03_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {lokalne; zdalne; sieciowe};*** |
| | **IA-03** | ***<IA-03_ODP[01] urządzenia lub typy urządzeń>*** podlegają jednoznacznej identyfikacji i uwierzytelnieniu przed ustanowieniem ***<WYBRANA WARTOŚĆ PARAMETRU IA-03_ODP[02]>*** połączenia. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury identyfikacji i uwierzytelniania urządzeń; dokumentacja projektowa systemu; lista urządzeń wymagających unikalnej identyfikacji i uwierzytelniania; raporty z połączeń urządzeń; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inne istotne dokumenty lub zapisy]. |
| | **IA-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za identyfikację i uwierzytelnianie urządzeń; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-03-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwości identyfikacji i uwierzytelniania urządzeń]. |

| | | |
|---|---|---|
| **IA-03(01)** | **IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA\| KRYPTOGRAFICZNE UWIERZYTELNIANIE DWUKIERUNKOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-03(01)_ODP[01]** | ***określono urządzenia lub typy urządzeń wymagających zastosowania kryptograficznego, dwukierunkowego uwierzytelniania przed ustanowieniem co najmniej jednego połączenia;*** |
| | **IA-03(01)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {lokalne; zdalne; sieciowe};*** |
| | **IA-03(01)** | ***<urządzenia lub typy urządzeń IA-03(01)_ODP[01]>*** są uwierzytelniane przed ustanowieniem ***<WYBRANA WARTOŚĆ PARAMETRÓW IA-03(01)_ODP[02]>*** połączenia przy użyciu opartego na kryptografii uwierzytelniania dwukierunkowego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury identyfikacji i uwierzytelniania urządzeń; dokumentacja projektowa systemu; lista urządzeń wymagających unikalnej identyfikacji i uwierzytelniania; raporty z połączeń urządzeń; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inne istotne dokumenty lub zapisy]. |
| | **IA-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za identyfikację i uwierzytelnianie urządzeń; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-03(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność uwierzytelniania urządzeń; mechanizmy uwierzytelniania dwukierunkowego oparte na kryptografii]. |

| | |
|---|---|
| **IA-03(02)** | **IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA \| DWUKIERUNKOWE SIECIOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE** |
| | [WYCOFANE: Włączone do IA-03(01)]. |

| | | |
|---|---|---|
| **IA-03(03)** | **IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA \| ALOKACJA ADRESU DYNAMICZNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-03(03)_ODP[01]** | ***określono informacje o dzierżawie, które mają być stosowane do znormalizowania dynamicznego przydzielania adresów dla urządzeń;*** |
| | **IA-03(03)_ODP[02]** | ***określono czas trwania dzierżawy, który ma być stosowany do znormalizowania dynamicznego przydzielania adresów dla urządzeń;*** |
| | **IA-03(03)(a)[01]** | w przypadku urządzeń posiadających automatycznie przydzielone adresy informacje o dzierżawie w ramach dynamicznej alokacji adresów są znormalizowane zgodnie z ***<informacjami o dzierżawie IA-03(03)_ODP[01]>***; |
| | **IA-03(03)(a)[02]** | w przypadku urządzeń posiadających automatycznie przydzielone adresy okres dzierżawy w ramach dynamicznej alokacji adresów jest znormalizowany zgodnie z ***<informacjami o dzierżawie IA-03(03)_ODP[02]>***; |
| | **IA-03(03)(b)** | Informacje o dzierżawie są kontrolowane po przypisaniu do urządzenia. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IA-03(03)** | **IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA \| ALOKACJA ADRESU DYNAMICZNEGO** | |
| | **IA-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące identyfikacji i uwierzytelniania urządzeń; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dowody na informacje o dzierżawie i czasie trwania dzierżawy przypisane do urządzeń; raporty dot. połączeń urządzeń; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za identyfikację i uwierzytelnianie urządzeń; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-03(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwości identyfikacji i uwierzytelniania urządzeń; mechanizmy wspierające lub wdrażające dynamiczną alokację adresów; mechanizmy wspierające lub wdrażające kontrolę informacji o dzierżawie]. |

| | | |
|---|---|---|
| **IA-03(04)** | **IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA \| ATESTACJA URZĄDZENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-03(04)_ODP** | ***określono proces zarządzania konfiguracją, który ma być stosowany do obsługi identyfikacji i uwierzytelniania urządzeń w oparciu o atestację;*** |
| | **IA-03(04)** | identyfikacja i uwierzytelnienie urządzenia są obsługiwane w oparciu o atestację przez ***<proces zarządzania konfiguracją IA-03(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IA-03(04)** | **IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA \| ATESTACJA URZĄDZENIA** | |
| | **IA-03(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące identyfikacji i uwierzytelniania urządzeń; procedury dotyczące zarządzania konfiguracją urządzeń; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące zarządzania konfiguracją; zapisy dotyczące zabezpieczania zmian; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-03(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za identyfikację i uwierzytelnianie urządzeń; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-03(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające funkcje identyfikacji i uwierzytelniania urządzeń; mechanizmy wspomagające lub wdrażające zarządzanie konfiguracją; mechanizmy kryptograficzne wspomagające atestację urządzeń]. |

| | | |
|---|---|---|
| **IA-04** | **ZARZĄDZANIE IDENTYFIKATOREM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-04_ODP[01]** | ***określono personel lub role, od których należy uzyskać upoważnienie przed przypisaniem identyfikatora;*** |
| | **IA-04_ODP[02]** | ***określono okres, w którym można zapobiec ponownemu użyciu identyfikatorów;*** |
| | **IA-04a.** | zarządzanie identyfikatorami systemowymi wymaga otrzymania upoważnienia od ***<personelu lub ról IA-04_ODP[01]>*** w celu przypisania identyfikatora do osoby, grupy, roli lub urządzenia; |

| | | |
|---|---|---|
| **IA-04** | **ZARZĄDZANIE IDENTYFIKATOREM** | |
| | **IA-04b.** | zarządzanie identyfikatorami systemowymi odbywa się poprzez wybór identyfikatora, który identyfikuje osobę, grupę, rolę, usługę lub urządzenie; |
| | **IA-04c.** | identyfikatorami systemowymi zarządza się poprzez przypisanie ich do odpowiednich osób, grup, ról, usług lub urządzeń; |
| | **IA-04d.** | identyfikatorami systemowymi zarządza się poprzez uniemożliwienie ich ponownego użycia przez ***<okres IA-04_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania identyfikatorami; procedury dotyczące zarządzanie kontami; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista kont systemowych; lista identyfikatorów wygenerowanych przez urządzenia kontroli dostępu fizycznego; inne istotne dokumenty lub zapisy]. |
| | **IA-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-04-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zarządzanie identyfikatorami]. |

| | | |
|---|---|---|
| **IA-04(01)** | **ZARZĄDZANIE IDENTYFIKATOREM \| ZAKAZ UŻYWANIA IDENTYFIKATORÓW KONT JAKO IDENTYFIKATORÓW PUBLICZNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-04(01)** | w przypadku kont indywidualnych zabronione jest stosowanie identyfikatorów kont systemowych, które są takie same jak identyfikatory publiczne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące zarządzania identyfikatorami; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **IA-04(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zarządzanie identyfikatorami]. |

| | |
|---|---|
| **IA-04(02)** | **ZARZĄDZANIE IDENTYFIKATOREM \| AUTORYZACJA PRZEŁOŻONEGO** |
| | [WYCOFANE: Włączone do IA-12(01)]. |

| | |
|---|---|
| **IA-04(03)** | **ZARZĄDZANIE IDENTYFIKATOREM \| WIELE FORM CERTYFIKACJI** |
| | [WYCOFANE: Włączone do IA-12(02)]. |

| | | |
|---|---|---|
| **IA-04(04)** | **ZARZĄDZANIE IDENTYFIKATOREM\| IDENTYFIKACJA STATUSU UŻYTKOWNIKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-04(04)_ODP** | ***określono cechy służące do identyfikacji statusu jednostki;*** |
| | **IA-04(04)** | zarządzanie identyfikatorami indywidualnymi odbywa się poprzez jednoznaczne zidentyfikowanie każdej osoby, przypisując jej ***<cechy IA-04(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-04(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące zarządzania identyfikatorami; procedury dotyczące zarządzania kontami; lista cech identyfikujących status jednostki; inne istotne dokumenty lub zapisy]. |
| | **IA-04(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **IA-04(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zarządzanie identyfikatorami]. |

| | | |
|---|---|---|
| **IA-04(05)** | **ZARZĄDZANIE IDENTYFIKATOREM \| ZARZĄDZANIE DYNAMICZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-04(05)_ODP** | ***określono dynamiczną politykę identyfikatorów do zarządzania indywidualnymi identyfikatorami;*** |

| | | |
|---|---|---|
| **IA-04(05)** | **ZARZĄDZANIE IDENTYFIKATOREM \| ZARZĄDZANIE DYNAMICZNE** | |
| | **IA-04(05)** | poszczególne identyfikatory są dynamicznie zarządzane zgodnie z ***<dynamiczną polityką identyfikatorów IA-04(05)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-04(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące zarządzania identyfikatorami; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-04(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-04(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające dynamiczne zarządzanie identyfikatorami]. |

| | | |
|---|---|---|
| **IA-04(06)** | **ZARZĄDZANIE IDENTYFIKATOREM \| ZARZĄDZANIE MIĘDZYORGANIZACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-04(06)_ODP** | ***określono organizacje zewnętrzne, z którymi należy koordynować międzyorganizacyjne zarządzanie identyfikatorami;*** |
| | **IA-04(06)** | międzyorganizacyjne zarządzanie identyfikatorami jest koordynowane z ***<organizacjami zewnętrznymi IA-04(06)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| IA-04(06) | ZARZĄDZANIE IDENTYFIKATOREM \| ZARZĄDZANIE MIĘDZYORGANIZACYJNE | |
|---|---|---|
| | **IA-04(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania identyfikatorami; procedury dotyczące zarządzania kontami; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-04(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **IA-04(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zarządzanie identyfikatorami]. |

| IA-04(07) | ZARZĄDZANIE IDENTYFIKATOREM \| REJESTRACJA OSOBISTA |
|---|---|
| | [WYCOFANE: Włączone do IA-12(04)]. |

| IA-04(08) | ZARZĄDZANIE IDENTYFIKATOREM \| PAROWANIE IDENTYFIKATORÓW PODCZAS PSEUDONIMIZACJI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-04(08)** | podczas pseudonimizacji dochodzi do parowania identyfikatorów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-04(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące zarządzania identyfikatorami; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IA-04(08)** | **ZARZĄDZANIE IDENTYFIKATOREM \| PAROWANIE IDENTYFIKATORÓW PODCZAS PSEUDONIMIZACJI** | |
| | **IA-04(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **IA-04(08)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zarządzanie identyfikatorami]. |

| | | |
|---|---|---|
| **IA-04(09)** | **ZARZĄDZANIE IDENTYFIKATOREM \| UTRZYMANIE I OCHRONA ATRYBUTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-04(09)_ODP** | ***określono chronioną centralną pamięć służącą do przechowywania atrybutów dla każdej jednoznacznie zidentyfikowanej osoby, urządzenia lub usługi;*** |
| | **IA-04(09)** | atrybuty dla każdej jednoznacznie zidentyfikowanej osoby, urządzenia lub usługi są przechowywane w ***<chronionym centralnym magazynie IA-04(09)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-04(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące zarządzania identyfikatorami; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-04(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| IA-04(09) | ZARZĄDZANIE IDENTYFIKATOREM \| UTRZYMANIE I OCHRONA ATRYBUTÓW | |
|---|---|---|
| | **IA-04(09)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zarządzanie identyfikatorami]. |

| IA-05 | ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05_ODP[01]** | ***określono okres na zmianę lub odświeżenie metody uwierzytelniania według jej typu;*** |
| | **IA-05_ODP[02]** | ***określono zdarzenia, które skutkują zmianą lub odświeżeniem metody uwierzytelniania;*** |
| | **IA-05a.** | zarządzanie systemowymi metodami uwierzytelniania odbywa się poprzez weryfikację tożsamości osoby, grupy, roli, usługi lub urządzenia, któremu przydzielono daną metodę w ramach wstępnej dystrybucji; |
| | **IA-05b.** | zarządzanie systemowymi metodami uwierzytelniania odbywa się poprzez wybranie początkowej treści uwierzytelniającej dla każdej z metod ustanowionych przez organizację; |
| | **IA-05c.** | systemowymi metodami uwierzytelniania zarządza się w celu zapewnienia, że ich mechanizmy są odpowiednio silne do zamierzonego wykorzystania tychże metod; |
| | **IA-05d.** | zarządzanie systemowymi metodami uwierzytelniania odbywa się poprzez ustanowienie i wdrożenie procedur administracyjnych dotyczących początkowej dystrybucji takich środków, a także środków zgubionych, naruszonych pod względem bezpieczeństwa lub uszkodzonych; oraz unieważniania metod uwierzytelniania; |

| | | |
|---|---|---|
| **IA-05** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA** | |
| | **IA-05e.** | systemowymi metodami uwierzytelniania zarządza się poprzez zmianę domyślnych metod przed pierwszym użyciem; |
| | **IA-05f.** | systemowymi metodami uwierzytelniania zarządza się poprzez zmianę lub odświeżenie metod zgodnie z zasadą ***<okres wg metody uwierzytelniania IA-05_ODP[01]> lub*** po wystąpieniu ***<zdarzeń IA-05_ODP[02]>***; |
| | **IA-05g.** | systemowymi metodami uwierzytelniania zarządza się poprzez ochronę ich zawartości przed nieuprawnionym ujawnieniem i modyfikacją; |
| | **IA-05h.[01]** | systemowymi metodami uwierzytelniania zarządza się poprzez wymóg stosowania przez osoby fizyczne określonych zabezpieczeń w celu ochrony tychże metod; |
| | **IA-05h.[02]** | systemowymi metodami uwierzytelniania zarządza się poprzez wymóg stosowania przez urządzenia określonych zabezpieczeń w celu ochrony takich metod; |
| | **IA-05i.** | systemowymi metodami uwierzytelniania zarządza się poprzez zmianę metod uwierzytelniania kont grup lub ról w momencie zmiany przynależności do tych kont. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu dotyczący zarządzania metodami uwierzytelniania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista systemowych metod uwierzytelniania; zapisy dotyczące zabezpieczania zmian związanych z zarządzaniem systemowymi metodami uwierzytelniania; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IA-05** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA** | |
| | **IA-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **IA-05-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności zarządzania metodami uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-05(01)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| UWIERZYTELNIANIE OPARTE NA HASŁACH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(01)_ODP[01]** | ***określono częstotliwość, z jaką należy aktualizować listę haseł powszechnie używanych, spodziewanych lub naruszonych pod względem bezpieczeństwa;*** |
| | **IA-05(01)_ODP[02]** | ***określono zasady kompozycji i złożoności metod uwierzytelniania;*** |
| | **IA-05(01)(a)** | w przypadku uwierzytelniania opartego na hasłach utrzymuje się i aktualizuje listę haseł powszechnie używanych, spodziewanych lub naruszonych pod względem bezpieczeństwa. Listę aktualizuje się z ***<częstotliwością IA-05(01)_ODP[01]>*** oraz w przypadku podejrzenia, że w odniesieniu do haseł stosowanych w organizacji doszło do pośredniego lub bezpośredniego naruszenia bezpieczeństwa; |
| | **IA-05(01)(b)** | w przypadku uwierzytelniania opartego na hasłach, gdy hasła są tworzone lub aktualizowane przez użytkowników, sprawdza się, czy nie znajdują się one na liście haseł powszechnie używanych, spodziewanych lub naruszonych pod względem bezpieczeństwa wymienionej w IA-05(01)(a); |

| | | |
|---|---|---|
| **IA-05(01)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| UWIERZYTELNIANIE OPARTE NA HASŁACH** | |
| | **IA-05(01)(c)** | w przypadku uwierzytelniania opartego na hasłach hasła są przesyłane wyłącznie za pośrednictwem kanałów chronionych kryptograficznie; |
| | **IA-05(01)(d)** | w przypadku uwierzytelniania opartego na hasłach hasła są przechowywane przy użyciu zatwierdzonej funkcji wyprowadzania klucza z ciągiem zaburzającym (tzw. *sól*), najlepiej przy użyciu klucza haszującego; |
| | **IA-05(01)(e)** | w przypadku uwierzytelniania opartego na hasłach po odzyskaniu konta wymagany jest natychmiastowy wybór nowego hasła; |
| | **IA-05(01)(f)** | w przypadku uwierzytelniania opartego na hasłach dopuszczalny jest wybór przez użytkownika długich haseł i fraz, włącznie ze spacjami i wszystkimi znakami drukowanymi; |
| | **IA-05(01)(g)** | w przypadku uwierzytelniania opartego na hasłach stosuje się automatyczne narzędzia, które pomagają użytkownikowi w wyborze silnych czynników uwierzytelniających hasła; |
| | **IA-05(01)(h)** | w przypadku uwierzytelniania opartego na hasłach egzekwuje się ***<zasady kompozycji i złożoności IA-05(01)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-05(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; polityka dotycząca haseł; procedury dotyczące zarządzania metodami uwierzytelniania; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracji systemu i związana z nimi dokumentacja; konfiguracje haseł i związana z nimi dokumentacja; inne istotne dokumenty lub zapisy]. |
| | **IA-05(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |

| | | |
|---|---|---|
| **IA-05(01)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| UWIERZYTELNIANIE OPARTE NA HASŁACH** | |
| | **IA-05(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność do zarządzania metodami uwierzytelniania opartymi na hasłach]. |

| | | |
|---|---|---|
| **IA-05(02)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| UWIERZYTELNIANIE OPARTE NA INFRASTRUKTURZE KLUCZA PUBLICZNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(02)(a)(01)** | w przypadku uwierzytelniania opartego na infrastrukturze klucza publicznego egzekwuje się autoryzowany dostęp do odpowiedniego klucza prywatnego; |
| | **IA-05(02)(a)(02)** | dokonuje się mapowania uwierzytelnionej tożsamości do konta osoby lub grupy w celu zastosowania uwierzytelniania opartego na infrastrukturze klucza publicznego; |
| | **IA-05(02)(b)(01)** | w przypadku stosowania infrastruktury klucza publicznego (PKI) walidacja certyfikatów następuje poprzez stworzenie i zweryfikowanie ścieżki certyfikacji do akceptowanej kotwicy zaufania, w tym sprawdzenie informacji o statusie certyfikatu; |
| | **IA-05(02)(b)(02)** | w przypadku korzystania z infrastruktury klucza publicznego (PKI) stosowana jest lokalna pamięć podręczna zawierająca dane dotyczące unieważnionych certyfikatów w celu wsparcia wyszukiwania i walidacji ścieżek. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IA-05(02)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| UWIERZYTELNIANIE OPARTE NA INFRASTRUKTURZE KLUCZA PUBLICZNEGO** | |
| | **IA-05(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania metodami uwierzytelniania; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dot. walidacji certyfikatów PKI; listy unieważnionych certyfikatów PKI; inne istotne dokumenty lub zapisy]. |
| | **IA-05(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie metodami uwierzytelniania opartymi na PKI; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu. |
| | **IA-05(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność do zarządzania metodami uwierzytelniania opartymi na PKI]. |

| | |
|---|---|
| **IA-05(03)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| REJESTRACJA OSOBISTA LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ** |
| | [WYCOFANE: Włączone do IA-12(04)]. |

| | |
|---|---|
| **IA-05(04)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| AUTOMATYCZNE WSPARCIE OKREŚLANIA SIŁY HASŁA** |
| | [WYCOFANE: Włączone do IA-05(01)]. |

| | | |
|---|---|---|
| **IA-05(05)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| ZMIANA METODY UWIERZYTELNIANIA PRZED DOSTAWĄ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(05)** | programiści i instalatorzy komponentów systemu są zobowiązani do dostarczania unikalnych metod uwierzytelniania lub zmiany tych domyślnych przed dostawą i instalacją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-05(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; polityka w zakresie zakupu systemów i usług; procedury dotyczące zarządzania metodami uwierzytelniania; procedury dotyczące włączania wymogów bezpieczeństwa do procesu realizacji zakupów; dokumentacja dotycząca zakupów; umowy kupna systemów lub usług; inne istotne dokumenty lub zapisy]. |
| | **IA-05(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji, zakupy i zawieranie umów; programiści systemu. |
| | **IA-05(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności zarządzania metodami uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-05(06)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| OCHRONA METOD UWIERZYTELNIANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(06)** | metody uwierzytelniania są chronione proporcjonalnie do kategorii bezpieczeństwa informacji, do których dostęp umożliwia ich użycie. |

| | | |
|---|---|---|
| **IA-05(06)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| OCHRONA METOD UWIERZYTELNIANIA** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-05(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania metodami uwierzytelniania; dokumentacja dotycząca kategorii bezpieczeństwa systemu; oceny bezpieczeństwa dot. zabezpieczeń metod uwierzytelniania; wyniki oceny ryzyka; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-05(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacyjny wdrażający lub utrzymujący zabezpieczenia metod uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci. |
| | **IA-05(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność zarządzania metodami uwierzytelniania; mechanizmy zabezpieczające metody uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-05(07)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| BRAK WBUDOWANYCH NIEZASZYFROWANYCH STATYCZNYCH ELEMENTÓW UWIERZYTELNIANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(07)** | niezaszyfrowane statyczne metody uwierzytelniania nie są osadzone w aplikacjach lub innych formach statycznego magazynu danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IA-05(07)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| BRAK WBUDOWANYCH NIEZASZYFROWANYCH STATYCZNYCH ELEMENTÓW UWIERZYTELNIANIA** | |
| | **IA-05(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące zarządzania metodami uwierzytelniania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; skrypty dostępu logicznego; przeglądy kodu aplikacji pod kątem wykrywania niezaszyfrowanych statycznych metod uwierzytelniania; inne stosowne dokumenty lub zapisy]. |
| | **IA-05(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-05(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność zarządzania metodami uwierzytelniania; mechanizmy wdrażające uwierzytelnianie w aplikacjach]. |

| | | |
|---|---|---|
| **IA-05(08)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| JEDNO KONTO W WIELU SYSTEMACH INFORMACYJNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(08)_ODP** | ***określono środki kontroli bezpieczeństwa wdrożone w celu zarządzania ryzykiem naruszenia bezpieczeństwa w związku z posiadaniem przez osoby fizyczne kont w wielu systemach;*** |
| | **IA-05(08)** | wdrożono ***<zabezpieczenia IA-05(08)_ODP>*** w celu zarządzania ryzykiem naruszenia bezpieczeństwa wynikającym z posiadania przez osoby fizyczne kont w wielu systemach. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IA-05(08)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| JEDNO KONTO W WIELU SYSTEMACH INFORMACYJNYCH** | |
| | **IA-05(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania metodami uwierzytelniania; plan bezpieczeństwa systemu; lista osób posiadających konta w wielu systemach; lista środków bezpieczeństwa mających na celu zarządzanie ryzykiem naruszenia bezpieczeństwa w związku z posiadaniem przez osoby fizyczne kont w wielu systemach; inne istotne dokumenty lub zapisy]. |
| | **IA-05(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **IA-05(08)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zabezpieczenia w zakresie zarządzania metodami uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-05(09)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| ZARZĄDZANIE DANYMI UWIERZYTELNIAJĄCYMI MIĘDZY ORGANIZACJAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(09)_ODP** | ***określono organizacje zewnętrzne, które mają być używane do uwierzytelniania poświadczeń;*** |
| | **IA-05(09)** | do uwierzytelniania poświadczeń wykorzystuje się ***<organizacje zewnętrzne IA-05(09)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IA-05(09)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| ZARZĄDZANIE DANYMI UWIERZYTELNIAJĄCYMI MIĘDZY ORGANIZACJAMI** | |
| | **IA-05(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania metodami uwierzytelniania; procedury dotyczące zarządzania kontami; plan bezpieczeństwa systemu; umowy dotyczące bezpieczeństwa; inne istotne dokumenty lub zapisy]. |
| | **IA-05(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **IA-05(09)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zabezpieczenia w zakresie zarządzania metodami uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-05(10)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| DYNAMICZNE KOJARZENIE DANYCH UWIERZYTELNIAJĄCYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(10)_ODP** | ***zdefiniowane są zasady dynamicznego kojarzenia tożsamości i metod uwierzytelniania;*** |
| | **IA-05(10)** | tożsamość i metody uwierzytelniania są dynamicznie kojarzone przy użyciu ***<zasad kojarzenia IA-05(10)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IA-05(10)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| DYNAMICZNE KOJARZENIE DANYCH UWIERZYTELNIAJĄCYCH** | |
| | **IA-05(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania metodami uwierzytelniania; plan bezpieczeństwa systemu; automatyczne mechanizmy zapewniające dynamiczne wiązanie identyfikatorów i metod uwierzytelniania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-05(10)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **IA-05(10)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wdrażające zdolność zarządzania identyfikatorami; automatyczne mechanizmy wdrażające dynamiczne wiązanie tożsamości i metod uwierzytelniania]. |

| | |
|---|---|
| **IA-05(11)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| UWIERZYTELNIANIE PRZY UŻYCIU TOKENA** |
| | [WYCOFANE: Włączone do IA-02(01), IA-02(02)]. |

| | | |
|---|---|---|
| **IA-05(12)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| WYDAJNOŚĆ UWIERZYTELNIANIA BIOMETRYCZNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(12)_ODP** | ***określono wymagania jakościowe dot. uwierzytelniania biometrycznego;*** |

| | | |
|---|---|---|
| **IA-05(12)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| WYDAJNOŚĆ UWIERZYTELNIANIA BIOMETRYCZNEGO** | |
| | **IA-05(12)** | stosuje się mechanizmy spełniające ***<wymagania jakościowe dot. biometrii IA-05(12)_ODP>*** |
| | | do uwierzytelniania opartego na biometrii. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-05(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; |
| | | procedury dotyczące zarządzania metodami uwierzytelniania; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; |
| | | mechanizmy wykorzystujące uwierzytelnianie biometryczne w systemie; lista |
| | | wymagań jakościowych dot. biometrii; ustawienia konfiguracyjne systemu i związana z nimi |
| | | dokumentacja, zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-05(12)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie metodami uwierzytelniania; |
| | | personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; |
| | | administratorzy systemu/sieci; programiści systemu. |
| | **IA-05(12)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności |
| | | zarządzania metodami uwierzytelniania opartymi na biometrii]. |

| | | |
|---|---|---|
| **IA-05(13)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| PRZEDAWNIENIE BUFOROWANYCH ELEMENTÓW UWIERZYTELNIANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(13)_ODP** | ***określono czas, po którym korzystanie z buforowanych metod uwierzytelniania jest zabronione;*** |
| | **IA-05(13)** | użycie buforowanych metod uwierzytelniania jest zabronione po upływie ***<okresu IA-05(13)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-05(13)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania metodami uwierzytelniania; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-05(13)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-05(13)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności zarządzania metodami uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-05(14)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| ZARZĄDZANIE ZAWARTOŚCIĄ MAGAZYNÓW ZAUFANIA PKI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(14)** | stosuje się ogólnoorganizacyjną metodologię zarządzania zawartością magazynów zaufania PKI na wszystkich platformach, w tym w sieciach, systemach operacyjnych, przeglądarkach i aplikacjach służących do uwierzytelniania opartego na PKI. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-05(14)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania metodami uwierzytelniania; plan bezpieczeństwa systemu; ogólnoorganizacyjna metodologia zarządzania zawartością magazynów zaufania PKI na wszystkich zainstalowanych platformach; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja architektury bezpieczeństwa przedsiębiorstwa; dokumentacja architektury przedsiębiorstwa; inne istotne dokumenty lub zapisy]. |
| | **IA-05(14)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-05(14)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zarządzanie metodami uwierzytelniania opartymi na PKI; mechanizmy wspierające lub wdrażające zdolności dot. magazynów zaufania PKI]. |

| | | |
|---|---|---|
| **IA-05(15)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| ZATWIERDZANIE PRODUKÓW I USŁUG WEDŁUG Z GÓRY USTALONYCH REGUŁ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(15)** | do zarządzania tożsamością, wiarygodnością i dostępem używa się wyłącznie produktów i usług zatwierdzonych przez stosowne organy. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-05(15)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania metodami uwierzytelniania; plan bezpieczeństwa systemu; mechanizmy zapewniające dynamiczne wiązanie identyfikatorów i metod uwierzytelniania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-05(15)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **IA-05(15)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwości zarządzania kontem; mechanizmy wspierające lub wdrażające zdolności zarządzania identyfikatorami i metodami uwierzytelniania w systemie]. |

| | | |
|---|---|---|
| **IA-05(16)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| WYDAWANIE POŚWIADCZEŃ UWIERZYTELNIAJĄCYCH OSOBIŚCIE LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(16)_ODP[01]** | ***określono konkretne metody uwierzytelniania bądź ich rodzaje, które mają być wydane;*** |
| | **IA-05(16)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {osobiście; przez zaufaną stronę zewnętrzną};*** |
| | **IA-05(16)_ODP[03]** | ***określono organ rejestrujący, który wydaje metody uwierzytelniania;*** |
| | **IA-05(16)_ODP[04]** | ***określono osoby lub role, które wydają upoważnienie do wydania metody uwierzytelniania;*** |
| | **IA-05(16)** | wydanie ***<metod uwierzytelniania lub ich rodzajów IA-05(16)_ODP[01]>*** jest wymagane do przeprowadzenia ***<WYBRANA WARTOŚĆ PARAMETRU IA-05(16)_ODP[02]>*** przed ***<organem rejestracyjnym IA-05(16)_ODP[03]>*** za upoważnieniem wydanym przez<br>***<personel lub role IA-05(16)_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-05(16)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania metodami uwierzytelniania; plan bezpieczeństwa systemu; mechanizmy zapewniające dynamiczne wiązanie identyfikatorów i metod uwierzytelniania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IA-05(16)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| WYDAWANIE POŚWIADCZEŃ UWIERZYTELNIAJĄCYCH OSOBIŚCIE LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ** | |
| | **IA-05(16)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **IA-05(16)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwości zarządzania kontem; mechanizmy wspierające lub wdrażające zdolności zarządzania identyfikatorami i metodami uwierzytelniania w systemie]. |

| | | |
|---|---|---|
| **IA-05(17)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| WYKRYWANIE ATAKÓW PREZENTACYJNYCH PODCZAS UWIERZYTELNIANIA BIOMETRYCZNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(17)** | w uwierzytelnianiu opartym na biometrii stosuje się mechanizmy wykrywania ataków prezentacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-05(17)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania metodami uwierzytelniania; plan bezpieczeństwa systemu; mechanizmy zapewniające dynamiczne wiązanie identyfikatorów i metod uwierzytelniania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IA-05(17)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| WYKRYWANIE ATAKÓW PREZENTACYJNYCH PODCZAS UWIERZYTELNIANIA BIOMETRYCZNEGO** | |
| | **IA-05(17)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **IA-05(17)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwości zarządzania kontem; mechanizmy wspierające lub wdrażające zdolności zarządzania identyfikatorami i metodami uwierzytelniania w systemie]. |

| | | |
|---|---|---|
| **IA-05(18)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| MENEDŻER HASEŁ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-05(18)_ODP[01]** | ***określono menedżery haseł stosowane do generowania i zarządzania hasłami;*** |
| | **IA-05(18)_ODP[02]** | ***określono zabezpieczenia dla haseł;*** |
| | **IA-05(18)(a)** | do generowania i zarządzania hasłami stosuje się ***<menedżery haseł IA-05(18)_ODP[01]>***; |
| | **IA-05(18)(b)** | hasła chronione są za pomocą ***<zabezpieczeń IA-05(18)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IA-05(18)** | **ZARZĄDZANIE METODAMI UWIERZYTELNIANIA \| MENEDŻER HASEŁ** | |
| | **IA-05(18)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące zarządzania metodami uwierzytelniania; plan bezpieczeństwa systemu; mechanizmy zapewniające dynamiczne wiązanie identyfikatorów i metod uwierzytelniania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-05(18)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **IA-05(18)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwości zarządzania kontem; mechanizmy wspierające lub wdrażające zdolności zarządzania identyfikatorami i metodami uwierzytelniania w systemie]. |

| | | |
|---|---|---|
| **IA-06** | **OCHRONA PROCESU UWIERZYTELNIANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-06** | podczas procesu uwierzytelniania informacje zwrotne dotyczące uwierzytelniania są ukryte w celu ochrony informacji przed ewentualnym wykorzystaniem przez osoby nieuprawnione. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IA-06** | **OCHRONA PROCESU UWIERZYTELNIANIA** | |
| | **IA-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące informacji zwrotnej dot. metod uwierzytelniania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-06-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające ukrywanie informacji zwrotnej dot. uwierzytelniania podczas procesu uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-07** | **UWIERZYTELNIANIE MODUŁU KRYPTOGRAFICZNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-07** | wdrożono mechanizmy uwierzytelniania do stosowania w module kryptograficznym, które to mechanizmy spełniają wymagania obowiązujących przepisów, rozporządzeń, dyrektyw, polityk, regulacji, norm i wytycznych dotyczących takiego uwierzytelniania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące uwierzytelniania modułów kryptograficznych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IA-07** | **UWIERZYTELNIANIE MODUŁU KRYPTOGRAFICZNEGO** | |
| | **IA-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za uwierzytelnianie modułów kryptograficznych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu]. |
| | **IA-07-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające uwierzytelnianie modułów kryptograficznych]. |

| | | |
|---|---|---|
| **IA-08** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-08** | użytkownicy spoza organizacji lub procesy działające w imieniu takich użytkowników są jednoznacznie identyfikowane i uwierzytelniane; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; lista kont systemowych; inne istotne dokumenty lub zapisy]. |
| | **IA-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za zarządzanie kontami; programiści systemu]. |
| | **IA-08-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-08(01)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)\| AKCEPTACJA POŚWIADCZEŃ TOŻSAMOŚCI WYDANYCH PRZEZ INNE ORGANIZACJE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-08(01)[01]** | Poświadczenia tożsamości zgodne ze standardem PIV, wydane przez inne odpowiednie organy, są akceptowane; |
| | **IA-08(01)[02]** | Poświadczenia tożsamości zgodne ze standardem PIV, wydane przez inne odpowiednie organy, są weryfikowane elektronicznie; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-08(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; zapisy z weryfikacji karty PIV; dowody posiadania poświadczeń PIV; autoryzacje dla poświadczeń PIV; inne istotne dokumenty lub zapisy]. |
| | **IA-08(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie kontami]. |
| | **IA-08(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwości identyfikacji i uwierzytelniania; mechanizmy przyjmujące i weryfikujące poświadczenia PIV]. |

| | | |
|---|---|---|
| **IA-08(02)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)\| AKCEPTACJA POŚWIADCZEŃ STRON TRZECICH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-08(02)(a)** | akceptowane są wyłącznie metody uwierzytelniania stron trzecich zgodne z wymogami NIST; |
| | **IA-08(02)(b)[01]** | sporządzono listę akceptowanych metod uwierzytelniania stron trzecich ; |
| | **IA-08(02)(b)[02]** | prowadzi się listę akceptowanych metod uwierzytelniania stron trzecich ; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-08(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; wykaz produktów, komponentów lub usług uwierzytelniania stron trzecich, które zostały zamówione i wdrożone przez organizację; zapisy dot. poświadczeń stron trzecich; dowody na posiadanie poświadczeń stron trzecich; autoryzacje poświadczeń stron trzecich; inne istotne dokumenty lub zapisy]. |
| | **IA-08(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie kontami]. |
| | **IA-08(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwości identyfikacji i uwierzytelniania; mechanizmy akceptujące zewnętrzne poświadczenia]. |

| | |
|---|---|
| **IA-08(03)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) \| WYKORZYSTANIE CERTYFIKOWANYCH PRODUKTÓW** |
| | [WYCOFANE: Włączone do IA-08(02)]. |

| | | |
|---|---|---|
| **IA-08(04)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) \| WYKORZYSTANIE PROFILI WYDAWANYCH PRZEZ STOSOWNE INSTYTUCJE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-08(04)_ODP** | ***określono profile zarządzania tożsamością;*** |
| | **IA-08(04)** | zarządzanie tożsamością odbywa się zgodnie z ***<profilami zarządzania tożsamością IA-08(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-08(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-08(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie kontami]. |
| | **IA-08(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania; mechanizmy wspomagające lub zapewniające zgodność z profilami]. |

| | | |
|---|---|---|
| **IA-08(05)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) \| AKCEPTACJA POŚWIADCZEŃ OSOBISTEJ WERYFIKACJI TOŻSAMOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-08(05)_ODP** | ***określono politykę korzystania z poświadczeń wydanych przez inne organy lub PKI;*** |
| | **IA-08(05)[01]** | poświadczenia wydawane przez inne organy lub PKI, które spełniają kryteria ***<polityki IA-08(05)_ODP>*** są akceptowane; |
| | **IA-08(05)[02]** | poświadczenia wydawane przez inne organy lub PKI, które spełniają kryteria ***<polityki IA-08(05)_ODP>*** są weryfikowane; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-08(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; zapisy dot. weryfikacji poświadczeń PIV-I; dowody dot. poświadczeń PIV-I; autoryzacje dot. poświadczeń PIV-I; inne istotne dokumenty lub zapisy]. |
| | **IA-08(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie kontami]. |
| | **IA-08(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwości identyfikacji i uwierzytelniania; mechanizmy przyjmujące i weryfikujące poświadczenia PIV]. |

| | | |
|---|---|---|
| **IA-08(06)** | **IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)\| NIEPOŁĄCZALNOŚĆ (DEZASOCJACYJNOŚĆ)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-08(06)_ODP** | ***określono środki w zakresie niepołączalności;*** |
| | **IA-08(06)** | wdrożono ***<środki IA-08(06)_ODP>*** do rozłączenia atrybutów użytkownika lub relacji poświadczenia identyfikatora w odniesieniu do osób, dostawców usług uwierzytelniających i stron ufających. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-08(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; plan ochrony prywatności; procedury identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-08(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie kontami; programiści systemu]. |
| | **IA-08(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-09** | **IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-09_ODP** | ***określono usługi i aplikacje systemowe, które mają być jednoznacznie identyfikowane i uwierzytelniane;*** |
| | **IA-09** | ***<usługi i aplikacje systemowe IA-09_ODP>*** są jednoznacznie identyfikowane i uwierzytelniane przed nawiązaniem komunikacji z urządzeniami, użytkownikami lub innymi usługami bądź aplikacjami. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania usług; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; zabezpieczenia stosowane do identyfikacji i uwierzytelniania usług systemowych; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania]. |
| | **IA-09-Test** | [WYBÓR SPOŚRÓD: Zabezpieczenia wdrażające możliwości identyfikacji i uwierzytelniania usług]. |

| | |
|---|---|
| **IA-09(01)** | **IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG \| WYMIANA INFORMACJI** |
| | [WYCOFANE: Włączone do IA-09]. |

| | |
|---|---|
| **IA-09(02)** | **IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG \| PRZEKAZYWANIE DECYZJI O POZYTYWNEJ IDENTYFIKACJI I UWIERZYTELNIENIU** |
| | [WYCOFANE: Włączone do IA-09]. |

| | | |
|---|---|---|
| **IA-10** | **UWIERZYTELNIANIE ADAPTACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-10_ODP[01]** | ***określono dodatkowe techniki lub mechanizmy uwierzytelniania, które mają być stosowane przy uzyskiwaniu dostępu do systemu w określonych okolicznościach lub sytuacjach;*** |
| | **IA-10_ODP[02]** | ***określono okoliczności lub sytuacje, które wymagają od osób uzyskujących dostęp do systemu zastosowania dodatkowych technik lub mechanizmów uwierzytelniania;*** |
| | **IA-10** | Osoby mające dostęp do systemu są zobowiązane do stosowania ***<dodatkowych technik lub mechanizmów uwierzytelniania IA-10_ODP[01]>*** w określonych ***<warunkach lub sytuacjach IA-10_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące adaptacyjnych/dodatkowych technik lub mechanizmów identyfikacji i uwierzytelniania; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dodatkowe techniki lub mechanizmy identyfikacji i uwierzytelniania; zapisy z audytu systemu; inne stosowne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IA-10** | **UWIERZYTELNIANIE ADAPTACYJNE** | |
| | **IA-10-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania]. |
| | **IA-10-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-11** | **PONOWNE UWIERZYTELNIENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-11_ODP** | ***określono okoliczności lub sytuacje wymagające ponownego uwierzytelnienia;*** |
| | **IA-11** | użytkownicy są zobowiązani do ponownego uwierzytelnienia w przypadku wystąpienia ***<okoliczności i sytuacji IA-11_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-11-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące ponownego uwierzytelniania użytkowników i urządzeń; plan bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz okoliczności lub sytuacji wymagających ponownego uwierzytelniania; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IA-11** | **PONOWNE UWIERZYTELNIENIE** | |
| | **IA-11-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania]. |
| | **IA-11-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-12** | **POTWIERDZENIE TOŻSAMOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-12a.** | tożsamość użytkowników, którzy potrzebują kont do logicznego dostępu do systemów opartych na odpowiednich wymaganiach w zakresie poziomu zapewnienia tożsamości, określonych w obowiązujących normach i wytycznych, jest weryfikowana; |
| | **IA-12b.** | tożsamość użytkownika jest przypisana do konkretnej osoby fizycznej; |
| | **IA-12c.[01]** | zbierane są dowody tożsamości; |
| | **IA-12c.[02]** | dowody tożsamości podlegają walidacji; |
| | **IA-12c.[03]** | dowody tożsamości podlegają weryfikacji; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-12-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące potwierdzenia tożsamości; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IA-12** | **POTWIERDZENIE TOŻSAMOŚCI** | |
| | **IA-12-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za eksploatację systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; radca prawny; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za identyfikację i uwierzytelnianie]. |
| | **IA-12-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-12(01)** | **POTWIERDZENIE TOŻSAMOŚCI \| AUTORYZACJA PRZEŁOŻONEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-12(01)** | proces rejestracji w celu otrzymania konta dostępu logicznego obejmuje autoryzację przełożonego lub sponsora. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-12(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące potwierdzenia tożsamości; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-12(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania]. |
| | **IA-12(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-12(02)** | **POTWIERDZENIE TOŻSAMOŚCI \| DOWODZENIE TOŻSAMOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-12(02)** | wymagane jest przedstawienie organowi rejestracyjnemu dowodu identyfikacji osobistej. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-12(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące potwierdzenia tożsamości; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-12(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania]. |
| | **IA-12(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-12(03)** | **POTWIERDZANIE TOŻSAMOŚCI \| POTWIERDZANIE I WERYFIKACJA DOWODÓW TOŻSAMOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-12(03)_ODP** | ***określono metody zatwierdzania i weryfikacji dowodów tożsamości;*** |
| | **IA-12(03)** | przedstawione dowody tożsamości są zatwierdzane i weryfikowane za pomocą ***<metod zatwierdzania i weryfikacji IA-12(03)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IA-12(03)** | **POTWIERDZANIE TOŻSAMOŚCI \| POTWIERDZANIE I WERYFIKACJA DOWODÓW TOŻSAMOŚCI** | |
| | **IA-12(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące potwierdzenia tożsamości; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-12(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania]. |
| | **IA-12(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-12(04)** | **POTWIERDZANIE TOŻSAMOŚCI \| OSOBISTE ZATWIERDZENIE I WERYFIKACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-12(04)** | zatwierdzanie i weryfikacja dowodów tożsamości odbywa przy osobistym stawiennictwie przed wyznaczonym organem rejestracyjnym. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-12(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące potwierdzenia tożsamości; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-12(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-12(04)** | **POTWIERDZANIE TOŻSAMOŚCI \| OSOBISTE ZATWIERDZENIE I WERYFIKACJA** | |
| | **IA-12(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-12(05)** | **POTWIERDZENIE TOŻSAMOŚCI \| POTWIERDZENIE ADRESU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-12(05)_ODP** | ***wybrano jedną z następujących WARTOŚCI PARAMETRÓW: {kod rejestracyjny; zawiadomienie o potwierdzeniu odbioru};*** |
| | **IA-12(05)** | ***<WYBRANA WARTOŚĆ PARAMETRU IA-12(05)_ODP>*** jest dostarczana poprzez kanał „poza pasmem” w celu weryfikacji (fizycznego lub cyfrowego) adresu użytkownika. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-12(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące potwierdzenia tożsamości; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-12(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania]. |
| | **IA-12(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania]. |

| | | |
|---|---|---|
| **IA-12(06)** | **POTWIERDZANIE TOŻSAMOŚCI \| AKCEPTACJA ZEWNETRZNYCH TOŻSAMOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IA-12(06)_ODP** | ***określono poziom zapewnienia tożsamości obowiązujący w przypadku akceptowania tożsamości potwierdzonych zewnętrznie;*** |
| | **IA-12(06)** | Tożsamości potwierdzone zewnętrznie są akceptowane przy zastosowaniu***<poziomu zapewnienia tożsamości IA-12(06)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IA-12(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie identyfikacji i uwierzytelniania; procedury dotyczące potwierdzenia tożsamości; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IA-12(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za operacje systemowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie identyfikatorami i metodami uwierzytelniania]. |
| | **IA-12(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie identyfikacji i uwierzytelniania]. |

## 4.8. KATEGORIA IR - REAGOWANIE NA INCYDENTY

| | | |
|---|---|---|
| **IR-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-01_ODP[01]** | ***określono personel lub role, którym należy przekazać politykę reagowania na incydenty;*** |
| | **IR-01_ODP[02]** | ***określono personel lub role, którym należy przekazać procedury reagowania na incydenty;*** |
| | **IR-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **IR-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami reagowania na incydenty;*** |
| | **IR-01_ODP[05]** | ***określono częstotliwość, z jaką dokonuje się przeglądu i aktualizacji obowiązującej polityki reagowania na incydenty;*** |
| | **IR-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji obowiązującej polityki reagowania na incydenty;*** |
| | **IR-01_ODP[07]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji obowiązujących procedur reagowania na incydenty;*** |
| | **IR-01_ODP[08]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji obowiązującej polityki reagowania na incydenty;*** |
| | **IR-01a.[01]** | opracowanie i udokumentowanie polityki reagowania na incydenty; |
| | **IR-01a.[02]** | polityka reagowania na incydenty jest rozpowszechniana wśród ***<personelu lub ról IR-01_ODP[01]>***; |
| | **IR-01a.[03]** | opracowano i udokumentowano procedury reagowania na incydenty ułatwiające wdrożenie polityki reagowania na incydenty i powiązanych zabezpieczeń w zakresie reagowania na incydenty; |

| IR-01 | POLITYKA I PROCEDURY | |
|---|---|---|
| | **IR-01a.[04]** | procedury reagowania na incydenty są rozpowszechniane wśród ***<personelu lub ról IR-01_ODP[02]>***; |
| | **IR-01a.01(a)[01]** | polityka reagowania na incydenty ***<WYBRANA WARTOŚĆ PARAMETRU IR-01_ODP[03]>*** odnosi się do celu; |
| | **IR-01a.01(a)[02]** | polityka reagowania na incydenty ***<WYBRANA WARTOŚĆ PARAMETRU IR-01_ODP[03]>*** odnosi się do zakresu; |
| | **IR-01a.01(a)[03]** | polityka reagowania na incydenty ***<WYBRANA WARTOŚĆ PARAMETRU IR-01_ODP[03]>*** odnosi się do ról; |
| | **IR-01a.01(a)[04]** | polityka reagowania na incydenty ***<WYBRANA WARTOŚĆ PARAMETRU IR-01_ODP[03]>*** odnosi się do obowiązków; |
| | **IR-01a.01(a)[05]** | polityka reagowania na incydenty ***<WYBRANA WARTOŚĆ PARAMETRU IR-01_ODP[03]>*** odnosi się do zaangażowania kierownictwa; |
| | **IR-01a.01(a)[06]** | polityka reagowania na incydenty ***<WYBRANA WARTOŚĆ PARAMETRU IR-01_ODP[03]>*** odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **IR-01a.01(a)[07]** | polityka reagowania na incydenty ***<WYBRANA WARTOŚĆ PARAMETRU IR-01_ODP[03]>*** odnosi się do zgodności; |
| | **IR-01a.01(b)** | polityka reagowania na incydenty ***<WYBRANA WARTOŚĆ PARAMETRU IR-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **IR-01b.** | ***<urzędnik CP-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur reagowania na incydenty; |
| | **IR-01c.01[01]** | obowiązująca polityka reagowania na incydenty podlega przeglądowi i aktualizacji z ***<częstotliwością IR-01_ODP[05]>***; |

| | | |
|---|---|---|
| **IR-01** | **POLITYKA I PROCEDURY** | |
| | **IR-01c.01[02]** | obowiązująca polityka reagowania na incydenty podlega przeglądowi i aktualizacji po ***<zdarzeniach IR-01_ODP[06]>***; |
| | **IR-01c.02[01]** | przegląd i aktualizacja procedur reagowania na incydenty odbywa się z ***<częstotliwością IR-01_ODP[07]>***; |
| | **IR-01c.02[02]** | przegląd i aktualizacja procedur reagowania na incydenty odbywa się po ***<zdarzeniach IR-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za reagowanie na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **IR-02** | **SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-02_ODP[01]** | ***określono okres, w którym należy przeprowadzić szkolenie w zakresie reagowania na incydenty dla użytkowników systemu obejmujących role lub obowiązki związane z reagowaniem na incydenty;*** |
| | **IR-02_ODP[02]** | ***określono częstotliwość, z jaką należy przeprowadzać szkolenia z zakresu reagowania na incydenty dla użytkowników;*** |
| | **IR-02_ODP[03]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji treści szkolenia w zakresie reagowania na incydenty;*** |

| | | |
|---|---|---|
| **IR-02** | **SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY** | |
| | **IR-02_ODP[04]** | ***określono zdarzenia, które skutkują rozpoczęciem przeglądu treści szkolenia z zakresu reagowania na incydenty;*** |
| | **IR-02a.01** | szkolenie z zakresu reagowania na incydenty jest zapewnione użytkownikom systemu zgodnie z przypisanymi rolami i obowiązkami w ciągu ***<okresu IR-02_ODP[01]>*** od objęcia roli lub obowiązków w zakresie reagowania na incydenty lub uzyskania dostępu do systemu; |
| | **IR-02a.02** | jeśli wymagają tego zmiany w systemie, przeprowadza się szkolenie dla użytkowników systemu w zakresie reagowania na incydenty zgodnie z przypisanymi rolami i obowiązkami; |
| | **IR-02a.03** | szkolenie z zakresu reagowania na incydenty jest następnie prowadzone dla użytkowników systemu zgodnie z przypisanymi rolami i obowiązkami z ***<częstotliwością IR-02_ODP[02]>***; |
| | **IR-02b.[01]** | obowiązująca treść szkolenia w zakresie reagowania na incydenty podlega przeglądowi i aktualizacji z ***<częstotliwością IR-02_ODP[03]>***; |
| | **IR-02b.[02].** | obowiązująca treść szkolenia w zakresie reagowania na incydenty podlega przeglądowi i aktualizacji po ***<zdarzeniach IR-02_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące szkolenia w zakresie reagowania na incydenty; program szkolenia w zakresie reagowania na incydenty; materiały szkoleniowe w zakresie reagowania na incydenty; plan ochrony prywatności; plan reagowania na incydenty; dokumentacja szkoleniowa w zakresie reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za szkolenie w zakresie reagowania na incydenty oraz za kwestie operacyjne; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **IR-02(01)** | **SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY \| ZDARZENIA SYMULOWANE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-02(01)** | Do szkolenia w zakresie reagowania na incydenty włącza się zdarzenia symulowane, aby ułatwić personelowi skuteczne reagowanie w sytuacjach kryzysowych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-02(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące szkolenia w zakresie reagowania na incydenty; program szkolenia w zakresie reagowania na incydenty; materiały szkoleniowe w zakresie reagowania na incydenty; plan reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-02(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za szkolenie w zakresie reagowania na incydenty oraz za kwestie operacyjne; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **IR-02(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdarzenia symulowane do szkoleń z zakresu reagowania na incydenty]. |

| | | |
|---|---|---|
| **IR-02(02)** | **SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY \| ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-02(02)_ODP** | ***określono automatyczne mechanizmy wykorzystywane w środowisku do szkoleń w zakresie reagowania na incydenty;*** |

| | | |
|---|---|---|
| **IR-02(02)** | **SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY \| ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE** | |
| | **IR-02(02)** | środowisko do szkoleń w zakresie reagowania na incydenty jest zapewniane przy użyciu ***<automatyzowanych mechanizmów IR-02(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące szkolenia w zakresie reagowania na incydenty; program szkolenia w zakresie reagowania na incydenty; materiały szkoleniowe w zakresie reagowania na incydenty; automatyczne mechanizmy wspierające szkolenie w zakresie reagowania na incydenty; plan reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za szkolenie w zakresie reagowania na incydenty oraz za kwestie operacyjne; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **IR-02(02)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy zapewniające wiarygodne i realistyczne środowisko do szkoleń w zakresie reagowania na incydenty]. |

| | | |
|---|---|---|
| **IR-02(03)** | **SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY \| NARUSZENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-02(03)[01]** | zapewnione jest szkolenie w zakresie reagowania na incydenty, które dotyczy identyfikacji naruszeń i reagowania na nie; |
| | **IR-02(03)[02]** | zapewnione jest szkolenie w zakresie reagowania na incydenty, które dotyczy procesu zgłaszania naruszeń w ramach organizacji. |

| | | |
|---|---|---|
| **IR-02(03)** | **SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY \| NARUSZENIE** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-02(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; polityka planowania awaryjnego; procedury dotyczące testowania reagowania na incydenty; procedury dotyczące testowania planu awaryjnego; materiały w zakresie testowania reagowania na incydenty; wyniki testów reagowania na incydenty; plan reagowania na incydenty; plan awaryjny; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-02(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za szkolenie w zakresie reagowania na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **IR-03** | **TESTOWANIE REAGOWANIA NA INCYDENTY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-03_ODP[01]** | ***określono częstotliwość, z jaką należy testować zdolności do reagowania na incydenty w systemie;*** |
| | **IR-03_ODP[02]** | ***określono testy stosowane do badania zdolności do reagowania na incydenty w systemie;*** |
| | **IR-03** | zdolność do reagowania na incydenty w systemie testuje się z ***<częstotliwością IR-03_ODP[01]>*** przy użyciu ***<testów IR-03_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IR-03** | **TESTOWANIE REAGOWANIA NA INCYDENTY** | |
| | **IR-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; polityka planowania awaryjnego; procedury dotyczące testowania reagowania na incydenty; procedury dotyczące testowania planu awaryjnego; materiały w zakresie testowania reagowania na incydenty; wyniki testów reagowania na incydenty; plan reagowania na incydenty; plan awaryjny; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za testowanie procesu reagowania na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **IR-03(01)** | **TESTOWANIE REAGOWANIA NA INCYDENTY \| AUTOMATYCZNE TESTOWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-03(01)_ODP** | ***określono automatyczne mechanizmy wykorzystywane do testowania zdolności reagowania na incydenty;*** |
| | **IR-03(01)** | zdolność do reagowania na incydenty jest testowana przy użyciu ***<automatycznych mechanizmów IR-03(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; polityka planowania awaryjnego; procedury dotyczące testowania reagowania na incydenty; procedury dotyczące testowania planu awaryjnego; dokumentacja dotycząca testowania reagowania na incydenty; wyniki testów reagowania na incydenty; plan reagowania na incydenty; plan awaryjny; plan bezpieczeństwa systemu; automatyczne mechanizmy wspierające testowanie reagowania na incydenty; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IR-03(01)** | **TESTOWANIE REAGOWANIA NA INCYDENTY \| AUTOMATYCZNE TESTOWANIE** | |
| | **IR-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za testowanie reagowania na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji. |
| | **IR-03(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy, które dokładniej i skuteczniej testują zdolności do reagowania na incydenty]. |

| | | |
|---|---|---|
| **IR-03(02)** | **TESTOWANIE REAGOWANIA NA INCYDENTY \| KOORDYNACJA Z POWIĄZANYMI PLANAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-03(02)** | testowanie reagowania na incydenty jest koordynowane z elementami organizacyjnymi odpowiedzialnymi za plany powiązane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; polityka planowania ciągłości działania; procedury dotyczące testowania reagowania na incydenty; dokumentacja testowania reagowania na incydenty; plan reagowania na incydenty; plany awaryjne; plany odzyskiwania danych po awarii; plany ciągłości działania; plany w zakresie komunikacji kryzysowej; plany dot. infrastruktury krytycznej; plany awaryjne dla mieszkańców; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za testowanie reagowania na incydenty; personel organizacyjny odpowiedzialny za weryfikację planów organizacyjnych związanych z testowaniem reagowania na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **IR-03(03)** | **TESTOWANIE REAGOWANIA NA INCYDENTY \| CIĄGŁE DOSKONALENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-03(03)(a)[01]** | dane jakościowe z testów są wykorzystywane do określenia skuteczności procesów reagowania na incydenty; |
| | **IR-03(03)(a)[02]** | dane ilościowe z testów są wykorzystywane do określenia skuteczności procesów reagowania na incydenty; |
| | **IR-03(03)(b)[01]** | dane jakościowe z testów są wykorzystywane do ciągłego doskonalenia procesów reagowania na incydenty; |
| | **IR-03(03)(b)[02]** | dane ilościowe z testów są wykorzystywane do ciągłego doskonalenia procesów reagowania na incydenty; |
| | **IR-03(03)(c)[01]** | dane jakościowe z testów są wykorzystywane do zapewnienia dokładnych pomiarów i metryk dotyczących reakcji na incydenty; |
| | **IR-03(03)(c)[02]** | dane ilościowe z testów są wykorzystywane do zapewnienia dokładnych pomiarów i metryk dotyczących reakcji na incydenty; |
| | **IR-03(03)(c)[03]** | dane jakościowe z testów są wykorzystywane do zapewnienia spójnych pomiarów i metryk dotyczących reakcji na incydenty; |
| | **IR-03(03)(c)[04]** | dane ilościowe z testów są wykorzystywane do zapewnienia spójnych pomiarów i metryk dotyczących reakcji na incydenty; |
| | **IR-03(03)(c)[05]** | dane jakościowe z testów są wykorzystywane do zapewnienia pomiarów i metryk dotyczących reakcji na incydenty, w powtarzalnym formacie; |
| | **IR-03(03)(c)[06]** | dane ilościowe z testów są wykorzystywane do zapewnienia pomiarów i metryk dotyczących reakcji na incydenty, w powtarzalnym formacie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IR-03(03)** | **TESTOWANIE REAGOWANIA NA INCYDENTY \| CIĄGŁE DOSKONALENIE** | |
| | **IR-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; polityka planowania ciągłości działania; procedury dotyczące testowania reagowania na incydenty; dokumentacja testowania reagowania na incydenty; plan reagowania na incydenty; plany awaryjne; plany odzyskiwania danych po awarii; plany ciągłości działania; plany w zakresie komunikacji kryzysowej; plany dot. infrastruktury krytycznej; plany awaryjne dla mieszkańców; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za testowanie reagowania na incydenty; personel organizacyjny odpowiedzialny za weryfikację planów organizacyjnych związanych z testowaniem reagowania na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **IR-04** | **OBSŁUGA INCYDENTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04a.[01]** | zapewniono zdolność do obsługi incydentów zgodnie z planem reagowania na incydenty; |
| | **IR-04a.[02]** | zdolność do obsługi incydentów obejmuje przygotowanie; |
| | **IR-04a.[03]** | zdolność do obsługi incydentów obejmuje wykrywanie i analizę; |
| | **IR-04a.[04]** | zdolność do obsługi incydentów obejmuje ich powstrzymywanie; |
| | **IR-04a.[05]** | możliwość obsługi incydentów obejmuje ich eliminację; |
| | **IR-04a.[06]** | zdolność do obsługi incydentów obejmuje odzyskiwanie; |
| | **IR-04b.** | działania związane z obsługą incydentów są skoordynowane z działaniami w zakresie planowania awaryjnego; |

| | | |
|---|---|---|
| **IR-04** | **OBSŁUGA INCYDENTÓW** | |
| | **IR-04c.[01]** | wnioski wyciągnięte z bieżących działań związanych z obsługą incydentów są włączane do procedur w zakresie reagowania na incydenty, szkolenia i testowania; |
| | **IR-04c.[02]** | zmiany wynikające z uwzględnionych wniosków są odpowiednio wdrażane; |
| | **IR-04d.[01]** | dyscyplina w zakresie działań związanych z obsługą incydentów jest porównywalna i przewidywalna w całej organizacji; |
| | **IR-04d.[02]** | intensywność działań związanych z obsługą incydentów jest porównywalna i przewidywalna w całej organizacji; |
| | **IR-04d.[03]** | zakres działań związanych z obsługą incydentów jest porównywalny i przewidywalny w całej organizacji; |
| | **IR-04d.[04]** | wyniki działań związanych z obsługą incydentów są porównywalne i przewidywalne w całej organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; polityka planowania awaryjnego; procedury dotyczące obsługi incydentów; plan reagowania na incydenty; plan awaryjny; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentów; personel organizacyjny odpowiedzialny za planowanie awaryjne; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **IR-04-Test** | [WYBÓR SPOŚRÓD: Możliwości organizacji w zakresie obsługi incydentów]. |

| | | |
|---|---|---|
| **IR-04(01)** | **OBSŁUGA INCYDENTÓW \| AUTOMATYCZNE PROCESY OBSŁUGI ZDARZEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(01)_ODP** | ***określono automatyczne mechanizmy wykorzystywane do wsparcia procesu obsługi incydentów;*** |
| | **IR-04(01)** | proces obsługi incydentów jest wspierany przy użyciu ***<automatycznych mechanizmów IR-04(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; automatyczne mechanizmy wspierające obsługę incydentów; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan reagowania na incydenty; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IR-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **IR-04(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspierające lub wdrażające proces obsługi incydentów]. |

| | | |
|---|---|---|
| **IR-04(02)** | **OBSŁUGA INCYDENTÓW \| DYNAMICZNA REKONFIGURACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(02)_ODP[01]** | ***określono rodzaje dynamicznej rekonfiguracji dla komponentów systemu;*** |

| | | |
|---|---|---|
| **IR-04(02)** | **OBSŁUGA INCYDENTÓW \| DYNAMICZNA REKONFIGURACJA** | |
| | **IR-04(02)_ODP[02]** | ***określono komponenty systemu, które wymagają dynamicznej rekonfiguracji;*** |
| | **IR-04(02)** | ***<rodzaje dynamicznej rekonfiguracji IR-04(02)_ODP[01]>*** dla ***<komponentów systemu IR-04(02)_ODP[02]>*** stanowią element zdolności do reagowania na incydenty. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; mechanizmy wspierające obsługę incydentów; wykaz komponentów systemu, podlegających dynamicznej rekonfiguracji w ramach zdolności do reagowania na incydenty; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan reagowania na incydenty; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IR-04(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **IR-04(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające dynamiczną rekonfigurację komponentów w ramach reakcji na incydenty]. |

| | | |
|---|---|---|
| **IR-04(04)** | **OBSŁUGA INCYDENTÓW \| KORELACJA INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(04)** | informacje o incydentach i indywidualnej reakcji na nie są skorelowane w celu uzyskania ogólnoorganizacyjnej perspektywy w zakresie świadomości i reakcji na incydenty. |

| IR-04(04) | OBSŁUGA INCYDENTÓW \| KORELACJA INFORMACJI | |
|---|---|---|
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04(04)-Badanie** | [WYBÓR SPOŚRÓD: polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; plan reagowania na incydenty; plan ochrony prywatności; mechanizmy wspierające korelację incydentów i korelację zdarzeń;<br>dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; plan ochrony prywatności; dzienniki korelacji zarządzania incydentami; dzienniki korelacji zarządzania zdarzeniami; dzienniki zarządzania informacjami o bezpieczeństwie i zdarzeniami; raporty korelacji zarządzania incydentami; raporty korelacji zarządzania zdarzeniami; raporty zarządzania informacjami o bezpieczeństwie i zdarzeniach; zapisy z audytu; inne istotne dokumenty lub zapisy]. |
| | **IR-04(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny, z którym mają być skorelowane informacje o incydencie i indywidualne reakcje na incydent]. |
| | **IR-04(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące korelacji informacji o incydencie i indywidualnych reakcji na incydent; mechanizmy wspierające i lub wdrażające korelację informacji o incydencie z indywidualnymi reakcjami na incydent]. |

| IR-04(05) | OBSŁUGA INCYDENTÓW \| AUTOMATYCZNE WYŁĄCZANIE SYSTEMU | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(05)_ODP** | ***określono naruszenia bezpieczeństwa, które skutkują automatycznym wyłączeniem systemu;*** |

| IR-04(05) | OBSŁUGA INCYDENTÓW \| AUTOMATYCZNE WYŁĄCZANIE SYSTEMU | |
|---|---|---|
| | **IR-04(05)** | wdrożono konfigurowalną możliwość automatycznego wyłączenia systemu w przypadku wykrycia ***<naruszenia bezpieczeństwa IR-04(05)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; automatyczne mechanizmy wspierające obsługę incydentów; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; plan reagowania na incydenty; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-04(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **IR-04(05)-Test** | [WYBÓR SPOŚRÓD: Zdolność organizacji do obsługi incydentów; automatyczne mechanizmy wspierające lub wdrażające mechanizmy automatycznego wyłączania systemu]. |

| IR-04(06) | OBSŁUGA INCYDENTÓW \| ZAGROŻENIA WEWNĘTRZNE | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(06)** | wdrożono zdolność do obsługi incydentów związanych z zagrożeniami wewnętrznymi. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IR-04(06)** | **OBSŁUGA INCYDENTÓW \| ZAGROŻENIA WEWNĘTRZNE** | |
| | **IR-04(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; mechanizmy wspierające obsługę incydentów; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan reagowania na incydenty; plan bezpieczeństwa systemu; zapisy z audytu; inne istotne dokumenty lub zapisy]. |
| | **IR-04(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **IR-04(06)-Test** | [WYBÓR SPOŚRÓD: Możliwości organizacji w zakresie obsługi incydentów]. |

| | | |
|---|---|---|
| **IR-04(07)** | **OBSŁUGA INCYDENTÓW \| ZAGROŻENIA WEWNĘTRZNE — KOORDYNACJA WEWNĄTRZ ORGANIZACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(07)_ODP** | ***określono podmioty, które wymagają koordynacji w zakresie zdolności do obsługi incydentów związanych z zagrożeniami wewnętrznymi;*** |
| | **IR-04(07)[01]** | zdolności do obsługi incydentów związanych z zagrożeniami wewnętrznymi są koordynowane; |
| | **IR-04(07)[02]** | zdolności do skoordynowanej obsługi incydentów obejmują ***<podmioty IR-04(07)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **IR-04(07)** | **OBSŁUGA INCYDENTÓW \| ZAGROŻENIA WEWNĘTRZNE — KOORDYNACJA WEWNĄTRZ ORGANIZACJI** | |
| | **IR-04(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; plan reagowania na incydenty; plan programowy dotyczący zagrożeń wewnętrznych; koncepcja działań operacyjnych w zakresie zagrożeń wewnętrznych; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-04(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel/elementy organizacyjne, z którymi ma być koordynowana zdolność do obsługi incydentów]. |
| | **IR-04(07)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie koordynacji obsługi incydentów]. |

| | | |
|---|---|---|
| **IR-04(08)** | **OBSŁUGA INCYDENTÓW \| KOORDYNACJA Z ORGANIZACJAMI ZEWNĘTRZNYMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(08)_ODP[01]** | ***określono organizacje zewnętrzne, którym mają być udostępniane informacje o incydencie w organizacji i z którymi informacje te mają być koordynowane;*** |
| | **IR-04(08)_ODP[02]** | ***określono informacje o incydentach, które mają być korelowane i udostępniane organizacjom zewnętrznym zdefiniowanym przez organizację;*** |
| | **IR-04(08)** | prowadzi się koordynację z ***<organizacjami zewnętrznymi IR-04(08)_ODP[01]>*** w celu korelacji i udostępniania ***<informacji o incydencie IR-04(08)_ODP[02]>***, aby wypracować międzyorganizacyjną perspektywę w zakresie świadomości incydentów i skuteczniejszego reagowania na nie. |

| IR-04(08) | OBSŁUGA INCYDENTÓW \| KOORDYNACJA Z ORGANIZACJAMI ZEWNĘTRZNYMI | |
|---|---|---|
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; lista organizacji zewnętrznych; zapisy dotyczące koordynacji obsługi incydentów z organizacjami zewnętrznymi; plan reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-04(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel z organizacji zewnętrznych, z którymi informacje dotyczące reakcji na incydent mają być koordynowane, współdzielone i skorelowane]. |
| | **IR-04(08)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie koordynowania informacji o obsłudze incydentów z organizacjami zewnętrznymi]. |

| IR-04(09) | OBSŁUGA INCYDENTÓW \| ZDOLNOŚĆ DO REAGOWANIA DYNAMICZNEGO | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(09)_ODP** | ***określono dynamiczne zdolności reagowania, które mają być wykorzystywane do reagowania na incydenty;*** |
| | **IR-04(09)** | stosuje się ***<dynamiczne zdolności reagowania IR-04(09)_ODP> do*** reagowania na incydenty. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| IR-04(09) | OBSŁUGA INCYDENTÓW \| ZDOLNOŚĆ DO REAGOWANIA DYNAMICZNEGO | |
|---|---|---|
| | **IR-04(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; automatyczne mechanizmy wspierające dynamiczne zdolności reagowania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan reagowania na incydenty; plan bezpieczeństwa systemu; zapisy z audytu; inne istotne dokumenty lub zapisy]. |
| | **IR-04(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **IR-04(09)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zdolności dynamicznego reagowania; automatyczne mechanizmy wspierające lub wdrażające zdolność organizacji do dynamicznego reagowania]. |

| IR-04(10) | OBSŁUGA INCYDENTÓW \| KOORDYNACJA ŁAŃCUCHA DOSTAW | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(10)** | Działania związane z obsługą incydentów dotyczących zdarzeń w łańcuchu dostaw są koordynowane z innymi organizacjami działającymi w ramach łańcucha dostaw. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące koordynacji łańcucha dostaw i wymiany informacji o ryzyku w łańcuchu dostaw z odpowiednim organem; umowy kupna; umowy o poziomie usług; plan reagowania na incydenty; plan zarządzania ryzykiem w łańcuchu dostaw; plan bezpieczeństwa systemu; plany innych organizacji działających w ramach łańcucha dostaw w zakresie reagowania na incydenty; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IR-04(10)** | **OBSŁUGA INCYDENTÓW \| KOORDYNACJA ŁAŃCUCHA DOSTAW** | |
| | **IR-04(10)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentów; Personel organizacyjny odpowiedzialny za kwestie misji i działalności biznesowej; personel organizacyjny odpowiedzialny za kwestie prawne; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem w łańcuchu dostaw; personel organizacyjny odpowiedzialny za zakupy]. |

| | | |
|---|---|---|
| **IR-04(11)** | **OBSŁUGA INCYDENTÓW \| ZINTEGROWANY ZESPÓŁ REAGOWANIA NA INCYDENTY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(11)_ODP** | ***określono okres, w którym może zostać powołany zintegrowany zespół reagowania na incydenty;*** |
| | **IR-04(11)[01]** | zespół reagowania na incydenty został powołany i kontynuuje działalność; |
| | **IR-04(11)[02]** | zintegrowany zespół reagowania na incydenty może zostać wysłany do dowolnej lokalizacji wskazanej przez organizację w ***<okresie IR-04(11)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04(11)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; procedury dotyczące planowania reakcji na incydenty; plan reakcji na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-04(11)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; członkowie zintegrowanego zespołu reagowania na incydenty]. |

| IR-04(12) | **OBSŁUGA INCYDENTÓW \| ANALIZA KRYMINALISTYCZNA ZŁOŚLIWEGO KODU** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(12)[01]** | złośliwy kod pozostający w systemie jest analizowany po incydencie; |
| | **IR-04(12)[02]** | inne szczątkowe artefakty pozostające w systemie (jeśli istnieją) są analizowane po incydencie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; procedury dotyczące złośliwego kodu i analizy kryminalistycznej; procedury dotyczące reagowania na incydenty; plan reagowania na incydenty; dokumentacja projektowa systemu; mechanizmy, narzędzia i techniki ochrony przed złośliwym kodem; wyniki analiz złośliwego kodu; plan bezpieczeństwa systemu; zapisy z audytu systemu; inne istotne dokumenty lub zapisy]. |
| | **IR-04(12)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny<br>odpowiedzialny za ochronę przed złośliwym kodem; personel organizacyjny odpowiedzialny za reagowanie na incydenty lub zarządzanie nimi]. |
| | **IR-04(12)-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny w zakresie reagowania na incydenty; procesy organizacyjne w zakresie prowadzenia analizy kryminalistycznej; narzędzia i techniki analizy cech i zachowania złośliwego kodu]. |

| | | |
|---|---|---|
| **IR-04(13)** | **OBSŁUGA INCYDENTÓW \| ANALIZA ZACHOWAŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(13)_ODP** | ***określono środowiska lub zasoby, które mogą zawierać lub mogą być związane z anormalnym bądź podejrzanym zachowaniem o wrogim charakterze;*** |
| | **IR-04(13)** | analizowane są zachowania anormalne lub podejrzane o wrogim charakterze, prowadzone w ***<środowiskach lub zasobach IR-04(13)_ODP>*** lub w związku z nimi; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04(13)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące narzędzi i technik monitorowania systemu; plan reagowania na incydenty; dzienniki lub rejestry monitorowania systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa; lista komponentów systemu; schemat sieci; dokumentacja protokołów systemowych; lista dopuszczalnych progów dla wyników fałszywie dodatnich i fałszywie ujemnych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IR-04(13)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **IR-04(13)-Test** | [WYBÓR SPOŚRÓD: Organizacyjne procesy wykrywania zachowań anormalnych]. |

| | | |
|---|---|---|
| **IR-04(14)** | **OBSŁUGA INCYDENTÓW \| OPERACYJNE CENTRUM BEZPIECZEŃSTWA (SOC)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(14)[01]** | ustanowiono operacyjne centrum bezpieczeństwa; |
| | **IR-04(14)[02]** | utrzymywane jest operacyjne centrum bezpieczeństwa; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04(14)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; polityka planowania awaryjnego; procedury dotyczące obsługi incydentów; procedury dotyczące działania operacyjnego centrum bezpieczeństwa; mechanizmy wspierające dynamiczne zdolności reagowania; plan reagowania na incydenty; plan awaryjny; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IR-04(14)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę incydentów; personel organizacyjny odpowiedzialny za planowanie awaryjne; personel operacyjnego centrum bezpieczeństwa; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **IR-04(14)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwości operacyjnego centrum bezpieczeństwa; mechanizmy, wspierające lub wdrażające proces obsługi incydentów]. |

| | | |
|---|---|---|
| **IR-04(15)** | **OBSŁUGA INCYDENTÓW \| RELACJE PUBLICZNE I NAPRAWA REPUTACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-04(15)(a)** | prowadzi się zarządzanie relacjami publicznymi w związku z incydentem; |

| | | |
|---|---|---|
| **IR-04(15)** | **OBSŁUGA INCYDENTÓW \| RELACJE PUBLICZNE I NAPRAWA REPUTACJI** | |
| | **IR-04(15)(b)** | stosuje się środki mające na celu naprawę reputacji organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-04(15)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące reagowania na incydenty; procedury dotyczące obsługi incydentów; plan reagowania na incydenty; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IR-04(15)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obsługę zdarzeń; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za komunikację lub relacje publiczne]. |

| | | |
|---|---|---|
| **IR-05** | **MONITOROWANIE INCYDENTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-05[01]** | incydenty są śledzone; |
| | **IR-05[02]** | incydenty są dokumentowane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące monitorowania incydentów; zapisy i dokumentacja dotycząca reagowania na incydenty; plan reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie zdarzeń; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |

| | | |
|---|---|---|
| **IR-05** | **MONITOROWANIE INCYDENTÓW** | |
| | **IR-05-Test** | [WYBÓR SPOŚRÓD: Zdolność organizacji do monitorowania incydentów; mechanizmy wspierające lub wdrażające śledzenie i dokumentowanie incydentów bezpieczeństwa w systemie]. |

| | | |
|---|---|---|
| **IR-05(01)** | **MONITOROWANIE INCYDENTÓW \| AUTOMATYCZNE ŚLEDZENIE, ZBIERANIE DANYCH I ANALIZA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-05(01)_ODP[01]** | ***określono automatyczne mechanizmy wykorzystywane do śledzenia incydentów;*** |
| | **IR-05(01)_ODP[02]** | ***określono automatyczne mechanizmy wykorzystywane do gromadzenia informacji o incydentach;*** |
| | **IR-05(01)_ODP[03]** | ***określono automatyczne mechanizmy wykorzystywane do analizy informacji o incydentach;*** |
| | **IR-05(01)[01]** | śledzenie incydentów odbywa się za pomocą ***<automatycznych mechanizmów IR-05(01)_ODP[01]>***; |
| | **IR-05(01)[02]** | informacje o incydentach zbierane są za pomocą ***<automatycznych mechanizmów IR-05(01)_ODP[02]>***; |
| | **IR-05(01)[03]** | informacje o incydentach są analizowane z wykorzystaniem ***<automatycznych mechanizmów IR-05(01)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-05(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące monitorowania incydentów; zapisy i dokumentacja dotycząca reagowania na incydenty; plan bezpieczeństwa systemu; plan reagowania na incydenty; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IR-05(01)** | **MONITOROWANIE INCYDENTÓW \| AUTOMATYCZNE ŚLEDZENIE, ZBIERANIE DANYCH I ANALIZA** | |
| | **IR-05(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie zdarzeń; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji. |
| | **IR-05(01)-Test** | [WYBÓR SPOŚRÓD: Zdolność organizacji do monitorowania incydentów; automatyczne mechanizmy wspierające lub wdrażające śledzenie i dokumentowanie incydentów bezpieczeństwa w systemie]. |

| | | |
|---|---|---|
| **IR-06** | **ZGŁASZANIE INCYDENTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-06_ODP[01]** | ***określono okres, w którym personel powinien zgłaszać podejrzenia co do wystąpienia incydentów do organizacyjnej jednostki reagowania na incydenty;*** |
| | **IR-06_ODP[02]** | ***określono organy, którym należy zgłaszać informacje o incydencie;*** |
| | **IR-06a.** | personel jest zobowiązany do zgłaszania podejrzeń co do wystąpienia incydentów do organizacyjnej komórki reagowania na incydenty w ***<okresie IR-06_ODP[01]>***; |
| | **IR-06b.** | informacje o incydencie zgłaszane są do ***<władz IR-06_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące zgłaszania incydentów; zapisy i dokumentacja dotycząca zgłaszania incydentów; plan reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **IR-06** | **ZGŁASZANIE INCYDENTÓW** | |
| | **IR-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zgłaszanie incydentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel, zgłaszający/zobowiązany do zgłaszania incydentów; personel (władze), któremu należy zgłaszać informacje o incydentach; użytkownicy systemu]. |
| | **IR-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zgłaszania incydentów; mechanizmy wspierające lub wdrażające zgłaszanie incydentów]. |

| | | |
|---|---|---|
| **IR-06(01)** | **ZGŁASZANIE INCYDENTÓW \| ZGŁASZANIE AUTOMATYCZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-06(01)_ODP** | ***określono automatyczne mechanizmy służące do zgłaszania incydentów;*** |
| | **IR-06(01)** | incydenty są zgłaszane przy użyciu ***<automatycznych mechanizmów IR-06(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-06(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące zgłaszania incydentów; automatyczne mechanizmy wspierające zgłaszanie incydentów; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>plan reagowania na incydenty; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IR-06(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zgłaszanie incydentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji. |

| | | |
|---|---|---|
| **IR-06(01)** | **ZGŁASZANIE INCYDENTÓW \| ZGŁASZANIE AUTOMATYCZNE** | |
| | **IR-06(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zgłaszania incydentów; automatyczne mechanizmy wspierające lub wdrażające zgłaszanie incydentów bezpieczeństwa]. |

| | | |
|---|---|---|
| **IR-06(02)** | **ZGŁASZANIE INCYDENTÓW \| PODATNOŚĆ NA INCYDENTY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-06(02)_ODP** | ***określono personel lub role, do których zgłaszane są podatności systemu związane ze zgłoszonymi incydentami;*** |
| | **IR-06(02)** | podatności systemu związane ze zgłoszonymi incydentami są zgłaszane do ***<personelu lub ról IR-06(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-06(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące zgłaszania incydentów; plan reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; raporty dotyczące incydentów bezpieczeństwa i związanych z nimi słabych punktów systemu; inne istotne dokumenty lub zapisy]. |
| | **IR-06(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zgłaszanie incydentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci; personel, któremu należy zgłaszać podatności związane z incydentami bezpieczeństwa]. |
| | **IR-06(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zgłaszania incydentów; mechanizmy wspierające lub wdrażające zgłaszanie podatności związanych z incydentami bezpieczeństwa]. |

| | | |
|---|---|---|
| **IR-06(03)** | **ZGŁASZANIE INCYDENTÓW \| KOORDYNACJA ŁAŃCUCHA DOSTAW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-06(03)** | informacje o incydentach przekazywane są dostawcy produktu lub usługi oraz innym organizacjom zaangażowanym w łańcuch dostaw lub zarządzanie nim na potrzeby systemu lub jego komponentów związanych z incydentem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-06(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące koordynacji łańcucha dostaw i wymiany informacji o ryzyku w łańcuchu dostaw z odpowiednim organem; umowy kupna; umowy o poziomie usług; plan reagowania na incydenty; plan zarządzania ryzykiem w łańcuchu dostaw; plan bezpieczeństwa systemu; plany innych organizacji działających w ramach łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **IR-06(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zgłaszanie incydentów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem w łańcuchu dostaw; personel organizacyjny odpowiedzialny za zakupy]. |
| | **IR-06(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zgłaszania incydentów; procesy organizacyjne dotyczące wymiany informacji o ryzyku w łańcuchu dostaw; mechanizmy wspierające lub wdrażające zgłaszanie informacji o incydentach zaangażowanych w łańcuch dostaw]. |

| | | |
|---|---|---|
| **IR-07** | **WSPARCIE REAGOWANIA NA INCYDENTY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-07[01]** | zapewnione są zasoby wsparcia w zakresie reagowania na incydenty, integralnie związane ze zdolnością organizacji do reagowania na incydenty; |
| | **IR-07[02]** | zasoby wsparcia w zakresie reagowania na incydenty zapewniają użytkownikom systemu porady i pomoc odnośnie do reagowania na incydenty i zgłaszania ich. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące wsparcia reagowania na incydenty; plan reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za wsparcie w reagowaniu na incydenty; personel organizacyjny z dostępem do zdolności w zakresie wsparcia w reagowaniu na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **IR-07-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wsparcia w reagowaniu na incydenty; mechanizmy wspierające lub wdrażające wsparcie w reagowaniu na incydenty]. |

| | | |
|---|---|---|
| **IR-07(01)** | **WSPARCIE REAGOWANIA NA INCYDENTY \| AUTOMATYCZNE WSPARCIE DOSTĘPNOŚCI INFORMACJI/OBSŁUGI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-07(01)_ODP** | ***określono automatyczne mechanizmy stosowane w celu zwiększenia dostępności informacji i wsparcia w zakresie reagowania na incydenty;*** |
| | **IR-07(01)** | dostępność informacji i wsparcia w zakresie reagowania na incydenty jest zwiększana przy użyciu ***<mechanizmów automatycznych IR-07(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-07(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące wsparcia w reagowaniu na incydenty; automatyczne mechanizmy pomagające w działaniach w zakresie wsparcia w reagowaniu na incydenty; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan reagowania na incydenty; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IR-07(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za wsparcie w reagowaniu na incydenty; personel organizacyjny z dostępem do zdolności w zakresie wsparcia w reagowaniu na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **IR-07(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wsparcia w reagowaniu na incydenty; automatyczne mechanizmy wspierające lub wdrażające zwiększenie dostępności informacji i wsparcia w zakresie reagowania na incydenty]. |

| | | |
|---|---|---|
| **IR-07(02)** | **WSPARCIE REAGOWANIA NA INCYDENTY \| KOORDYNACJA Z DOSTAWCAMI ZEWNĘTRZNYMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-07(02)(a)** | ustanowiono bezpośrednie, oparte na współpracy relacje między jednostką reagowania na incydenty a zewnętrznymi dostawcami funkcji ochrony systemu; |
| | **IR-07(02)(b)** | dostawcom zewnętrznym wskazuje się członków organizacyjnego zespołu reagowania na incydenty. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-07(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące wsparcia reagowania na incydenty; plan reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **IR-07(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za wsparcie i pomoc w reagowaniu na incydenty; zewnętrzni dostawcy środków ochrony systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i prywatność]. |

| | | |
|---|---|---|
| **IR-08** | **PLAN REAGOWANIA NA INCYDENTY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-08_ODP[01]** | ***Określono personel lub role odpowiedzialne za przeglądanie i zatwierdzanie planu reagowania na incydenty;*** |
| | **IR-08_ODP[02]** | ***określono częstotliwość przeglądów i zatwierdzania planu reagowania na incydenty;*** |

| IR-08 | PLAN REAGOWANIA NA INCYDENTY | |
|---|---|---|
| | **IR-08_ODP[03]** | ***określono podmioty, personel lub role, którym powierzono odpowiedzialność za reagowanie na incydenty;*** |
| | **IR-08_ODP[04]** | ***określono personel odpowiedzialny za reagowanie na incydenty (zidentyfikowany z imienia i nazwiska lub pełnionej funkcji), któremu należy przekazać kopie planu reagowania na incydenty;*** |
| | **IR-08_ODP[05]** | ***określono elementy organizacyjne, którym mają być przekazane kopie planu reagowania na incydenty;*** |
| | **IR-08_ODP[06]** | ***określono personel reagujący na incydenty (zidentyfikowany z imienia i nazwiska lub pełnionej funkcji), któremu należy przekazać kopie planu reagowania na incydenty;*** |
| | **IR-08_ODP[07]** | ***określono elementy organizacyjne, którym przekazywane są zmiany w planie reagowania na incydenty;*** |
| | **IR-08a.01** | opracowano plan reagowania na incydenty, który stanowi dla organizacji mapę drogową w procesie wdrażania zdolności do reagowania na incydenty; |
| | **IR-08a.02** | opracowano plan reagowania na incydenty, który opisuje strukturę i organizację zdolności do reagowania na incydenty; |
| | **IR-08a.03** | opracowano plan reagowania na incydenty, który zapewnia ogólne ujęcie tego, jak zdolność reagowania na incydenty wpisuje się w działania całej organizacji; |
| | **IR-08a.04** | opracowano plan reagowania na incydenty, który spełnia unikalne wymagania organizacji w odniesieniu do jej misji, wielkości, struktury i funkcji; |
| | **IR-08a.05** | opracowano plan reagowania na incydenty, który określa incydenty podlegające zgłoszeniu; |
| | **IR-08a.06** | opracowano plan reagowania na incydenty, który dostarcza metryki do pomiaru zdolności reagowania na incydenty w organizacji; |

| IR-08 | PLAN REAGOWANIA NA INCYDENTY | |
|---|---|---|
| | **IR-08a.07** | opracowano plan reagowania na incydenty, który określa zasoby i wsparcie niezbędne do skutecznego utrzymania i rozwoju zdolności do reagowania na incydenty; |
| | **IR-08a.08** | opracowano plan reagowania na incydenty, który obejmuje wymianę informacji o incydentach; |
| | **IR-08a.09** | opracowano plan reagowania na incydenty, który jest przeglądany i zatwierdzany przez ***<personel lub role IR-08_ODP[01]>*** z ***<częstotliwością IR-08_ODP[02]>***; |
| | **IR-08a.10** | opracowano plan reagowania na incydenty, który jednoznacznie określa, że za reagowanie na incydenty odpowiada***<personel lub role IR-08_ODP[03]>***. |
| | **IR-08b.[01]** | kopie planu reagowania na incydenty są przekazywane ***<personelowi reagującemu na incydenty IR-08_ODP[04]>***; |
| | **IR-08b.[02]** | kopie planu reagowania na incydenty są przekazywane ***<elementom organizacyjnym IR-08_ODP[05]>***; |
| | **IR-08c.** | plan reagowania na incydenty jest aktualizowany w celu uwzględnienia zmian systemowych i organizacyjnych lub problemów napotkanych podczas jego wdrażania, realizacji lub testowania; |
| | **IR-08d.[01]** | zmiany w planie reagowania na incydenty są przekazywane do ***<IR-08_ODP[06] personelu reagującego na incydenty>***; |
| | **IR-08d.[02]** | Zmiany w planie reagowania na incydenty są przekazywane do ***<elementom organizacyjnym IR-08_ODP[07]>***; |
| | **IR-08e.[01]** | plan reagowania na incydenty jest chroniony przed nieuprawnionym ujawnieniem; |
| | **IR-08e.[02]** | plan reagowania na incydenty jest chroniony przed nieuprawnioną modyfikacją. |

| **IR-08** | **PLAN REAGOWANIA NA INCYDENTY** | |
|---|---|---|
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące planowania reagowania na incydenty; plan reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; zapisy z przeglądów i zatwierdzeń planu reagowania na incydenty; inne istotne dokumenty lub zapisy]. |
| | **IR-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie reagowania na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **IR-08-Test** | [WYBÓR SPOŚRÓD: Plan reagowania na incydenty i powiązane procesy organizacyjne]. |

| **IR-08(01)** | **PLAN REAGOWANIA NA INCYDENTY \| NARUSZENIA** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-08(01)(a)** | plan reagowania na incydenty dotyczące naruszeń związanych z danymi identyfikacyjnymi obejmuje proces mający na celu ustalenie, czy konieczne jest powiadomienie osób fizycznych lub innych organizacji, w tym organów nadzorczych; |
| | **IR-08(01)(b)** | plan reagowania na incydenty dotyczące naruszeń związanych z danymi identyfikacyjnymi obejmuje proces oceny mający na celu określenie, w jakim zakresie osoby dotknięte naruszeniem doznały szkód, upokorzeń, niedogodności lub niesprawiedliwości, a także wszelkich mechanizmów łagodzących powyższe; |
| | **IR-08(01)(c)** | plan reagowania na incydenty dotyczące naruszeń związanych z danymi identyfikacyjnymi obejmuje identyfikację obowiązujących wymogów w zakresie ochrony prywatności. |

| | | |
|---|---|---|
| **IR-08(01)** | **PLAN REAGOWANIA NA INCYDENTY \| NARUSZENIA** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-08(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące planowania reagowania na incydenty; plan reagowania na incydenty; plan bezpieczeństwa systemu; plan ochrony prywatności; zapisy z przeglądów i zatwierdzeń planu reagowania na incydenty; inne istotne dokumenty lub zapisy]. |
| | **IR-08(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie reagowania na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji]. |
| | **IR-08(01)-Test** | [WYBÓR SPOŚRÓD: Plan reagowania na incydenty i powiązane procesy organizacyjne]. |

| | | |
|---|---|---|
| **IR-09** | **REAKCJA NA WYCIEK/UJAWNIENIE INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-09_ODP[01]** | ***określono personel lub role, którym powierzono odpowiedzialność za reagowanie na wycieki informacji;*** |
| | **IR-09_ODP[02]** | ***określono personel lub role, które mają być ostrzegane o wycieku informacji przy użyciu metody komunikacji niepowiązanej z wyciekiem;*** |
| | **IR-09_ODP[03]** | ***określono działania, które mają być zrealizowane;*** |
| | **IR-09a.** | ***<personel lub role IR-09_ODP[01]>*** ponoszą odpowiedzialność za reagowanie na wycieki informacji; |
| | **IR-09b.** | w odpowiedzi na wycieki informacji identyfikuje się konkretne informacje związane ze „skażeniem” systemu; |

| | | |
|---|---|---|
| **IR-09** | **REAKCJA NA WYCIEK/UJAWNIENIE INFORMACJI** | |
| | **IR-09c.** | ***<personel lub role IR-09_ODP[02]>*** otrzymują powiadomienie o wycieku informacji za pomocą metody komunikacji niepowiązanej z wyciekiem; |
| | **IR-09d.** | w odpowiedzi na wyciek informacji „skażony" system lub komponent systemu zostaje odizolowany; |
| | **IR-09e.** | w odpowiedzi na wyciek informacji usuwa się informacje z „skażonego" systemu lub komponentu; |
| | **IR-09f.** | w odpowiedzi na wyciek informacji identyfikowane są inne systemy lub elementy systemu, które mogły zostać „skażone" w dalszej kolejności; |
| | **IR-09g.** | w odpowiedzi na wyciek informacji przeprowadza się ***<działania IR-09_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące wycieku informacji; plan reagowania na incydenty; plan bezpieczeństwa systemu; zapisy dotyczące alertów/powiadomień o wycieku informacji; lista pracowników, powiadamianych o wycieku informacji; lista działań, które należy podjąć w związku z wyciekiem informacji; inne istotne dokumenty lub zapisy]. |
| | **IR-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za reagowanie na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **IR-09-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące reagowania na wycieki informacji; mechanizmy wspierające lub wdrażające działania w zakresie reagowania na wycieki informacji i związane z tym komunikaty]. |

| | |
|---|---|
| **IR-09(01)** | **REAKCJA NA WYCIEK/UJAWNIENIE INFORMACJI \| ODPOWIEDZIALNY PERSONEL** |
| | [WYCOFANE: Włączone do IR-09]. |

| | | |
|---|---|---|
| **IR-09(02)** | **REAKCJA NA WYCIEK/UJAWNIENIE INFORMACJI \| SZKOLENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-09(02)_ODP** | ***określono częstotliwość, z jaką należy przeprowadzać szkolenia z zakresu reagowania na wycieki informacji;*** |
| | **IR-09(02)** | szkolenie w zakresie reagowania na wyciek informacji jest realizowane z ***<częstotliwością IR-09(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-09(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące szkolenia w zakresie reagowania na wyciek informacji; program szkolenia w zakresie reagowania na wyciek informacji; materiały szkoleniowe w zakresie reagowania na wyciek informacji; plan reagowania na incydenty; plan bezpieczeństwa systemu; dokumentacja szkolenia w zakresie reagowania na wyciek informacji; inne istotne dokumenty lub zapisy]. |
| | **IR-09(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za szkolenia w zakresie reagowania na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **IR-09(03)** | **REAKCJA NA WYCIEK/UJAWNIENIE INFORMACJI \| DZIAŁANIA PO UJAWNIENIU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-09(03)_ODP** | ***określono procedury, które należy wdrożyć, aby zapewnić, że personel organizacyjny dotknięty wyciekiem informacji może nadal wykonywać przydzielone zadania w czasie prowadzenia działań naprawczych w „skażonych" systemach;*** |
| | **IR-09(03)** | wdrożono ***<procedury IR-09(03)_ODP>*** w celu zapewnienia, że personel organizacyjny dotknięty wyciekiem informacji może nadal wykonywać przydzielone zadania w czasie prowadzenia działań naprawczych w „skażonych" systemach. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-09(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące reagowania na incydenty; procedury dotyczące wycieku informacji; plan reagowania na incydenty; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **IR-09(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za reagowanie na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **IR-09(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące działań podejmowanych po wycieku]. |

| | | |
|---|---|---|
| **IR-09(04)** | **REAKCJA NA WYCIEK/UJAWNIENIE INFORMACJI \| WYSTAWIENIE NA DZIAŁANIA OSÓB NIEAUTORYZOWANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **IR-09(04)_ODP** | ***określono zabezpieczenia stosowane wobec pracowników, którzy uzyskali dostęp do informacji wykraczających poza przypisane im uprawnienia dostępu;*** |
| | **IR-09(04)** | wobec pracowników, którzy uzyskali dostęp do informacji wykraczających poza przypisane im uprawnienia dostępu stosuje się ***<zabezpieczenia IR-09(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **IR-09(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka reagowania na incydenty; procedury dotyczące reagowania na incydenty; procedury dotyczące wycieku informacji; plan reagowania na incydenty; plan bezpieczeństwa systemu; zabezpieczenia dotyczące wycieku informacji/uzyskania dostępu do nich przez nieupoważniony personel; inne istotne dokumenty lub zapisy]. |
| | **IR-09(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za reagowanie na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **IR-09(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące postępowania z informacjami, do których dostęp uzyskał nieupoważniony personel; mechanizmy wspierające lub wdrażające zabezpieczenia stosowane wobec pracowników, którzy uzyskali dostęp do informacji wykraczających poza przypisane im uprawnienia dostępu]. |

| | |
|---|---|
| **IR-10** | **ZINTEGROWANY ZESPÓŁ DS. ANALIZY BEZPIECZEŃSTWA INFORMACJI** |
| | [WYCOFANE: Włączone do IR-04(11)]. |

## 4.9. KATEGORIA MA - UTRZYMANIE I WSPARCIE

| | | |
|---|---|---|
| **MA-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-01_ODP[01]** | ***określono personel lub role, którym należy przekazać politykę utrzymania;*** |
| | **MA-01_ODP[02]** | ***określono personel lub role, którym należy przekazać procedury utrzymania;*** |
| | **MA-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **MA-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami utrzymania;*** |
| | **MA-01_ODP[05]** | ***określono częstotliwość, z jaką polityka utrzymania jest przeglądana i aktualizowana;*** |
| | **MA-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji obowiązującej polityki utrzymania;*** |
| | **MA-01_ODP[07]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji obowiązujących procedur utrzymania;*** |
| | **MA-01_ODP[08]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji procedur utrzymania;*** |
| | **MA-01a.[01]** | opracowano i udokumentowano politykę utrzymania; |
| | **MA-01a.[02]** | polityka utrzymania jest rozpowszechniana wśród ***<personelu lub ról MA-01_ODP[01]>***; |
| | **MA-01a.[03]** | opracowano i udokumentowano procedury utrzymania ułatwiające wdrożenie polityki utrzymania i związane z nią środki; |

| **MA-01** | **POLITYKA I PROCEDURY** | |
|---|---|---|
| | **MA-01a.[04]** | procedury utrzymania są rozpowszechniane wśród ***<personelu lub ról MA-01_ODP[02]>***; |
| | **MA-01a.01(a)[01]** | polityka utrzymania ***<WYBRANA WARTOŚĆ PARAMETRU MA-01_ODP[03]>*** odnosi się do celu; |
| | **MA-01a.01(a)[02]** | polityka utrzymania ***<WYBRANA WARTOŚĆ PARAMETRU MA-01_ODP[03]>*** odnosi się do zakresu; |
| | **MA-01a.01(a)[03]** | polityka utrzymania ***<WYBRANA WARTOŚĆ PARAMETRU MA-01_ODP[03]>*** odnosi się do ról; |
| | **MA-01a.01(a)[04]** | polityka utrzymania ***<WYBRANA WARTOŚĆ PARAMETRU MA-01_ODP[03]>*** odnosi się do obowiązków; |
| | **MA-01a.01(a)[05]** | polityka utrzymania ***<WYBRANA WARTOŚĆ PARAMETRU MA-01_ODP[03]>*** odnosi się do zaangażowania kierownictwa; |
| | **MA-01a.01(a)[06]** | polityka utrzymania ***<WYBRANA WARTOŚĆ PARAMETRU MA-01_ODP[03]>*** odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **MA-01a.01(a)[07]** | polityka utrzymania ***<WYBRANA WARTOŚĆ PARAMETRU MA-01_ODP[03]>*** odnosi się do zgodności; |
| | **MA-01a.01(b)** | polityka utrzymania ***<WYBRANA WARTOŚĆ PARAMETRU MA-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **MA-01b.** | ***<urzędnik MA-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur utrzymania; |
| | **MA-01c.01[01]** | aktualna polityka utrzymania jest przeglądana i aktualizowana z ***<częstotliwością MA-01_ODP[05]>***; |

| | | |
|---|---|---|
| **MA-01** | **POLITYKA I PROCEDURY** | |
| | **MA-01c.01[02]** | aktualna polityka utrzymania jest przeglądana i aktualizowana po ***<zdarzeniach MA-01_ODP[06]>***; |
| | **MA-01c.02[01]** | aktualne procedury utrzymania są przeglądane i aktualizowane z ***<częstotliwością MA-01_ODP[07]>***; |
| | **MA-01c.02[02]** | aktualne procedury utrzymania są przeglądane i aktualizowane po ***<zdarzeniach MA-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury utrzymania; plan bezpieczeństwa systemu; plan ochrony prywatności; strategia zarządzania ryzykiem organizacyjnym; inne istotne dokumenty lub zapisy]. |
| | **MA-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **MA-02** | **NADZÓR NAD UTRZYMANIEM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-02_ODP[01]** | ***określono personel lub role, których wyraźne zatwierdzenie jest wymagane do przeniesienia systemu lub jego komponentów poza obiekt organizacji w celu przeprowadzenia konserwacji lub napraw poza terenem obiektu organizacji;*** |
| | **MA-02_ODP[02]** | ***określono informacje, które należy usunąć z powiązanych nośników przed przeniesieniem systemu lub komponentów poza obiekt organizacji w celu przeprowadzenia konserwacji, naprawy bądź wymiany;*** |

| MA-02 | NADZÓR NAD UTRZYMANIEM | |
|---|---|---|
| | **MA-02_ODP[03]** | ***określono informacje, które mają być zawarte w organizacyjnej dokumentacji dotyczącej konserwacji;*** |
| | **MA-02a.[01]** | konserwacja, naprawa i wymiana komponentów systemu są zaplanowane zgodnie ze specyfikacjami producenta lub sprzedawcy lub wymaganiami organizacyjnymi; |
| | **MA-02a.[02]** | konserwacja, naprawa i wymiana komponentów systemu są dokumentowane zgodnie ze specyfikacjami producenta lub sprzedawcy lub wymaganiami organizacyjnymi; |
| | **MA-02a.[03]** | zapisy dotyczące konserwacji, naprawy i wymiany komponentów systemu są poddawane przeglądowi zgodnie ze specyfikacjami producenta lub sprzedawcy lub wymogami organizacji; |
| | **MA-02b.[01]** | wszystkie czynności związane z konserwacją podlegają zatwierdzeniu, niezależnie od tego, czy są wykonywane na miejscu, czy zdalnie oraz czy system lub jego komponenty są serwisowane na miejscu, czy też są dostarczane w tym celu do innej lokalizacji; |
| | **MA-02b.[02]** | wszystkie czynności związane z konserwacją podlegają monitorowaniu, niezależnie od tego, czy są wykonywane na miejscu, czy zdalnie oraz czy system lub jego komponenty są serwisowane na miejscu, czy też są dostarczane w tym celu do innej lokalizacji; |
| | **MA-02c.** | ***<personel lub role MA-02_ODP[01]>*** musza wyraźnie zatwierdzić przeniesienie systemu lub jego komponentów z obiektów organizacji w celu przeprowadzenia konserwacji lub napraw poza jej terenem; |
| | **MA-02d.** | sprzęt jest poddawany sanityzacji w celu usunięcia ***<informacji MA-02_ODP[02]> z*** powiązanych nośników przed ich przeniesieniem z obiektów organizacji w celu przeprowadzenia konserwacji, naprawy lub wymiany poza jej terenem; |

| | | |
|---|---|---|
| **MA-02** | **NADZÓR NAD UTRZYMANIEM** | |
| | **MA-02e.** | wszystkie zabezpieczenia mające potencjalny wpływ są sprawdzane w celu zweryfikowania, czy nadal funkcjonują prawidłowo po przeprowadzeniu działań związanych z konserwacją, naprawą lub wymianą; |
| | **MA-02f.** | ***<informacje MA-02_ODP[03]>*** znajdują się w organizacyjnej dokumentacji dotyczącej utrzymania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące kontrolowanego utrzymania systemu; zapisy dotyczące utrzymania; specyfikacje utrzymania dostarczone przez producenta/dostawcę; zapisy dotyczące sanityzacji sprzętu; zapisy dotyczące sanityzacji nośników; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za sanityzację nośników; administratorzy systemu/sieci]. |
| | **MA-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące planowania, wykonywania, dokumentowania, przeglądu, zatwierdzania i monitorowania utrzymania oraz napraw systemu; procesy organizacyjne dotyczące sanityzacji elementów systemu; mechanizmy wspierające lub wdrażające kontrolowane utrzymanie; mechanizmy wdrażające sanityzację komponentów systemu]. |

| | |
|---|---|
| **MA-02(01)** | **NADZÓR NAD UTRZYMANIEM\| ZAWARTOŚĆ REKORDU** |
| | [WYCOFANE: Włączone do MA-02]. |

| | | |
|---|---|---|
| **MA-02(02)** | **NADZÓR NAD UTRZYMANIEM \| AUTOMATYCZNE DZIAŁANIA KONSERWACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-02(02)_ODP[01]** | ***określono automatyczne mechanizmy wykorzystywane do planowania działań związanych z utrzymaniem oraz naprawą i wymianą w zakresie systemu;*** |
| | **MA-02(02)_ODP[02]** | ***określono automatyczne mechanizmy wykorzystywane do przeprowadzania działań związanych z utrzymaniem oraz naprawą i wymianą w zakresie systemu;*** |
| | **MA-02(02)_ODP[03]** | ***określono automatyczne mechanizmy wykorzystywane do dokumentowania działań związanych z utrzymaniem oraz naprawą i wymianą w zakresie systemu;*** |
| | **MA-02(02)(a)[01]** | stosuje się ***<automatyczne mechanizmy MA-02(02)_ODP[01]>*** ***do*** planowania działań związanych z utrzymaniem oraz naprawą i wymianą w zakresie systemu; |
| | **MA-02(02)(a)[02]** | stosuje się ***<automatyczne mechanizmy MA-02(02)_ODP[02]>*** ***do*** przeprowadzania działań związanych z utrzymaniem oraz naprawą i wymianą w zakresie systemu; |
| | **MA-02(02)(a)[03]** | stosuje się ***<automatyczne mechanizmy MA-02(02)_ODP[03]>*** ***do*** dokumentowania działań związanych z utrzymaniem oraz naprawą i wymianą w zakresie systemu; |
| | **MA-02(02)(b)[01]** | sporządzane są aktualne, dokładne i kompletne zapisy wszystkich działań w zakresie utrzymania, o które wnioskowano, które zostały zaplanowane, które są w trakcie realizacji i które zostały zakończone. |
| | **MA-02(02)(b)[02]** | sporządzane są aktualne, dokładne i kompletne zapisy wszystkich działań w zakresie napraw, o które wnioskowano, które zostały zaplanowane, które są w trakcie realizacji i które zostały zakończone. |

| | | |
|---|---|---|
| **MA-02(02)** | **NADZÓR NAD UTRZYMANIEM \| AUTOMATYCZNE DZIAŁANIA KONSERWACYJNE** | |
| | **MA-02(02)(b)[03]** | sporządzane są aktualne, dokładne i kompletne zapisy wszystkich działań w zakresie wymiany, o które wnioskowano, które zostały zaplanowane, które są w trakcie realizacji i które zostały zakończone. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące kontrolowanego utrzymania systemu; automatyczne mechanizmy wspierające działania związane z utrzymaniem systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące utrzymania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MA-02(02)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspomagające lub wdrażające kontrolowane utrzymanie; automatyczne mechanizmy wspomagające lub wdrażające tworzenie rejestrów działań związanych z utrzymaniem oraz naprawą]. |

| | | |
|---|---|---|
| **MA-03** | **NARZĘDZIA UTRZYMANIOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-03_ODP** | ***Określono częstotliwość, z jaką należy dokonywać przeglądu wcześniej zatwierdzonych narzędzi do utrzymania systemu;*** |
| | **MA-03a.[01]** | stosowanie narzędzi do utrzymania systemu podlega zatwierdzeniu; |
| | **MA-03a.[02]** | stosowanie narzędzi do utrzymania systemu podlega kontroli; |
| | **MA-03a.[03]** | stosowanie narzędzi do utrzymania systemu podlega monitorowaniu; |

| | | |
|---|---|---|
| **MA-03** | **NARZĘDZIA UTRZYMANIOWE** | |
| | **MA-03b.** | uprzednio zatwierdzone narzędzia do utrzymania systemu są poddawane przeglądowi z ***<częstotliwością MA-03_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące narzędzi do utrzymania systemu; narzędzia do utrzymania systemu i związana z nimi dokumentacja; zapisy dotyczące utrzymania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MA-03-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zatwierdzania, kontroli i monitorowania narzędzi do utrzymania; mechanizmy wspierające lub wdrażające zatwierdzanie, kontrolę lub monitorowanie do narzędzi utrzymania]. |

| | | |
|---|---|---|
| **MA-03(01)** | **NARZĘDZIA UTRZYMANIOWE \| SPRAWDZANIE NARZĘDZI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-03(01)** | narzędzia używane przez pracowników obsługi technicznej są sprawdzane pod kątem niewłaściwych lub nieuprawnionych modyfikacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **MA-03(01)** | **NARZĘDZIA UTRZYMANIOWE \| SPRAWDZANIE NARZĘDZI** | |
| | **MA-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące narzędzi do utrzymania systemu; narzędzia do utrzymania systemu i związana z nimi dokumentacja; zapisy z inspekcji narzędzi do utrzymania; zapisy dotyczące utrzymania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MA-03(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące kontroli narzędzi do utrzymania; mechanizmy wspierające lub wdrażające kontrolę narzędzi do utrzymania]. |

| | | |
|---|---|---|
| **MA-03(02)** | **NARZĘDZIA UTRZYMANIOWE \| SPRAWDZANIE NOŚNIKÓW DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-03(02)** | nośniki zawierające programy diagnostyczne i testowe są sprawdzane pod kątem obecności złośliwego kodu, zanim nośniki te zostaną użyte w systemie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące narzędzi do utrzymania systemu; narzędzia do utrzymania systemu i związana z nimi dokumentacja; zapisy dotyczące utrzymania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **MA-03(02)** | **NARZĘDZIA UTRZYMANIOWE \| SPRAWDZANIE NOŚNIKÓW DANYCH** | |
| | **MA-03(02)-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny w zakresie sprawdzania nośników pod kątem obecności złośliwego kodu; mechanizmy wspierające lub wdrażające sprawdzanie nośników używanych do utrzymania]. |

| | | |
|---|---|---|
| **MA-03(03)** | **NARZĘDZIA UTRZYMANIOWE \| ZAPOBIEGANIE NIEAUTORYZOWANEMU USUWANIU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-03(03)_ODP** | **zdefiniowano personel lub role, które mogą wydać upoważnienie do przeniesienia sprzętu poza obiekt organizacji;** |
| | **MA-03(03)(a)** | przeniesienie sprzętu do utrzymania, który zawiera informacje organizacji, jest uniemożliwione poprzez sprawdzenie, że na sprzęcie nie ma informacji organizacyjnych; lub |
| | **MA-03(03)(b)** | przeniesienie sprzętu do utrzymania, który zawiera informacje organizacji, jest uniemożliwione poprzez sanityzację lub zniszczenie sprzętu; lub |
| | **MA-03(03)(c)** | przeniesienie sprzętu do utrzymania, który zawiera informacje organizacji, jest uniemożliwione poprzez zatrzymanie sprzętu na terenie obiektu; lub |
| | **MA-03(03)(d)** | przeniesienie sprzętu do utrzymania, który zawiera informacje organizacji, jest uniemożliwione poprzez konieczność uzyskania wyraźnej zgody ***<personelu lub ról MA-03(03)_ODP> na*** przeniesienie sprzętu poza teren obiektu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **MA-03(03)** | **NARZĘDZIA UTRZYMANIOWE \| ZAPOBIEGANIE NIEAUTORYZOWANEMU USUWANIU** | |
| | **MA-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące narzędzi do utrzymania systemu; narzędzia do utrzymania systemu i związana z nimi dokumentacja; zapisy dotyczące utrzymania; zapisy dotyczące sanityzacji sprzętu; zapisy dotyczące sanityzacji nośników; zgody dotyczące przenoszenia sprzętu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za sanityzację nośników]. |
| | **MA-03(03)-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny zapobiegający nieuprawnionemu przenoszeniu informacji; mechanizmy wspierające sanityzację nośników lub niszczenie urządzeń; mechanizmy wspierające weryfikację sanityzacji nośników]. |

| | | |
|---|---|---|
| **MA-03(04)** | **NARZĘDZIA UTRZYMANIOWE \| OGRANICZANIE UŻYWANIA NARZĘDZI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-03(04)** | narzędzi do utrzymania może używać wyłącznie upoważniony personel. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **MA-03(04)** | **NARZĘDZIA UTRZYMANIOWE \| OGRANICZANIE UŻYWANIA NARZĘDZI** | |
| | **MA-03(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące narzędzi do utrzymania systemu; narzędzia do utrzymania systemu i związana z nimi dokumentacja; lista personelu upoważnionego do używania narzędzi do utrzymania; zapisy dotyczące używania narzędzi do utrzymania; zapisy dotyczące utrzymania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-03(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MA-03(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne ograniczania stosowania narzędzi utrzymania; mechanizmy wspierające lub wdrażające ograniczenia w stosowaniu narzędzi utrzymania]. |

| | | |
|---|---|---|
| **MA-03(05)** | **NARZĘDZIA UTRZYMANIOWE \| WYKORZYSTYWANIE PODWYŻSZONYCH UPRAWNIEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-03(05)** | monitorowane jest użycie narzędzi utrzymania, które są uruchamiane z podwyższonymi uprawnieniami. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **MA-03(05)** | **NARZĘDZIA UTRZYMANIOWE \| WYKORZYSTYWANIE PODWYŻSZONYCH UPRAWNIEŃ** | |
| | **MA-03(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące narzędzi do utrzymania systemu; narzędzia do utrzymania systemu i związana z nimi dokumentacja; lista personelu upoważnionego do używania narzędzi do utrzymania; zapisy dotyczące używania narzędzi do utrzymania; zapisy dotyczące utrzymania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-03(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MA-03(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ograniczania wykorzystania narzędzi utrzymania; Proces organizacyjny dotyczący monitorowania narzędzi utrzymania i wykorzystania narzędzi utrzymania; mechanizmy monitorujące wykorzystanie narzędzi utrzymania]. |

| | | |
|---|---|---|
| **MA-03(06)** | **NARZĘDZIA UTRZYMANIOWE \| AKTUALIZACJE I POPRAWKI OPROGRAMOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-03(06)** | narzędzia do utrzymania są sprawdzane w celu zapewnienia, że zainstalowano najnowsze aktualizacje oprogramowania i poprawki. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-03(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące narzędzi do utrzymania systemu; narzędzia do utrzymania systemu i związana z nimi dokumentacja; lista personelu upoważnionego do używania narzędzi do utrzymania; zapisy dotyczące używania narzędzi do utrzymania; zapisy dotyczące utrzymania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **MA-03(06)** | **NARZĘDZIA UTRZYMANIOWE \| AKTUALIZACJE I POPRAWKI OPROGRAMOWANIA** | |
| | **MA-03(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MA-03(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące kontroli narzędzi do utrzymania; procesy organizacyjne dotyczące aktualizacji narzędzi utrzymania ruchu; mechanizmy wspierające lub wdrażające kontrolę narzędzi do utrzymania; mechanizmy wspierające lub realizujące aktualizację narzędzi do utrzymania]. |

| | | |
|---|---|---|
| **MA-04** | **UTRZYMANIE ZDALNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-04a.[01]** | zdalne czynności diagnostyczne i utrzymaniowe podlegają zatwierdzeniu; |
| | **MA-04a.[02]** | zdalne czynności diagnostyczne i utrzymaniowe podlegają monitorowaniu; |
| | **MA-04b.[01]** | korzystanie ze zdalnych narzędzi utrzymaniowych i diagnostycznych jest dozwolone tylko w sposób zgodny z polityką organizacyjną i udokumentowany w planie bezpieczeństwa systemu; |
| | **MA-04b.[02]** | stosowanie zdalnych narzędzi utrzymaniowych i diagnostycznych jest udokumentowane w planie bezpieczeństwa dla systemu; |
| | **MA-04c.** | przy nawiązywaniu zdalnych sesji utrzymania i diagnostyki stosuje się silne uwierzytelnianie; |
| | **MA-04d.** | prowadzone są zapisy dotyczące zdalnych działań utrzymaniowych i diagnostycznych; |

| | | |
|---|---|---|
| **MA-04** | **UTRZYMANIE ZDALNE** | |
| | **MA-04e.[01]** | połączenia sesyjne są kończone po zakończeniu działań dot. zdalnego utrzymania; |
| | **MA-04e.[02]** | połączenia sieciowe są przerywane po zakończeniu działań dot. zdalnego utrzymania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące zdalnego utrzymania systemu; polityka zdalnego dostępu; procedury zdalnego dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące utrzymania; zapisy dotyczące zdalnego dostępu; zapisy diagnostyczne; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MA-04-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zarządzania utrzymaniem zdalnym; mechanizmy wdrażające, wspierające lub zarządzające utrzymaniem zdalnym; mechanizmy silnego uwierzytelniania sesji diagnostycznych utrzymania zdalnego; mechanizmy kończenia sesji utrzymania zdalnego i połączeń sieciowych]. |

| | | |
|---|---|---|
| **MA-04(01)** | **UTRZYMANIE ZDALNE \| AUDYT I PRZEGLĄD** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-04(01)_ODP[01]** | ***określono zdarzenia kontrolne, które mają być rejestrowane w przypadku zdalnego utrzymania;*** |

| | | |
|---|---|---|
| **MA-04(01)** | **UTRZYMANIE ZDALNE \| AUDYT I PRZEGLĄD** | |
| | **MA-04(01)_ODP[02]** | ***określono zdarzenia kontrolne, które mają być rejestrowane dla sesji diagnostycznych;*** |
| | **MA-04(01)(a)[01]** | rejestruje się ***<zdarzenia kontrolne MA-04(01)_ODP[01]>*** dla zdalnych sesji utrzymania; |
| | **MA-04(01)(a)[02]** | rejestruje się ***<zdarzenia kontrolne MA-04(01)_ODP[02]>*** dla zdalnych sesji diagnostycznych; |
| | **MA-04(01)(b)[01]** | zapisy z audytu sesji utrzymania są przeglądane w celu wykrycia anomalii; |
| | **MA-04(01)(b)[02]** | zapisy z audytu sesji diagnostycznych są przeglądane w celu wykrycia anomalii w zachowaniu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące utrzymania systemu zdalnego; lista zdarzeń kontrolnych; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące utrzymania; zapisy diagnostyczne; zapisy z audytu; przeglądy zapisów sesji utrzymaniowych i diagnostycznych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za audyt i przegląd; administratorzy systemu/sieci]. |
| | **MA-04(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące audytu i przeglądu utrzymania zdalnego; mechanizmy wspierające lub wdrażające audyt i przegląd utrzymania zdalnego]. |

| | |
|---|---|
| **MA-04(02)** | **UTRZYMANIE ZDALNE \| DOKUMENTY ZDALNEGO UTRZYMANIA** |
| | [WYCOFANE: Włączone do MA-01, MA-04]. |

| | | |
|---|---|---|
| **MA-04(03)** | **UTRZYMANIE ZDALNE \| PORÓWNYWALNE POZIOMY BEZPIECZEŃSTWA/SANITYZACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-04(03)(a)[01]** | zdalne usługi utrzymania muszą być wykonywane za pośrednictwem systemu, w którym wdrożono funkcje bezpieczeństwa porównywalne z tymi wdrożonymi w serwisowanym systemie; |
| | **MA-04(03)(a)[02]** | zdalne usługi diagnostyczne muszą być wykonywane za pośrednictwem systemu, w którym wdrożono funkcje bezpieczeństwa porównywalne z tymi wdrożonymi w serwisowanym systemie; lub |
| | **MA-04(03)(b)[01]** | komponent, który ma być serwisowany, jest usuwany z systemu przed wykonaniem zdalnego utrzymania lub usług diagnostycznych; |
| | **MA-04(03)(b)[02]** | komponent przeznaczony do serwisowania przechodzi sanityzację (pod kątem informacji organizacyjnych); |
| | **MA-04(03)(b)[03]** | komponent jest sprawdzany i oczyszczany (pod kątem potencjalnie złośliwego oprogramowania) po wykonaniu usługi i przed ponownym podłączeniem do systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-04(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące utrzymania systemu zdalnego; umowy z dostawcami usług lub umowy o poziomie usług; zapisy dotyczące utrzymania; zapisy dotyczące inspekcji; zapisy z audytu; zapisy dotyczące sanityzacji sprzętu; zapisy dotyczące sanityzacji nośników; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **MA-04(03)** | **UTRZYMANIE ZDALNE \| PORÓWNYWALNE POZIOMY BEZPIECZEŃSTWA/SANITYZACJA** | |
| | **MA-04(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; dostawca usług utrzymania systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za sanityzację nośników danych; administratorzy systemu/sieci]. |
| | **MA-04(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące porównywalnego zabezpieczenia i sanityzacji dla utrzymania zdalnego; procesy organizacyjne dotyczące usuwania, sanityzacji i kontroli komponentów obsługiwanych przez utrzymanie zdalne; mechanizmy wspierające lub wdrażające sanityzację i kontrolę komponentów]. |

| | | |
|---|---|---|
| **MA-04(04)** | **UTRZYMANIE ZDALNE \| UWIERZYTELNIANIE/SEPARACJA SESJI UTRZYMANIOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-04(04)_ODP** | ***określono metody uwierzytelniania, które są odporne na atak metodą powtórzenia;*** |
| | **MA-04(04)(a)** | zdalne sesje utrzymania są chronione przez zastosowanie ***<metod uwierzytelniania odpornych na atak metodą powtórzenia MA-04(04)_ODP>***; |
| | **MA-04(04)(b)(01)** | zdalne sesje utrzymania są chronione poprzez ich oddzielenie od innych sesji sieciowych za pomocą fizycznie oddzielonych ścieżek komunikacyjnych; lub |
| | **MA-04(04)(b)(02)** | zdalne sesje utrzymania są chronione poprzez ich oddzielenie od innych sesji sieciowych za pomocą logicznie oddzielonych ścieżek komunikacyjnych. |

| | | |
|---|---|---|
| **MA-04(04)** | **UTRZYMANIE ZDALNE \| UWIERZYTELNIANIE/SEPARACJA SESJI UTRZYMANIOWYCH** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-04(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące zdalnego utrzymania systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące utrzymania; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-04(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; inżynierowie sieciowi; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MA-04(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ochrony sesji zdalnego utrzymania; mechanizmy wdrażające metody uwierzytelniania odporne na atak metodą powtórzenia; mechanizmy wdrażające logicznie odseparowane/szyfrowane ścieżki komunikacyjne]. |

| | | |
|---|---|---|
| **MA-04(05)** | **UTRZYMANIE ZDALNE \| ZGODY I POWIADOMIENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-04(05)_ODP[01]** | ***określono personel lub role wymagane do zatwierdzenia każdej sesji zdalnego utrzymania;*** |
| | **MA-04(05)_ODP[02]** | ***określono personel i role, które mają być powiadamiane o dacie i godzinie planowanych działań w zakresie zdalnego utrzymania;*** |
| | **MA-04(05)(a)** | wymaga się, aby każda sesja zdalnego utrzymania została zatwierdzona przez ***<personel lub role MA-04(05)_ODP[01]>***; |

| | | |
|---|---|---|
| **MA-04(05)** | **UTRZYMANIE ZDALNE \| ZGODY I POWIADOMIENIA** | |
| | **MA-04(05)(b)** | ***<personel i role MA-04(05)_ODP[02]>*** otrzymują powiadomienie o dacie i godzinie planowanych sesji zdalnego utrzymania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-04(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące zdalnego utrzymania systemu; powiadomienia wspierające sesje zdalnego utrzymania; zapisy dotyczące utrzymania; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-04(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za powiadamianie; personel organizacyjny odpowiedzialny za zatwierdzanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MA-04(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zatwierdzania i powiadamiania personelu w zakresie utrzymania zdalnego; mechanizmy wspierające powiadamianie i zatwierdzanie w zakresie utrzymania zdalnego]. |

| | | |
|---|---|---|
| **MA-04(06)** | **UTRZYMANIE ZDALNE \| OCHRONA KRYPTOGRAFICZNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-04(06)_ODP** | ***określono mechanizmy kryptograficzne, które należy wdrożyć w celu ochrony integralności i poufności komunikacji w zakresie zdalnego utrzymania i diagnostyki;*** |
| | **MA-04(06)[01]** | wdrożono ***<mechanizmy kryptograficzne MA-04(06)_ODP>*** w celu ochrony integralności komunikacji w zakresie zdalnego utrzymania i diagnostyki; |

| | | |
|---|---|---|
| **MA-04(06)** | **UTRZYMANIE ZDALNE \| OCHRONA KRYPTOGRAFICZNA** | |
| | **MA-04(06)[02]** | wdrożono ***<mechanizmy kryptograficzne MA-04(06)_ODP>*** w celu ochrony poufności komunikacji w zakresie zdalnego utrzymania i diagnostyki; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-04(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące zdalnego utrzymania systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; mechanizmy kryptograficzne zabezpieczające zdalne działania związane z utrzymaniem systemu;<br>zapisy dotyczące utrzymania; dokumentacja diagnostyczna; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-04(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; inżynierowie sieciowi; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MA-04(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne chroniące zdalne utrzymanie i komunikację diagnostyczną]. |

| | | |
|---|---|---|
| **MA-04(07)** | **UTRZYMANIE ZDALNE \| ZDALNA WERYFIKACJA ZAKOŃCZENIA SESJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-04(07)[01]** | weryfikuje się, czy zakończono połączenie sesyjne po zakończeniu sesji zdalnego utrzymania i sesji diagnostycznych; |
| | **MA-04(07)[02]** | weryfikuje się, czy zakończono połączenie sieciowe po zakończeniu sesji zdalnego utrzymania i sesji diagnostycznych; |

| | | |
|---|---|---|
| **MA-04(07)** | **UTRZYMANIE ZDALNE \| ZDALNA WERYFIKACJA ZAKOŃCZENIA SESJI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-04(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące zdalnego utrzymania systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dzienniki zakończenia sesji/połączenia sieciowego; mechanizmy kryptograficzne chroniące zdalne utrzymanie; zapisy dotyczące utrzymania; dokumentacja diagnostyczna; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-04(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; inżynierowie sieciowi; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MA-04(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające weryfikację rozłączenia zakończonych sesji zdalnego utrzymania i sesji diagnostycznych]. |

| | | |
|---|---|---|
| **MA-05** | **PERSONEL UTRZYMANIOWY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-05a.[01]** | ustanowiony jest proces autoryzacji personelu utrzymania; |
| | **MA-05a.[02]** | prowadzony jest wykaz autoryzowanych organizacji lub personelu zajmującego się utrzymaniem; |
| | **MA-05b.** | personel realizujący utrzymanie systemu bez nadzoru posiada wymagane uprawnienia dostępu; |

| | | |
|---|---|---|
| **MA-05** | **PERSONEL UTRZYMANIOWY** | |
| | **MA-05c.** | personel organizacyjny z wymaganymi uprawnieniami dostępu i kompetencjami technicznymi jest wyznaczony do nadzorowania czynności utrzymania ruchu realizowanych przez personel nieposiadający wymaganych uprawnień dostępu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące personelu utrzymania; umowy z dostawcami usług; umowy o poziomie usług; lista upoważnionego personelu; zapisy dotyczące utrzymania; zapisy kontroli dostępu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MA-05-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące autoryzacji i zarządzania personelem utrzymania; mechanizmy wspierające lub wdrażające autoryzację personelu utrzymania]. |

| | | |
|---|---|---|
| **MA-05(01)** | **PERSONEL UTRZYMANIOWY \| OSOBY NIEPOSIADAJĄCE STOSOWNYCH PRAW DOSTĘPU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-05(01)_ODP** | ***określono alternatywne zabezpieczenia, które należy opracować i wdrożyć, jeżeli komponentu systemu nie można poddać sanityzacji, usunąć lub odłączyć od systemu;*** |

| | | |
|---|---|---|
| **MA-05(01)** | **PERSONEL UTRZYMANIOWY \| OSOBY NIEPOSIADAJĄCE STOSOWNYCH PRAW DOSTĘPU** | |
| | **MA-05(01)(a)(01)** | wdrożono procedury zapewniające, że personel utrzymania, który nie posiada niezbędnych uprawnień dostępu lub polskiego obywatelstwa, jest eskortowany i nadzorowany podczas wykonywania czynności serwisowych i diagnostycznych w systemie przez zatwierdzony personel organizacyjny, który posiada poświadczenia bezpieczeństwa, odpowiednie zezwolenia na dostęp oraz kwalifikacje techniczne; |
| | **MA-05(01)(a)(02)** | wdrożono procedury zapewniające, że przed rozpoczęciem czynności utrzymaniowych lub diagnostycznych przez personel nieposiadający uprawnień dostępu, poświadczeń bezpieczeństwa lub formalnych zezwoleń na dostęp, wszystkie komponenty systemu przechowujące informacje w pamięci ulotnej są czyszczone, a wszystkie nieulotne nośniki pamięci są usuwane lub fizycznie odłączane od systemu i zabezpieczane; |
| | **MA-05(01)(b)** | opracowano i wdrożono ***<alternatywne zabezpieczenia MA-05(01)_ODP>***, stosowane w przypadku gdy komponent nie może zostać wyczyszczony, usunięty lub odłączony od systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-05(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące personelu utrzymania; polityka ochrony systemowych nośników danych; polityka ochrony fizycznej i środowiskowej; lista personelu utrzymania wymagającego eskorty/nadzoru; zapisy dotyczące utrzymania; zapisy dotyczące kontroli dostępu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-05(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo personelu; personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za sanityzację nośników; administratorzy systemu/sieci]. |

| | | |
|---|---|---|
| **MA-05(01)** | **PERSONEL UTRZYMANIOWY \| OSOBY NIEPOSIADAJĄCE STOSOWNYCH PRAW DOSTĘPU** | |
| | **MA-05(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zarządzania personelem utrzymania nieposiadającym odpowiednich upoważnień; mechanizmy wspierające lub wdrażające alternatywne zabezpieczenia; mechanizmy wspierające lub wdrażające sanityzację komponentów do przechowywania informacji]. |

| | | |
|---|---|---|
| **MA-05(02)** | **PERSONEL UTRZYMANIOWY \| POŚWIADCZENIA BEZPIECZEŃSTWA/SYSTEMY NIEJAWNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-05(02)[01]** | personel wykonujący czynności związane z utrzymaniem i diagnostyką systemu przetwarzającego, przechowującego lub przekazującego informacje niejawne posiada odpowiednie poświadczenia bezpieczeństwa co najmniej do najwyższego poziomu klasyfikacji informacji i przedziałów informacji w systemie; |
| | **MA-05(02)[02]** | personel wykonujący czynności związane z utrzymaniem i diagnostyką systemu przetwarzającego, przechowującego lub przesyłającego informacje niejawne posiada formalne zezwolenia na dostęp do informacji, które są odpowiednie co najmniej do najwyższego poziomu klasyfikacji informacji i przedziałów informacji w systemie |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-05(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące personelu utrzymania; akta osobowe; zapisy dotyczące utrzymania; zapisy dotyczące kontroli dostępu; poświadczenia dostępu; upoważnienia dostępu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **MA-05(02)** | **PERSONEL UTRZYMANIOWY \| POŚWIADCZENIA BEZPIECZEŃSTWA/SYSTEMY NIEJAWNE** | |
| | **MA-05(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo personelu; personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MA-05(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zarządzania poświadczeniami bezpieczeństwa dla personelu utrzymania ruchu]. |

| | | |
|---|---|---|
| **MA-05(03)** | **PERSONEL UTRZYMANIOWY \| OBYWATELSTWO/SYSTEMY NIEJAWNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-05(03)** | personel wykonujący czynności związane z utrzymaniem i diagnostyką systemu przetwarzającego, przechowującego lub przekazującego informacje posiada polskie obywatelstwo. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-05(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące personelu utrzymania; akta osobowe; zapisy dotyczące utrzymania; zapisy dotyczące kontroli dostępu; poświadczenia dostępu; upoważnienia dostępu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-05(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo personelu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **MA-05(04)** | **PERSONEL UTRZYMANIOWY \| CUDZOZIEMCY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-05(04)(a)** | obcokrajowcy posiadający odpowiednie poświadczenia bezpieczeństwa są wykorzystywani do prowadzenia działań związanych z utrzymaniem i diagnostyką systemów niejawnych tylko wtedy, gdy systemy te stanowią wspólną własność i są eksploatowane przez Polskę i zagraniczne rządy sojusznicze lub są eksploatowane wyłącznie przez zagraniczne rządy sojusznicze i stanowią ich wyłączną własność; |
| | **MA-05(04)(b)[01]** | zezwolenia dotyczące wykorzystania cudzoziemców do prowadzenia działań związanych z utrzymaniem i diagnostyką systemów niejawnych są w pełni udokumentowane w protokołach ustaleń; |
| | **MA-05(04)(b)[02]** | zgody dotyczące wykorzystania cudzoziemców do prowadzenia działań związanych z utrzymaniem i diagnostyką systemów niejawnych są w pełni udokumentowane w protokołach ustaleń; |
| | **MA-05(04)(b)[03]** | szczegółowe warunki operacyjne dotyczące wykorzystywania cudzoziemców do prowadzenia działań związanych z utrzymaniem i diagnostyką systemów niejawnych są w pełni udokumentowane w protokołach ustaleń. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-05(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące personelu utrzymania; polityka ochrony nośników systemowych; polityka i procedury kontroli dostępu; polityka i procedury ochrony fizycznej i środowiskowej; protokół ustaleń; zapisy dotyczące utrzymania; zapisy dotyczące kontroli dostępu; dane uwierzytelniające dostęp; upoważnienia do dostępu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **MA-05(04)** | **PERSONEL UTRZYMANIOWY \| CUDZOZIEMCY** | |
| | **MA-05(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu, personel organizacyjny odpowiedzialny za bezpieczeństwo personelu; personel organizacyjny zarządzający protokołami ustaleń; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MA-05(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zarządzania pracownikami utrzymania posiadającymi obywatelstwo innego kraju]. |

| | | |
|---|---|---|
| **MA-05(05)** | **PERSONEL UTRZYMANIOWY \| OBSŁUGA NIEZWIĄZANA Z UTRZYMANIEM SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-05(05)** | personel wykonujący bez nadzoru czynności związane z utrzymaniem, które nie są bezpośrednio związane z systemem, ale są realizowane w fizycznej bliskości systemu, posiada wymagane uprawnienia dostępu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-05(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące personelu utrzymania; polityka ochrony nośników systemowych; polityka i procedury kontroli dostępu; polityka i procedury ochrony fizycznej i środowiskowej; zapisy dotyczące utrzymania; zapisy dotyczące kontroli dostępu; upoważnienia do dostępu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-05(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo personelu; personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **MA-06** | **TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-06_ODP[01]** | ***określono komponenty systemu, dla których uzyskuje się wsparcie w zakresie utrzymania lub części zamienne;*** |
| | **MA-06_ODP[02]** | **określono okres, w którym należy uzyskać wsparcie w zakresie utrzymania lub części zamienne po wystąpieniu awarii;** |
| | **MA-06** | wsparcie w zakresie utrzymania lub części zamienne dla ***<komponentów systemu MA-06_ODP[01]>*** uzyskuje się w ciągu ***<okresu MA-06_ODP[02]>*** od wystąpienia awarii. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące utrzymania systemu; umowy z dostawcami usług; umowy o poziomie usług; lista i informacje o dostępności części zamiennych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MA-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zapewniające terminową realizację prac utrzymaniowych]. |

| | | |
|---|---|---|
| **MA-06(01)** | **TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI \| KONSERWACJA ZAPOBIEGAWCZA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-06(01)_ODP[01]** | ***określono komponenty systemu, które mają być objęte konserwacją zapobiegawczą;*** |
| | **MA-06(01)_ODP[02]** | ***określono przedziały czasowe, w których należy przeprowadzić konserwację zapobiegawczą komponentów systemu;*** |
| | **MA-06(01)** | konserwację zapobiegawczą przeprowadza się na ***<komponentach systemu MA-06(01)_ODP[01]>*** w ***<odstępach czasu MA-06(01)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-06(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące utrzymania systemu; umowy z dostawcami usług; umowy o poziomie usług; dokumentacja dotycząca utrzymania; lista komponentów systemu wymagających konserwacji zapobiegawczej; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-06(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MA-06(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie konserwacji zapobiegawczej; mechanizmy wspierające lub wdrażające konserwację zapobiegawczą]. |

| MA-06(02) | TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI \| KONSERWACJA PLANOWA | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-06(02)_ODP[01]** | ***określono komponenty systemu, na których ma być przeprowadzona konserwacja planowa;*** |
| | **MA-06(02)_ODP[02]** | ***określono przedziały czasowe, w których należy przeprowadzić planową konserwację komponentów systemu;*** |
| | **MA-06(02)** | planową konserwację wykonuje się na ***<komponentach systemu MA-06(02)_ODP[01]>*** w ***<odstępach czasu MA-06(02)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-06(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące utrzymania systemu; umowy z dostawcami usług; umowy o poziomie usług; zapisy dotyczące utrzymania; lista komponentów systemu wymagających konserwacji planowej; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-06(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MA-06(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie konserwacji planowej; mechanizmy wspierające lub wdrażające konserwację planową]. |

| | | |
|---|---|---|
| **MA-06(03)** | **TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI \| AUTOMATYCZNE WSPARCIE W ZAKRESIE KONSERWACJI PLANOWEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-06(03)_ODP** | ***określono automatyczne mechanizmy wykorzystywane do przekazywania danych dotyczących konserwacji planowej do systemu zarządzania utrzymaniem;*** |
| | **MA-06(03)** | dane dotyczące konserwacji planowej są przekazywane do systemu zarządzania utrzymaniem z wykorzystaniem ***<automatycznych mechanizmów MA-06(03)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-06(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące utrzymania systemu; umowy z dostawcami usług; umowy o poziomie usług; zapisy dotyczące utrzymania; lista komponentów systemu wymagających konserwacji planowej; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-06(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MA-06(03)-Test** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące utrzymania systemu; umowy z dostawcami usług; umowy o poziomie usług; dokumentacja dotycząca utrzymania; lista komponentów systemu wymagających konserwacji planowej; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **MA-07** | **KONSERWACJA W TERENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MA-07_ODP[01]** | ***określono systemy lub komponenty systemu, w przypadku których konserwację w terenie można przeprowadzać wyłącznie w zaufanych obiektach obsługi technicznej;*** |
| | **MA-07_ODP[02]** | ***określono zaufane obiekty obsługi technicznej, które nie są objęte ograniczeniami ani zakazami co do prowadzenia konserwacji w terenie;*** |
| | **MA-07** | konserwację w terenie na ***<systemach lub komponentach systemu MA-07_ODP[01]>*** można realizować wyłącznie w ***<MA-07_ODP[02] zaufanych obiektach obsługi technicznej>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MA-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka utrzymania; procedury dotyczące konserwacji w terenie; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące utrzymania; zapisy diagnostyczne; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MA-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za utrzymanie systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MA-07-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zarządzania konserwacją w terenie; mechanizmy wdrażające, wspierające lub zarządzające konserwacją w terenie; mechanizmy silnego uwierzytelniania sesji diagnostycznych związanych z konserwacją w terenie; mechanizmy kończenia sesji i połączeń sieciowych związanych z konserwacją w terenie]. |

## 4.10. KATEGORIA MP - OCHRONA NOŚNIKÓW DANYCH

| | | |
|---|---|---|
| **MP-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-01_ODP[01]** | ***określono personel lub role, wśród których ma być rozpowszechniana polityka ochrony nośników danych;*** |
| | **MP-01_ODP[02]** | ***określono personel lub role, wśród których mają być rozpowszechniane procedury ochrony nośników danych;*** |
| | **MP-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **MP-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami ochrony nośników danych;*** |
| | **MP-01_ODP[05]** | ***określono częstotliwość, z jaką polityka ochrony nośników danych jest przeglądana i aktualizowana;*** |
| | **MP-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji obowiązującej polityki ochrony nośników danych;*** |
| | **MP-01_ODP[07]** | ***określono częstotliwość, z jaką aktualne procedury ochrony nośników danych są przeglądane i aktualizowane;*** |
| | **MP-01_ODP[08]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji obowiązujących procedur ochrony nośników danych;*** |
| | **MP-01a.[01]** | opracowano i udokumentowano politykę ochrony nośników danych; |
| | **MP-01a.[02]** | polityka ochrony nośników danych jest rozpowszechniana wśród ***<personelu lub ról MP-01_ODP[01]>***; |
| | **MP-01a.[03]** | opracowano i udokumentowano procedury ochrony nośników danych ułatwiające wdrożenie polityki ochrony nośników danych i związanych z nią zabezpieczeń dotyczących ochrony nośników danych; |

| MP-01 | POLITYKA I PROCEDURY | |
|---|---|---|
| | **MP-01a.[04]** | procedury ochrony nośników danych są rozpowszechniane wśród ***<personelu lub ról MP-01_ODP[02]>***; |
| | **MP-01a.01(a)[01]** | polityka ochrony nośników danych ***<WYBRANA WARTOŚĆ PARAMETRU MP-01_ODP[03]>***odnosi się do celu; |
| | **MP-01a.01(a)[02]** | polityka ochrony nośników danych ***<WYBRANA WARTOŚĆ PARAMETRU MP-01_ODP[03]>***odnosi się do zakresu; |
| | **MP-01a.01(a)[03]** | polityka ochrony nośników danych ***<WYBRANA WARTOŚĆ PARAMETRU MP-01_ODP[03]>***odnosi się do ról; |
| | **MP-01a.01(a)[04]** | polityka ochrony nośników danych ***<WYBRANA WARTOŚĆ PARAMETRU MP-01_ODP[03]>***odnosi się do obowiązków; |
| | **MP-01a.01(a)[05]** | polityka ochrony nośników danych ***<WYBRANA WARTOŚĆ PARAMETRU MP-01_ODP[03]>***odnosi się do zaangażowania kierownictwa; |
| | **MP-01a.01(a)[06]** | polityka ochrony nośników danych ***<WYBRANA WARTOŚĆ PARAMETRU MP-01_ODP[03]>***odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **MP-01a.01(a)[07]** | polityka ochrony nośników danych ***<WYBRANA WARTOŚĆ PARAMETRU MP-01_ODP[03]>***odnosi się do zgodności; |
| | **MP-01a.01(b)** | polityka ochrony nośników danych jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **MP-01b.** | ***<urzędnik MP-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur ochrony nośników danych; |
| | **MP-01c.01[01]** | aktualna polityka ochrony nośników danych jest przeglądana i aktualizowana z ***<częstotliwością MP-01_ODP[05]>***; |

| | | |
|---|---|---|
| **MP-01** | **POLITYKA I PROCEDURY** | |
| | **MP-01c.01[02]** | aktualna polityka ochrony nośników danych jest przeglądana i aktualizowana po ***<zdarzeniach MP-01_ODP[06]>***; |
| | **MP-01c.02[01]** | przeglądu i aktualizacji procedur ochrony nośników danych dokonuje się z ***<częstotliwością MP-01_ODP[07]>***; |
| | **MP-01c.02[02]** | przeglądu i aktualizacji procedur ochrony nośników danych dokonuje się po ***<zdarzeniach MP-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury ochrony nośników danych; strategia zarządzania ryzykiem organizacyjnym; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **MP-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **MP-02** | **DOSTĘP DO NOŚNIKÓW DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-02_ODP[01]** | ***określono rodzaje nośników cyfrowych, do których dostęp jest ograniczony;*** |
| | **MP-02_ODP[02]** | ***określono personel lub role upoważnione do dostępu do nośników cyfrowych;*** |
| | **MP-02_ODP[03]** | ***określono rodzaje nośników niecyfrowych, do których dostęp jest ograniczony;*** |
| | **MP-02_ODP[04]** | ***określono personel lub role upoważnione do dostępu do nośników niecyfrowych;*** |

| | | |
|---|---|---|
| **MP-02** | **DOSTĘP DO NOŚNIKÓW DANYCH** | |
| | **MP-02[01]** | dostęp do ***<rodzajów nośników cyfrowych MP-02_ODP[01]>*** jest ograniczony do<br>***<personelu lub ról MP-02_ODP[02]>***; |
| | **MP-02[02]** | dostęp do ***<rodzajów nośników niecyfrowych MP-02_ODP[03]>*** jest ograniczony do<br>***<personelu lub ról MP-02_ODP[04]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony nośników danych w systemie; procedury dotyczące ograniczeń dostępu do nośników; polityka i procedury kontroli dostępu;<br>polityka i procedury dotyczące ochrony fizycznej i środowiskowej; urządzenia do przechowywania nośników danych; zapisy dotyczące kontroli dostępu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę nośników danych w systemie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MP-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ograniczeń dotyczących nośników z informacjami; mechanizmy wspierające lub wdrażające ograniczenia dostępu do nośników]. |

| | |
|---|---|
| **MP-02(01)** | **DOSTĘP DO NOŚNIKÓW DANYCH\| OGRANICZONY DOSTĘP AUTOMATYCZNY** |
| | [WYCOFANE: Włączone do MP-04(02)]. |

| | |
|---|---|
| **MP-02(02)** | **DOSTĘP DO NOŚNIKÓW DANYCH \| OCHRONA KRYPTOGRAFICZNA** |
| | [WYCOFANE: Włączone do SC-28(01)]. |

| | | |
|---|---|---|
| **MP-03** | **OZNAKOWANIE NOŚNIKÓW DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-03_ODP[01]** | ***określono rodzaje nośników systemowych zwolnionych z obowiązku znakowania, jeżeli pozostają w obszarze kontrolowanym;*** |
| | **MP-03_ODP[02]** | ***określono obszary kontrolowane, w których nośniki nie podlegają obowiązkowi znakowania;*** |
| | **MP-03a.** | nośniki systemowe są znakowane w celu wskazania ograniczeń w dystrybucji przechowywanych na nich informacji, a także zastrzeżeń dotyczących postępowania z takimi informacjami oraz związanych z nimi oznaczeń bezpieczeństwa (jeśli dotyczy); |
| | **MP-03b.** | ***<rodzaje nośników zwolnione z obowiązku znakowania MP-03_ODP[01]>*** pozostają w ***<obszarach kontrolowanych MP-03_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony nośników danych systemowych; procedury dotyczące znakowania nośników; polityka i procedury ochrony fizycznej i środowiskowej; lista atrybutów bezpieczeństwa dotyczących znakowania nośników systemowych; wyznaczone obszary kontrolowane; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę i znakowanie systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **MP-03** | **OZNAKOWANIE NOŚNIKÓW DANYCH** | |
| | **MP-03-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące znakowania nośników zawierających informacje; mechanizmy wspierające lub wdrażające znakowanie nośników]. |

| | | |
|---|---|---|
| **MP-04** | **PRZECHOWYWANIE NOŚNIKÓW DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-04_ODP[01]** | ***określono rodzaje cyfrowych nośników danych, które mają być fizycznie kontrolowane (jeśli wybrano);*** |
| | **MP-04_ODP[02]** | ***określono rodzaje niecyfrowych nośników danych, które mają być fizycznie kontrolowane (jeśli wybrano);*** |
| | **MP-04_ODP[03]** | ***określono rodzaje cyfrowych nośników danych, które mają być bezpiecznie przechowywane (jeśli wybrano);*** |
| | **MP-04_ODP[04]** | ***określono rodzaje niecyfrowych nośników danych, które mają być bezpiecznie przechowywane (jeśli wybrano);*** |
| | **MP-04_ODP[05]** | ***określono kontrolowane obszary, w których można bezpiecznie przechowywać cyfrowe nośniki danych;*** |
| | **MP-04_ODP[06]** | ***określono kontrolowane obszary, w których można bezpiecznie przechowywać niecyfrowe nośniki danych;*** |
| | **MP-04a.[01]** | ***<rodzaje nośników cyfrowych MP-04_ODP[01]>*** są fizycznie kontrolowane; |
| | **MP-04a.[02]** | ***<rodzaje nośników niecyfrowych MP-04_ODP[02]>*** są fizycznie kontrolowane; |
| | **MP-04a.[03]** | ***<rodzaje nośników cyfrowych MP-04_ODP[03]>*** są bezpiecznie przechowywane w ***<obszarach kontrolowanych MP-04_ODP[05]>***; |

| | | |
|---|---|---|
| **MP-04** | **PRZECHOWYWANIE NOŚNIKÓW DANYCH** | |
| | **MP-04a.[04]** | ***<rodzaje nośników cyfrowych MP-04_ODP[04]>*** są bezpiecznie przechowywane w ***<obszarach kontrolowanych MP-04_ODP[06]>***; |
| | **MP-04b.** | rodzaje nośników danych systemowych (określone w MP-04_ODP[01], MP-04_ODP[02], MP-04_ODP[03], MP-04_ODP[04]) są chronione do czasu zniszczenia lub sanityzacji takich nośników przy użyciu zatwierdzonych urządzeń, technik i procedur. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące przechowywania nośników; polityka i procedury ochrony fizycznej i środowiskowej; polityka i procedury kontroli dostępu; systemowe nośniki danych; wyznaczone obszary kontrolowane; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę i przechowywanie systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MP-04-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przechowywania nośników danych; mechanizmy wspierające lub wdrażające bezpieczne przechowywanie/ochronę nośników danych]. |

| | |
|---|---|
| **MP-04(01)** | **PRZECHOWYWANIE NOŚNIKÓW DANYCH \| OCHRONA KRYPTOGRAFICZNA** |
| | [WYCOFANE: Włączone do SC-28(01)]. |

| | | |
|---|---|---|
| **MP-04(02)** | **PRZECHOWYWANIE NOŚNIKÓW DANYCH \| OGRANICZONY DOSTĘP AUTOMATYCZNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-04(02)_ODP[01]** | ***określono automatyczne mechanizmy ograniczania dostępu do nośników danych;*** |
| | **MP-04(02)_ODP[02]** | ***określono automatyczne mechanizmy rejestrowania prób dostępu do obszarów przechowywania nośników danych;*** |
| | **MP-04(02)_ODP[03]** | ***określono automatyczne mechanizmy rejestrowania przyznanego dostępu do obszarów przechowywania nośników danych;*** |
| | **MP-04(02)[01]** | dostęp do obszarów przechowywania nośników danych jest ograniczony przy użyciu ***<automatycznych mechanizmów MP-04(02)_ODP[01]>***; |
| | **MP-04(02)[02]** | próby dostępu do obszarów przechowywania nośników danych są rejestrowane przy użyciu ***<automatycznych mechanizmów MP-04(02)_ODP[02]>***; |
| | **MP-04(02)[03]** | przyznany dostęp do obszarów przechowywania nośników danych jest rejestrowany przy użyciu ***<automatycznych mechanizmów MP-04(02)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-04(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące przechowywania nośników; polityka i procedury kontroli dostępu; polityka i procedury ochrony fizycznej i środowiskowej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; obiekty do przechowywania nośników; urządzenia kontroli dostępu; zapisy dotyczące kontroli dostępu; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **MP-04(02)** | **PRZECHOWYWANIE NOŚNIKÓW DANYCH \| OGRANICZONY DOSTĘP AUTOMATYCZNY** | |
| | **MP-04(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę i przechowywanie systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MP-04(02)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy ograniczające dostęp do obszarów przechowywania nośników danych; automatyczne mechanizmy kontrolujące próby dostępu oraz przyznany dostęp do obszarów przechowywania nośników danych]. |

| | | |
|---|---|---|
| **MP-05** | **TRANSPORT NOŚNIKÓW DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-05_ODP[01]** | ***określono rodzaje systemowych nośników danych, które wymagają ochrony i kontroli przy przenoszeniu poza obszary kontrolowane;*** |
| | **MP-05_ODP[02]** | ***określono zabezpieczenia stosowane do ochrony systemowych nośników danych poza obszarami kontrolowanymi;*** |
| | **MP-05_ODP[03]** | ***określono zabezpieczenia stosowane do zabezpieczania systemowych nośników danych poza obszarami kontrolowanymi;*** |
| | **MP-05a.[01]** | ***<rodzaje systemowych nośników danych MP-05_ODP[01]>*** są chronione przy przenoszeniu poza obszary kontrolowane za pomocą ***<zabezpieczeń MP-05_ODP[02]>***; |
| | **MP-05a.[02]** | ***<rodzaje systemowych nośników danych MP-05_ODP[01]>*** są zabezpieczane przy przenoszeniu poza obszary kontrolowane za pomocą ***<zabezpieczeń MP-05_ODP[03]>***; |

| | | |
|---|---|---|
| **MP-05** | **TRANSPORT NOŚNIKÓW DANYCH** | |
| | **MP-05b.** | zachowana jest rozliczalność w zakresie systemowych nośników danych przy przenoszeniu ich poza obszary kontrolowane; |
| | **MP-05c.** | dokumentuje się czynności związane z przenoszeniem systemowych nośników danych; |
| | **MP-05d.[01]** | określono personel upoważniony do prowadzenia działań w zakresie przenoszenia nośników danych; |
| | **MP-05d.[02]** | czynności związane z przenoszeniem systemowych nośników danych wykonuje jedynie określony, upoważniony personel; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące przechowywania nośników; polityka i procedury ochrony fizycznej i środowiskowej; polityka i procedury kontroli dostępu; lista upoważnionego personelu; systemowe nośniki danych; wyznaczone obszary kontrolowane; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę i przechowywanie systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MP-05-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne przechowywania nośników zawierających informacje; mechanizmy wspierające lub wdrażające przechowywanie/ochronę nośników danych]. |

| | |
|---|---|
| **MP-05(01)** | **TRANSPORT NOŚNIKÓW DANYCH \| OCHRONA POZA OBSZARAMI KONTROLOWANYMI** |
| | [WYCOFANE: Włączone do MP-05]. |

| MP-05(02) | TRANSPORT NOŚNIKÓW DANYCH \| DOKUMENTACJA DZIAŁAŃ | |
|---|---|---|
| | [WYCOFANE: Włączone do MP-05]. | |

| MP-05(03) | TRANSPORT NOŚNIKÓW DANYCH \| KONWOJENCI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-05(03)[01]** | wskazano konwojenta nadzorującego przeniesienie nośników danych poza obszar kontrolowany; |
| | **MP-05(03)[02]** | wskazany konwojent nadzoruje przeniesienie nośników danych poza obszar kontrolowany; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-05(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące transportu nośników; polityka i procedury ochrony fizycznej i środowiskowej; zapisy dotyczące transportu systemowych nośników danych; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-05(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przenoszenie nośników systemowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji. |
| | **MP-05(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne związane z wyznaczeniem i wykorzystaniem konwojenta do realizacji transportu nośników danych poza obszar kontrolowany]. |

| MP-05(04) | TRANSPORT NOŚNIKÓW DANYCH \| OCHRONA KRYPTOGRAFICZNA | |
|---|---|---|
| | [WYCOFANE: Włączone do SC-28(01)]. | |

| | | |
|---|---|---|
| **MP-06** | **SANITYZACJA NOŚNIKÓW DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-06_ODP[01]** | ***określono systemowe nośniki danych, które należy poddać sanityzacji przed utylizacją;*** |
| | **MP-06_ODP[02]** | ***określono systemowe nośniki danych, które należy poddać sanityzacji, zanim organizacja zakończy stosowanie wobec nich swoich zabezpieczeń;*** |
| | **MP-06_ODP[03]** | ***określono systemowe nośniki danych, które należy poddać sanityzacji przed dopuszczeniem nośnika do ponownego wykorzystania;*** |
| | **MP-06_ODP[04]** | ***określono techniki i procedury sanityzacji, które należy stosować przed utylizacją nośników danych;*** |
| | **MP-06_ODP[05]** | ***określono techniki i procedury sanityzacji, które należy zastosować zanim organizacja zakończy stosowanie wobec nośników danych swoich zabezpieczeń;*** |
| | **MP-06_ODP[06]** | ***określono techniki i procedury sanityzacji, które należy zastosować przed dopuszczeniem nośnika do ponownego użycia;*** |
| | **MP-06a.[01]** | ***<nośniki systemowe MP-06_ODP[01]>*** przechodzą sanityzację przy użyciu ***<procedur i technik sanityzacji MP-06_ODP[04]>*** przed utylizacją; |
| | **MP-06a.[02]** | ***<nośniki systemowe MP-06_ODP[02]>*** przechodzą sanityzację przy użyciu ***<procedur i technik sanityzacji MP-06_ODP[05]>*** zanim organizacja zakończy stosowanie wobec nich swoich zabezpieczeń; |
| | **MP-06a.[03]** | ***<nośniki systemowe MP-06_ODP[03]>*** przechodzą sanityzację przy użyciu ***<procedur i technik sanityzacji MP-06_ODP[06]>*** przed dopuszczeniem do ponownego użycia; |
| | **MP-06b.** | stosuje się mechanizmy sanityzacji o sile i integralności proporcjonalnej do kategorii bezpieczeństwa lub klasyfikacji informacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **MP-06** | **SANITYZACJA NOŚNIKÓW DANYCH** | |
|---|---|---|
| | **MP-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące sanityzacji i utylizacji nośników danych; obowiązujące normy i polityki krajowe dotyczące polityki sanityzacji nośników danych; zapisy dotyczące sanityzacji nośników danych; zapisy z audytu systemu; dokumentacja projektowa systemu; polityka przechowywania i utylizacji zapisów;<br>zapisy dotyczące procedury przechowywania i utylizacji dokumentacji; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **MP-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sanityzację nośników danych; personel organizacyjny odpowiedzialny za przechowywanie i utylizację dokumentacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci]. |
| | **MP-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące sanityzacji nośników danych; mechanizmy wspierające lub wdrażające sanityzację nośników danych]. |

| **MP-06(01)** | **SANITYZACJA NOŚNIKÓW DANYCH \| PRZEGLĄD/ZATWIERDZANIE/ŚLEDZENIE/DOKUMENTOWANIE/ WERYFIKACJA** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-06(01)[01]** | działania związane z sanityzacją i utylizacją nośników danych podlegają przeglądowi; |
| | **MP-06(01)[02]** | działania związane z sanityzacją i utylizacją nośników danych podlegają zatwierdzeniu; |

| | | |
|---|---|---|
| **MP-06(01)** | **SANITYZACJA NOŚNIKÓW DANYCH \| PRZEGLĄD/ZATWIERDZANIE/ŚLEDZENIE/DOKUMENTOWANIE/ WERYFIKACJA** | |
| | **MP-06(01)[03]** | działania związane z sanityzacją i utylizacją nośników danych podlegają śledzeniu; |
| | **MP-06(01)[04]** | działania związane z sanityzacją i utylizacją nośników danych podlegają dokumentowaniu; |
| | **MP-06(01)[05]** | działania związane z sanityzacją i utylizacją nośników danych podlegają weryfikacji; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-06(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące sanityzacji i utylizacji nośników danych; polityka przechowywania i utylizacji zapisów; procedury przechowywania i utylizacji zapisów; zapisy dotyczące sanityzacji i utylizacji nośników danych; zapisy dotyczące przeglądu działań związanych z sanityzacją i utylizacją nośników danych; zatwierdzenia działań związanych z sanityzacją i utylizacją nośników danych; zapisy dotyczące śledzenia; zapisy dotyczące weryfikacji; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **MP-06(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sanityzację i utylizację systemowych nośników danych; personel organizacyjny odpowiedzialny za przechowywanie i utylizację dokumentacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci]. |
| | **MP-06(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące sanityzacji nośników danych; mechanizmy wspierające lub wdrażające sanityzację nośników danych; mechanizmy wspierające lub wdrażające weryfikację sanityzacji nośników danych]. |

| | | |
|---|---|---|
| **MP-06(02)** | **SANITYZACJA NOŚNIKÓW DANYCH \| TESTOWANIE SPRZĘTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-06(02)_ODP[01]** | ***określono częstotliwość, z jaką należy testować urządzenia do sanityzacji;*** |
| | **MP-06(02)_ODP[02]** | ***określono częstotliwość, z jaką należy testować procedury sanityzacji;*** |
| | **MP-06(02)[01]** | urządzenia do sanityzacji są testowane z ***<częstotliwością MP-06(02)_ODP[01]>***, aby zapewnić, że sanityzacja przynosi zamierzone efekty; |
| | **MP-06(02)[02]** | procedury sanityzacji są testowane z ***<częstotliwością MP-06(02)_ODP[02]>***, zapewnić, że sanityzacja przynosi zamierzone efekty. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-06(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące sanityzacji i utylizacji nośników danych; procedury dotyczące testowania urządzeń do sanityzacji nośników danych; wyniki testowania urządzeń i procedur do sanityzacji nośników danych; zapisy z audytu systemu; polityka przechowywania i zarządzania dokumentacją; procedury przechowywania i zarządzania dokumentacją; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **MP-06(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sanityzację systemowych nośników danych; personel organizacyjny odpowiedzialny za przechowywanie i utylizację dokumentacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **MP-06(02)** | **SANITYZACJA NOŚNIKÓW DANYCH \| TESTOWANIE SPRZĘTU** | |
| | **MP-06(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące sanityzacji nośników danych; automatyczne mechanizmy wspierające lub wdrażające sanityzację nośników danych; automatyczne mechanizmy wspierające lub wdrażające procedury sanityzacji nośników danych; urządzenia do sanityzacji nośników danych]. |

| | | |
|---|---|---|
| **MP-06(03)** | **SANITYZACJA NOŚNIKÓW DANYCH \| TECHNIKI NIEDESTRUKCYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-06(03)_ODP** | ***określono okoliczności wymagające sanityzacji przenośnych urządzeń pamięci masowej;*** |
| | **MP-06(03)** | niedestrukcyjne techniki sanityzacji są stosowane do przenośnych urządzeń pamięci masowej przed podłączeniem takich urządzeń do systemu w ***<okolicznościach MP-06(03)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-06(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące sanityzacji i utylizacji nośników; informacje o przenośnych nośnikach danych dla systemu; lista okoliczności wymagających sanityzacji przenośnych urządzeń pamięci masowej; zapisy dotyczące sanityzacji nośników; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-06(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sanityzację systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MP-06(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące sanityzacji przenośnych urządzeń pamięci masowej; mechanizmy wspierające lub realizujące sanityzację nośników danych]. |

| **MP-06(04)** | **SANITYZACJA NOŚNIKÓW DANYCH \| KONTROLOWANE INFORMACJE JAWNE** |
|---|---|
| | [WYCOFANE: Włączone do MP-06]. |

| **MP-06(05)** | **SANITYZACJA NOŚNIKÓW DANYCH \| INFORMACJE NIEJAWNE** |
|---|---|
| | [WYCOFANE: Włączone do MP-06]. |

| **MP-06(06)** | **SANITYZACJA NOŚNIKÓW DANYCH \| NISZCZENIE NOŚNIKÓW DANYCH** |
|---|---|
| | [WYCOFANE: Włączone do MP-06]. |

| **MP-06(07)** | **SANITYZACJA NOŚNIKÓW DANYCH \| PODWÓJNA AUTORYZACJA** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-06(07)_ODP** | ***określono systemowe nośniki danych, których sanityzacja wymaga podwójnej autoryzacji;*** |
| | **MP-06(07)** | egzekwuje się stosowanie podwójnej autoryzacji przy sanityzacji ***<systemowych nośników danych MP-06(07)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-06(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące sanityzacji i utylizacji nośników danych; polityka i procedury podwójnej autoryzacji; lista systemowych nośników danych, których sanityzacja wymaga podwójnej autoryzacji; zapisy dotyczące autoryzacji; zapisy dotyczące sanityzacji nośników danych; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **MP-06(07)** | **SANITYZACJA NOŚNIKÓW DANYCH \| PODWÓJNA AUTORYZACJA** | |
| | **MP-06(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sanityzację systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MP-06(07)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne wymagające podwójnej autoryzacji do sanityzacji nośników danych; mechanizmy wspierające lub wdrażające sanityzację nośników danych; mechanizmy wspierające lub wdrażające podwójną autoryzację]. |

| | | |
|---|---|---|
| **MP-06(08)** | **SANITYZACJA NOŚNIKÓW DANYCH \| ZDALNE KASOWANIE/WYMAZYWANIE INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-06(08)_ODP[01]** | ***określono systemy lub komponenty systemu umożliwiające kasowanie lub wymazywanie informacji na odległość lub w określonych warunkach;*** |
| | **MP-06(08)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {zdalnie;***<br>***<w warunkach MP-06(08)_ODP[03]>};*** |
| | **MP-06(08)_ODP[03]** | ***określono warunki, w jakich informacje mają być kasowane lub wymazywane (jeśli wybrano);*** |
| | **MP-06(08)** | zapewniono możliwość kasowania lub wymazywania informacji z ***<systemów lub komponentów systemu MP-06(08)_ODP[01]>*** ***<WYBRANA WARTOŚĆ PARAMETRU MP-06(08)_ODP[02]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **MP-06(08)** | **SANITYZACJA NOŚNIKÓW DANYCH \| ZDALNE KASOWANIE/WYMAZYWANIE INFORMACJI** | |
| | **MP-06(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące sanityzacji i utylizacji nośników danych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące autoryzacji; zapisy dotyczące sanityzacji nośników danych; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-06(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sanityzację systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MP-06(08)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za sanityzację systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |

| | | |
|---|---|---|
| **MP-07** | **UŻYWANIE NOŚNIKÓW DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-07_ODP[01]** | ***określono rodzaje systemowych nośników danych, których stosowanie w systemach lub komponentach systemu jest ograniczone lub zabronione;*** |
| | **MP-07_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {ograniczone; zabronione};*** |
| | **MP-07_ODP[03]** | ***określono systemy lub komponenty systemu, w których korzystanie z wyznaczonych rodzajów systemowych nośników danych jest ograniczone lub zabronione;*** |

| | | |
|---|---|---|
| **MP-07** | **UŻYWANIE NOŚNIKÓW DANYCH** | |
| | **MP-07_ODP[04]** | ***określono zabezpieczenia ograniczające lub zakazujące stosowania określonych rodzajów systemowych nośników danych w systemach lub komponentach systemu;*** |
| | **MP-07a.** | stosowanie ***<rodzajów systemowych nośników danych MP-07_ODP[01]>*** jest ***<WYBRANA WARTOŚĆ PARAMETRU MP-07_ODP[02]>*** w ***<systemach lub komponentach systemu MP-07_ODP[03]>*** z wykorzystaniem ***<zabezpieczeń MP-07_ODP[04]>***; |
| | **MP-07b.** | używanie przenośnych urządzeń pamięci masowej w systemach organizacji jest zabronione, jeśli urządzenia te nie mają określonego właściciela. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; polityka użytkowania systemu; procedury dotyczące ograniczeń w korzystaniu z nośników; zasady postępowania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za korzystanie z systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MP-07-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące korzystania z nośników danych; mechanizmy ograniczające lub zakazujące korzystania z systemowych nośników danych w systemach lub komponentach systemu]. |

| | |
|---|---|
| **MP-07(01)** | **UŻYWANIE NOŚNIKÓW DANYCH \| ZABRONIONE WYKORZYSTANIE NIEZIDENTYFIKOWANEJ WŁASNOŚCI** |
| | [WYCOFANE: Włączone do MP-07]. |

| | | |
|---|---|---|
| **MP-07(02)** | **UŻYWANIE NOŚNIKÓW DANYCH \| ZABRONIONE WYKORZYSTANIE MEDIÓW ODPORNYCH NA SANITYZACJĘ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-07(02)[01]** | określono nośniki danych odporne na sanityzację; |
| | **MP-07(02)[02]** | zabrania się stosowania w systemach organizacyjnych nośników danych odpornych na sanityzację. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-07(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; polityka użytkowania systemu; procedury dotyczące ograniczeń w korzystaniu z nośników danych; zasady postępowania; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-07(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za korzystanie z systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MP-07(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące korzystania z nośników danych; mechanizmy zakazujące korzystania z nośników danych w systemach lub komponentach systemu]. |

| | | |
|---|---|---|
| **MP-08** | **DEKLASYFIKACJA NOŚNIKÓW DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-08_ODP[01]** | ***określono proces obniżania klasyfikacji systemowych nośników danych;*** |
| | **MP-08_ODP[02]** | ***określono systemowe nośniki danych wymagające obniżania klasyfikacji;*** |
| | **MP-08a.[01]** | ***ustanowiono <proces obniżania klasyfikacji systemowych nośników danych MP-08_ODP[01]>;*** |
| | **MP-08a.[02]** | ***proces obniżania klasyfikacji systemowych nośników danych MP-08_ODP[01]>*** obejmuje zastosowanie mechanizmów obniżania klasyfikacji o sile i integralności współmiernej do kategorii bezpieczeństwa lub klasyfikacji informacji; |
| | **MP-08b.[01]** | weryfikuje się, czy proces obniżania klasyfikacji nośników systemowych jest współmierny do kategorii bezpieczeństwa lub poziomu klasyfikacji informacji, które mają zostać usunięte; |
| | **MP-08b.[02]** | weryfikuje się, czy proces obniżania klasyfikacji nośników danych jest współmierny do uprawnień dostępu potencjalnych odbiorców informacji o obniżonej klasyfikacji; |
| | **MP-08c.** | określono ***<systemowe nośniki danych wymagające obniżania klasyfikacji MP-08_ODP[02]>;*** |
| | **MP-08d.** | klasyfikacja zidentyfikowanych nośników danych jest obniżana przy użyciu procesu ***<obniżania klasyfikacji nośników systemowych MP-08_ODP[01]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **MP-08** | **DEKLASYFIKACJA NOŚNIKÓW DANYCH** | |
| | **MP-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące obniżania klasyfikacji; dokumentacja dotycząca kategoryzacji systemu; lista nośników wymagających obniżania klasyfikacji; zapisy dotyczące obniżania klasyfikacji; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obniżanie klasyfikacji systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MP-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące obniżania klasyfikacji nośników danych; mechanizmy wspierające lub wdrażające obniżanie klasyfikacji]. |

| | | |
|---|---|---|
| **MP-08(01)** | **DEKLASYFIKACJA NOŚNIKÓW DANYCH \| DOKUMENTACJA PROCESU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-08(01)** | dokumentuje się działania związane z obniżaniem klasyfikacji systemowych nośników danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **MP-08(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące obniżania klasyfikacji; dokumentacja dotycząca kategoryzacji systemu; lista nośników wymagających obniżania klasyfikacji; zapisy dotyczące obniżania klasyfikacji; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **MP-08(01)** | **DEKLASYFIKACJA NOŚNIKÓW DANYCH \| DOKUMENTACJA PROCESU** | |
| | **MP-08(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obniżanie klasyfikacji systemowych nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MP-08(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące obniżania klasyfikacji nośników danych; mechanizmy wspierające lub wdrażające obniżanie klasyfikacji]. |

| | | |
|---|---|---|
| **MP-08(02)** | **DEKLASYFIKACJA NOŚNIKÓW DANYCH \| TESTOWANIE SPRZĘTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-08(02)_ODP[01]** | ***określono częstotliwość, z jaką należy badać sprzęt do obniżania klasyfikacji danych;*** |
| | **MP-08(02)_ODP[02]** | **określono częstotliwość, z jaką należy testować procedury obniżania klasyfikacji danych;** |
| | **MP-08(02)[01]** | sprzęt do obniżania klasyfikacji danych jest testowany z ***<częstotliwością MP-08(02)_ODP[01]>*** w celu zapewnienia, że działania związane z obniżaniem klasyfikacji danych są realizowane; |
| | **MP-08(02)[02]** | procedury obniżania klasyfikacji danych są testowane z ***<częstotliwością MP-08(02)_ODP[01]>*** w celu zapewnienia, że działania związane z obniżaniem klasyfikacji danych są realizowane; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| MP-08(02) | DEKLASYFIKACJA NOŚNIKÓW DANYCH \| TESTOWANIE SPRZĘTU | |
|---|---|---|
| | **MP-08(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; procedury dotyczące obniżania klasyfikacji; procedury dotyczące testowania sprzętu do obniżania klasyfikacji; wyniki testowania sprzętu i procedur obniżających klasyfikację; zapisy dotyczące obniżania klasyfikacji; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-08(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obniżanie klasyfikacji nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MP-08(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące obniżania klasyfikacji nośników danych; mechanizmy wspierające lub wdrażające obniżanie klasyfikacji]. |

| MP-08(03) | DEKLASYFIKACJA NOŚNIKÓW DANYCH \| KONTROLOWANE INFORMACJE JAWNE | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-08(03)[01]** | określono systemowe nośniki danych zawierające kontrolowane informacje jawne; |
| | **MP-08(03)[02]** | klasyfikacja systemowych nośników danych zawierających kontrolowane informacje jawne jest obniżana przed ich publicznym ujawnieniem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| MP-08(03) | DEKLASYFIKACJA NOŚNIKÓW DANYCH \| KONTROLOWANE INFORMACJE JAWNE | |
|---|---|---|
| | **MP-08(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; polityka autoryzacji dostępu; procedury dotyczące obniżania klasyfikacji nośników danych zawierających KIJ; obowiązujące krajowe i organizacyjne standardy i polityki dotyczące ochrony KIJ; zapisy dotyczące obniżania klasyfikacji nośników; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-08(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obniżanie klasyfikacji nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MP-08(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące obniżania klasyfikacji nośników danych; mechanizmy wspierające lub wdrażające obniżanie klasyfikacji]. |

| MP-08(04) | DEKLASYFIKACJA NOŚNIKÓW DANYCH \| INFORMACJE NIEJAWNE | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **MP-08(04)[01]** | określono systemowe nośniki danych zawierające informacje niejawne; |
| | **MP-08(04)[02]** | systemowe nośniki danych zawierające informacje niejawne poddawane są obniżeniu klasyfikacji przed wydaniem osobom nieposiadającym wymaganych uprawnień dostępu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| MP-08(04) | DEKLASYFIKACJA NOŚNIKÓW DANYCH \| INFORMACJE NIEJAWNE | |
|---|---|---|
| | **MP-08(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemowych nośników danych; polityka upoważniania do dostępu; procedury dotyczące obniżania klasyfikacji nośników danych zawierających informacje niejawne; procedury dotyczące postępowania z informacjami niejawnymi; normy i polityki krajowej władzy bezpieczeństwa dotyczące ochrony informacji niejawnych; dokumentacja dotycząca obniżania klasyfikacji nośników danych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **MP-08(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za obniżanie klasyfikacji nośników danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **MP-08(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące obniżania klasyfikacji nośników danych; mechanizmy wspierające lub wdrażające obniżanie klasyfikacji]. |

## 4.11. KATEGORIA PE - OCHRONA FIZYCZNA I ŚRODOWISKOWA

| | | |
|---|---|---|
| **PE-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-01_ODP[01]** | ***określono personel lub role, wśród których ma być rozpowszechniana polityka ochrony fizycznej i środowiskowej;*** |
| | **PE-01_ODP[02]** | ***określono personel lub role, wśród których mają być rozpowszechniane procedury ochrony fizycznej i środowiskowej;*** |
| | **PE-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **PE-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami ochrony fizycznej i środowiskowej;*** |
| | **PE-01_ODP[05]** | ***określono częstotliwość, z jaką polityka ochrony fizycznej i środowiskowej jest przeglądana i aktualizowana;*** |
| | **PE-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji polityki ochrony fizycznej i środowiskowej;*** |
| | **PE-01_ODP[07]** | ***określono częstotliwość przeglądu i aktualizacji procedur ochrony fizycznej i środowiskowej;*** |
| | **PE-01_ODP[08]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji procedur ochrony fizycznej i środowiskowej;*** |
| | **PE-01a.[01]** | opracowano i udokumentowano politykę ochrony fizycznej i środowiskowej; |
| | **PE-01a.[02]** | polityka ochrony fizycznej i środowiskowej jest rozpowszechniana wśród ***<personelu lub ról PE-01_ODP[01]>***; |

| **PE-01** | **POLITYKA I PROCEDURY** | |
|---|---|---|
| | **PE-01a.[03]** | opracowano i udokumentowano procedury ochrony fizycznej i środowiskowej ułatwiające realizację polityki ochrony fizycznej i środowiskowej oraz związane z nią zabezpieczenia w zakresie ochrony fizycznej i środowiskowej; |
| | **PE-01a.[04]** | procedury ochrony fizycznej i środowiskowej są rozpowszechniane wśród ***<personelu lub ról PE-01_ODP[02]>***; |
| | **PE-01a.01(a)[01]** | polityka ochrony fizycznej i środowiskowej ***<WYBRANA WARTOŚĆ PARAMETRU PE-01_ODP[03]>*** odnosi się do celu; |
| | **PE-01a.01(a)[02]** | polityka ochrony fizycznej i środowiskowej ***<WYBRANA WARTOŚĆ PARAMETRU PE-01_ODP[03]>*** odnosi się do zakresu; |
| | **PE-01a.01(a)[03]** | polityka ochrony fizycznej i środowiskowej ***<WYBRANA WARTOŚĆ PARAMETRU PE-01_ODP[03]>*** odnosi się do ról; |
| | **PE-01a.01(a)[04]** | polityka ochrony fizycznej i środowiskowej ***<WYBRANA WARTOŚĆ PARAMETRU PE-01_ODP[03]>*** odnosi się do obowiązków; |
| | **PE-01a.01(a)[05]** | polityka ochrony fizycznej i środowiskowej ***<WYBRANA WARTOŚĆ PARAMETRU PE-01_ODP[03]>*** odnosi się do zaangażowania kierownictwa; |
| | **PE-01a.01(a)[06]** | polityka ochrony fizycznej i środowiskowej ***<WYBRANA WARTOŚĆ PARAMETRU PE-01_ODP[03]>*** odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **PE-01a.01(a)[07]** | polityka ochrony fizycznej i środowiskowej ***<WYBRANA WARTOŚĆ PARAMETRU PE-01_ODP[03]>*** odnosi się do zgodności; |
| | **PE-01a.01(b)** | polityka ochrony fizycznej i środowiskowej ***<WYBRANA WARTOŚĆ PARAMETRU PE-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |

| | | |
|---|---|---|
| **PE-01** | **POLITYKA I PROCEDURY** | |
| | **PE-01b.** | ***<urzędnik PE-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur ochrony fizycznej i środowiskowej; |
| | **PE-01c.01[01]** | polityka ochrony fizycznej i środowiskowej jest przeglądana i aktualizowana z ***<częstotliwością PE-01_ODP[05]>***; |
| | **PE-01c.01[02]** | polityka ochrony fizycznej i środowiskowej jest przeglądana i aktualizowana po ***<zdarzeniach PE-01_ODP[06]>***; |
| | **PE-01c.02[01]** | procedury ochrony fizycznej i środowiskowej są przeglądane i aktualizowane z ***<częstotliwością PE-01_ODP[07]>***; |
| | **PE-01c.02[02]** | procedury ochrony fizycznej i środowiskowej są przeglądane i aktualizowane po***<zdarzeniach PE-01_ODP[08]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury ochrony fizycznej i środowiskowej; plan bezpieczeństwa systemu; plan ochrony prywatności; strategia zarządzania ryzykiem organizacyjnym; inne istotne dokumenty lub zapisy]. |
| | **PE-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę fizyczną i środowiskową; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PE-02** | **ZEZWOLENIA NA DOSTĘP FIZYCZNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-02_ODP** | ***określono częstotliwość, z jaką należy dokonywać przeglądu listy osób upoważnionych do dostępu do obiektu, w którym znajduje się system;*** |

| | | |
|---|---|---|
| **PE-02** | **ZEZWOLENIA NA DOSTĘP FIZYCZNY** | |
| | **PE-02a.[01]** | opracowano listę osób upoważnionych do dostępu do obiektu, w którym znajduje się system; |
| | **PE-02a.[02]** | zatwierdzono listę osób upoważnionych do dostępu do obiektu, w którym znajduje się system; |
| | **PE-02a.[03]** | prowadzi się listę osób upoważnionych do dostępu do obiektu, w którym znajduje się system; |
| | **PE-02b.** | w celu uzyskania dostępu do obiektu wydawane są upoważnienia; |
| | **PE-02c.** | dokonuje się przeglądu listy osób upoważnionych do dostępu do obiektu, w którym znajduje się system;<br>***<częstotliwość PE-02_ODP>***; |
| | **PE-02d.** | osoby są usuwane z listy, gdy nie potrzebują już dostępu do obiektu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące uprawnień do dostępu fizycznego; lista osób upoważnionych do dostępu; poświadczenia uprawnień; przeglądy listy osób upoważnionych do dostępu fizycznego; zapisy dotyczące wycofania upoważnienia do dostępu fizycznego i związana z tym dokumentacja; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zatwierdzanie dostępu fizycznego; personel organizacyjny odpowiedzialny za kontrolę fizycznego dostępu do obiektu zawierającego systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące upoważnień do dostępu fizycznego; mechanizmy wspierające lub wdrażające upoważnienia do dostępu fizycznego]. |

| | | |
|---|---|---|
| **PE-02(01)** | **ZEZWOLENIA NA DOSTĘP FIZYCZNY \| DOSTĘP ZGODNIE Z POSIADANYM STANOWISKIEM/ROLĄ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-02(01)** | uprawnienia do fizycznego dostępu do obiektu, w którym znajduje się system, przyznaje się zgodnie ze stanowiskiem lub rolą danej osoby. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-02(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące uprawnień do dostępu fizycznego; dzienniki lub zapisy dotyczące kontroli dostępu fizycznego; lista stanowisk/ról i odpowiadających im uprawnień do dostępu fizycznego; punkty wejścia i wyjścia z systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-02(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zatwierdzanie dostępu fizycznego; personel organizacyjny odpowiedzialny za kontrolę fizycznego dostępu do obiektu zawierającego systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-02(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące upoważnień do dostępu fizycznego; mechanizmy wspierające lub wdrażające upoważnienia do dostępu fizycznego]. |

| | | |
|---|---|---|
| **PE-02(02)** | **ZEZWOLENIA NA DOSTĘP FIZYCZNY \| PODWÓJNA IDENTYFIKACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-02(02)_ODP** | ***określono listę akceptowalnych form identyfikacji osób odwiedzających obiekt, w którym znajduje się system;*** |

| | | |
|---|---|---|
| **PE-02(02)** | **ZEZWOLENIA NA DOSTĘP FIZYCZNY \| PODWÓJNA IDENTYFIKACJA** | |
| | **PE-02(02)** | wymagane są dwie formy identyfikacji, wpisane na listę ***<akceptowalnych form identyfikacji PE-02(02)_ODP>*** osób odwiedzających obiekt, w którym znajduje się system. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące upoważnień do dostępu fizycznego; lista akceptowalnych form identyfikacji osób odwiedzających obiekt, w którym znajduje się system; formularze zezwoleń na dostęp; dane uwierzytelniające; dzienniki lub zapisy dotyczące kontroli dostępu fizycznego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zatwierdzanie dostępu fizycznego; personel organizacyjny odpowiedzialny za kontrolę fizycznego dostępu do obiektu zawierającego systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-02(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące upoważnień do dostępu fizycznego; mechanizmy wspierające lub wdrażające upoważnienia do dostępu fizycznego]. |

| | | |
|---|---|---|
| **PE-02(03)** | **ZEZWOLENIA NA DOSTĘP FIZYCZNY \| OGRANICZANIE DOSTĘPU BEZ ASYSTY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-02(03)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {poświadczenia bezpieczeństwa dotyczące wszystkich informacji zawartych w systemie; formalne uprawnienia dostępu dotyczące wszystkich informacji zawartych w systemie; uzasadniona potrzeba dostępu do wszystkich informacji zawartych w systemie; <upoważnienia do dostępu fizycznego PE-02(03)_ODP[02]>};*** |

| **PE-02(03)** | **ZEZWOLENIA NA DOSTĘP FIZYCZNY \| OGRANICZANIE DOSTĘPU BEZ ASYSTY** | |
|---|---|---|
| | **PE-02(03)_ODP[02]** | ***określono upoważnienia do dostępu fizycznego bez asysty do obiektu, w którym znajduje się system (jeśli wybrano);*** |
| | **PE-02(03)** | Dostęp bez asysty do obiektu, w którym znajduje się system, jest ograniczony do personelu z **<WYBRANA WARTOŚĆ PARAMETRU PE-02(03)_ODP[01]>.** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-02(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące upoważnień do dostępu fizycznego; lista upoważnionego personelu; poświadczenia bezpieczeństwa; upoważnienia do dostępu; poświadczenia dostępu; dzienniki lub zapisy dotyczące kontroli dostępu fizycznego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-02(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zatwierdzanie dostępu fizycznego; personel organizacyjny odpowiedzialny za kontrolę fizycznego dostępu do obiektu zawierającego systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-02(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące upoważnień do dostępu fizycznego; mechanizmy wspierające lub wdrażające upoważnienia do dostępu fizycznego]. |

| **PE-03** | **KONTROLA DOSTĘPU FIZYCZNEGO** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-03_ODP[01]** | ***określono punkty wejścia i wyjścia do obiektu, w którym znajduje się system;*** |

| **PE-03** | **KONTROLA DOSTĘPU FIZYCZNEGO** | |
|---|---|---|
| | **PE-03_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {<systemy lub urządzenia PE-03_ODP[03]>; ochrona};*** |
| | **PE-03_ODP[03]** | ***określono systemy lub urządzenia kontroli dostępu fizycznego stosowane do zabezpieczenia wejścia i wyjścia z obiektu (jeśli wybrano);*** |
| | **PE-03_ODP[04]** | ***określono punkty wejścia lub wyjścia, dla których prowadzi się dzienniki dostępu fizycznego;*** |
| | **PE-03_ODP[05]** | ***określono środki kontroli dostępu fizycznego używane w celu zabezpieczenia obszarów w obrębie obiektu wyznaczonych jako publicznie dostępne;*** |
| | **PE-03_ODP[06]** | ***określono okoliczności wymagające eskorty odwiedzających i kontroli ich aktywności;*** |
| | **PE-03_ODP[07]** | ***określono urządzenia kontroli dostępu fizycznego, które należy poddawać inwentaryzacji;*** |
| | **PE-03_ODP[08]** | ***określono częstotliwość, z jaką należy poddawać inwentaryzacji urządzenia kontroli dostępu fizycznego;*** |
| | **PE-03_ODP[09]** | ***określono częstotliwość zmiany kombinacji zamków szyfrowych;*** |
| | **PE-03_ODP[10]** | ***określono częstotliwość zmiany kluczy;*** |
| | **PE-03a.01** | uprawnienia dostępu fizycznego są egzekwowane w ***<punktach wejścia i wyjścia PE-03_ODP[01]>*** poprzez weryfikację indywidualnych uprawnień przed udzieleniem dostępu do obiektu; |
| | **PE-03a.02** | uprawnienia dostępu fizycznego są egzekwowane w ***<punktach wejścia i wyjścia PE-03_ODP[01]>*** poprzez kontrolę wejścia i wyjścia do obiektu za pomocą ***<WYBRANA WARTOŚĆ PARAMETRU PE-03_ODP[02]>*** |
| | **PE-03b.** | prowadzi się dzienniki kontroli dostępu fizycznego dla ***<punktów wejścia lub wyjścia PE-03_ODP[04]>***; |

| | | |
|---|---|---|
| **PE-03** | **KONTROLA DOSTĘPU FIZYCZNEGO** | |
| | **PE-03c.** | dostęp do obszarów w obiekcie wyznaczonych jako publicznie dostępne jest zabezpieczany poprzez wdrożenie ***<kontroli dostępu fizycznego PE-03_ODP[05]>***; |
| | **PE-03d.[01]** | odwiedzający poruszają się w asyście; |
| | **PE-03d.[02]** | aktywność odwiedzających jest monitorowana w ***<okolicznościach PE-03_ODP[06]>***; |
| | **PE-03e.[01]** | klucze są zabezpieczone; |
| | **PE-03e.[02]** | kombinacje są zabezpieczane; |
| | **PE-03e.[03]** | inne urządzenia kontroli dostępu fizycznego są zabezpieczone; |
| | **PE-03f.** | ***<urządzenia kontroli dostępu fizycznego PE-03_ODP[07]>*** są poddawane inwentaryzacji z***<częstotliwością PE-03_ODP[08]>***; |
| | **PE-03g.[01]** | kombinacje są zmieniane z ***<częstotliwością PE-03_ODP[09]>***, a także wówczas, gdy doszło do ich naruszenia lub gdy osoby będące w ich posiadaniu są przenoszone lub kończą pracę; |
| | **PE-03g.[02]** | klucze są zmieniane z ***<częstotliwością PE-03_ODP[10]>***, a także wówczas, gdy zostaną zgubione lub gdy osoby będące w ich posiadaniu są przenoszone lub kończą pracę; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **PE-03** | **KONTROLA DOSTĘPU FIZYCZNEGO** | |
|---|---|---|
| | **PE-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli dostępu fizycznego; dzienniki lub zapisy dotyczące kontroli dostępu fizycznego; rejestry inwentaryzacyjne urządzeń kontroli dostępu fizycznego; punkty wejścia i wyjścia z systemu; zapisy dotyczące zmian kombinacji zamków oraz kluczy; miejsca przechowywania urządzeń kontroli dostępu fizycznego; urządzenia kontroli dostępu fizycznego; lista zabezpieczeń kontrolujących dostęp do wyznaczonych publicznie dostępnych obszarów w obrębie obiektu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-03-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące kontroli dostępu fizycznego; mechanizmy wspierające lub wdrażające kontrolę dostępu fizycznego; urządzenia do kontroli dostępu fizycznego]. |

| **PE-03(01)** | **KONTROLA DOSTĘPU FIZYCZNEGO \| DOSTĘP DO SYSTEMU** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-03(01)_ODP** | ***określono fizyczne przestrzenie zawierające jeden lub więcej komponentów systemu;*** |
| | **PE-03(01)[01]** | egzekwowane są uprawnienia do fizycznego dostępu do systemu; |
| | **PE-03(01)02]** | w obiekcie, w ***<przestrzeniach fizycznych PE-03(01)_ODP>***, egzekwuje się stosowanie kontroli dostępu fizycznego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **PE-03(01)** | **KONTROLA DOSTĘPU FIZYCZNEGO \| DOSTĘP DO SYSTEMU** | |
|---|---|---|
| | **PE-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli dostępu fizycznego; dzienniki lub zapisy dotyczące kontroli dostępu fizycznego; urządzenia kontroli dostępu fizycznego; upoważnienia do dostępu; dane uwierzytelniające;<br>punkty wejścia i wyjścia z systemu; lista obszarów w obrębie obiektu zawierających koncentracje komponentów systemu lub komponenty wymagające dodatkowej ochrony fizycznej; plan ochrony systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za upoważnienia do dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-03(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące kontroli dostępu fizycznego do systemu informatycznego/ komponentów; mechanizmy wspierające lub wdrażające kontrolę dostępu fizycznego do obszarów obiektu zawierających komponenty systemu]. |

| **PE-03(02)** | **KONTROLA DOSTĘPU FIZYCZNEGO \| OBIEKT/OBSZAR SYSTEMU** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-03(02)_ODP** | ***określono częstotliwość, z jaką należy przeprowadzać kontrole bezpieczeństwa dotyczące dostępu do fizycznej strefy obiektu lub do systemu informatycznego w celu uniemożliwienia nieautoryzowanego upublicznienia informacji lub usunięcia komponentów systemu;*** |
| | **PE-03(02)** | przeprowadza się kontrole bezpieczeństwa z ***<częstotliwością PE-03(02)_ODP>*** dotyczące dostępu do fizycznej strefy obiektu lub systemu, pod kątem nieautoryzowanego upublicznienia informacji lub usunięcia komponentów systemu. |

| | | |
|---|---|---|
| **PE-03(02)** | **KONTROLA DOSTĘPU FIZYCZNEGO \| OBIEKT/OBSZAR SYSTEMU** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli dostępu fizycznego; dzienniki lub zapisy dotyczące kontroli dostępu fizycznego; zapisy dotyczące kontroli bezpieczeństwa; zapisy z audytów bezpieczeństwa; sprawozdania z inspekcji bezpieczeństwa; dokumentacja rozmieszczenia obiektów; punkty wejścia i wyjścia z systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-03(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące kontroli dostępu fizycznego do obiektu lub systemu; mechanizmy wspierające lub wdrażające kontrolę dostępu fizycznego do obiektu lub systemu; mechanizmy wspierające lub wdrażające kontrole bezpieczeństwa w zakresie nieautoryzowanego upublicznienia informacji]. |

| | | |
|---|---|---|
| **PE-03(03)** | **KONTROLA DOSTĘPU FIZYCZNEGO \|CIĄGŁOŚĆ OCHRONY FIZYCZNEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-03(03)_ODP** | ***określono punkty dostępu fizycznego do obiektu, w którym znajduje się system;*** |
| | **PE-03(03)** | do kontroli ***<punktów dostępu fizycznego PE-03(03)_ODP> do*** obiektu, w którym znajduje się system, zatrudniona jest ochrona pracująca 24 godziny na dobę, 7 dni w tygodniu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **PE-03(03)** | **KONTROLA DOSTĘPU FIZYCZNEGO \|CIĄGŁOŚĆ OCHRONY FIZYCZNEJ** | |
|---|---|---|
| | **PE-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli dostępu fizycznego; dzienniki lub zapisy dotyczące kontroli dostępu fizycznego; urządzenia kontroli dostępu fizycznego; zapisy dotyczące nadzoru nad obiektem; dokumentacja dotycząca układu obiektu; punkty wejścia i wyjścia z systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-03(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące kontroli dostępu fizycznego do obiektu, w którym znajduje się system; mechanizmy wspierające lub wdrażające kontrolę dostępu fizycznego do obiektu, w którym znajduje się system]. |

| **PE-03(04)** | **KONTROLA DOSTĘPU FIZYCZNEGO \| ZAMYKANE OBUDOWY** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-03(04)_ODP** | ***określono komponenty systemu, które mają być chronione przed nieuprawnionym dostępem fizycznym;*** |
| | **PE-03(04)** | stosuje się zamykane, fizyczne obudowy do ochrony ***<komponentów systemu PE-03(04)_ODP>*** przed dostępem osób nieupoważnionych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-03(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli dostępu fizycznego; lista komponentów systemu wymagających ochrony poprzez zastosowanie zamykanych, fizycznych obudów; zamykane, fizyczne obudowy; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| **PE-03(04)** | **KONTROLA DOSTĘPU FIZYCZNEGO \| ZAMYKANE OBUDOWY** | |
|---|---|---|
| | **PE-03(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-03(04)-Test** | [WYBÓR SPOŚRÓD: Zamykane, fizyczne obudowy]. |

| **PE-03(05)** | **KONTROLA DOSTĘPU FIZYCZNEGO \| OCHRONA PRZED MANIPULACJĄ** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-03(05)_ODP[01]** | ***określono technologie zabezpieczania przed manipulacją, które należy zastosować;*** |
| | **PE-03(05)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {wykrywanie; zapobieganie};*** |
| | **PE-03(05)_ODP[03]** | ***określono komponenty sprzętowe, które mają być chronione przed fizyczną manipulacją lub zmianą;*** |
| | **PE-03(05)** | stosuje się ***<technologie zabezpieczania przed manipulacją PE-03(05)_ODP[01]>*** w celu ***<WYBRANA WARTOŚĆ PARAMETRU PE-03(05)_ODP[02]>*** fizycznej manipulacji lub zmiany ***<PE-03(05)_ODP[03] komponentów sprzętowych>*** w systemie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-03(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli dostępu fizycznego; lista zabezpieczeń służących wykrywaniu/zapobieganiu fizycznej manipulacji lub zmianie komponentów sprzętowych systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PE-03(05)** | **KONTROLA DOSTĘPU FIZYCZNEGO \| OCHRONA PRZED MANIPULACJĄ** | |
| | **PE-03(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-03(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne wykrywające/zapobiegające fizycznym manipulacjom lub zmianie komponentów sprzętowych systemu; mechanizmy/zabezpieczenia wspierające lub wdrażające wykrywanie/zapobieganie fizycznym manipulacjom/zmianom komponentów sprzętowych systemu]. |

| | | |
|---|---|---|
| **PE-03(06)** | **KONTROLA DOSTĘPU FIZYCZNEGO \| TESTY PENETRACYJNE OBIEKTU** | |
| | [WYCOFANE: Włączone do CA-08]. | |

| | | |
|---|---|---|
| **PE-03(07)** | **KONTROLA DOSTĘPU FIZYCZNEGO \| BARIERY FIZYCZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-03(07)** | W celu ograniczenia dostępu stosuje się bariery fizyczne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-03(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli dostępu fizycznego; lista barier fizycznych ograniczających dostęp do systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-03(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **PE-03(08)** | **KONTROLA DOSTĘPU FIZYCZNEGO \| ŚLUZY W KONTROLI DOSTĘPU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-03(08)_ODP** | ***określono miejsca w obiekcie, w których mają być zastosowane śluzy w kontroli dostępu;*** |
| | **PE-03(08)** | w ***<lokalizacjach PE-03(08)_ODP>*** stosuje się śluzy kontroli dostępu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-03(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli dostępu fizycznego; lista śluz i lokalizacji kontroli dostępu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-03(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-03(08)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące śluz w kontroli dostępu, zabezpieczające przed nieuprawnionym dostępem]. |

| | | |
|---|---|---|
| **PE-04** | **KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-04_ODP[01]** | ***określono systemowe linie dystrybucji i transmisji wymagające kontroli dostępu fizycznego;*** |
| | **PE-04_ODP[02]** | ***określono środki kontroli bezpieczeństwa, które należy wdrożyć w celu kontroli fizycznego dostępu do systemowych linii dystrybucji i transmisji w obrębie obiektu organizacji;*** |

| | | |
|---|---|---|
| **PE-04** | **KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO** | |
| | **PE-04** | dostęp fizyczny do ***<systemowych linii dystrybucji i transmisji PE-04_ODP[01]>*** w obrębie obiektów organizacji jest kontrolowany przy użyciu ***<zabezpieczeń PE-04_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli dostępu do nośników danych; dokumentacja projektowa systemu; schematy komunikacyjne i elektryczne obiektu; lista zabezpieczeń fizycznych stosowanych w systemowych liniach dystrybucji i transmisji; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-04-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące kontroli dostępu do linii dystrybucji i transmisji; mechanizmy/zabezpieczenia wspierające lub wdrażające kontrolę dostępu do linii dystrybucji i transmisji]. |

| | | |
|---|---|---|
| **PE-05** | **KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-05_ODP** | ***określono urządzenia wyjścia, które wymagają kontroli dostępu fizycznego do wyjścia;*** |
| | **PE-05** | fizyczny dostęp do danych wyjściowych z ***<urządzeń wyjścia PE-05_ODP>*** jest kontrolowany w celu uniemożliwienia uzyskania danych wyjściowych przez osoby nieupoważnione. |

| | | |
|---|---|---|
| **PE-05** | **KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli dostępu do nośników danych; rozmieszczenie elementów systemu w obiekcie; wyświetlanie rzeczywistych danych z komponentów systemu; lista urządzeń wyjścia i związanych z nimi wyjść wymagających kontroli dostępu fizycznego; dzienniki lub zapisy dotyczące kontroli dostępu fizycznego do obszarów zawierających urządzenia wyjścia oraz związane z nimi wyjścia; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-05-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | |
|---|---|
| **PE-05(01)** | **KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA \| DOSTĘP UPOWAŻNIONYCH OSÓB DO URZĄDZEŃ** |
| | [WYCOFANE: Włączone do PE-05]. |

| | | |
|---|---|---|
| **PE-05(02)** | **KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA \| DOSTĘP DO DANYCH NA PODSTAWIE INDYWIDUALNEJ TOŻSAMOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-05(02)** | indywidualna tożsamość jest powiązana udzielaniem dostępu do danych wyjściowych z urządzeń wyjścia. |

| | | |
|---|---|---|
| **PE-05(02)** | **KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA \| DOSTĘP DO DANYCH NA PODSTAWIE INDYWIDUALNEJ TOŻSAMOŚCI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-05(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli dostępu fizycznego; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista urządzeń wyjścia i związanych z nimi wyjść wymagających kontroli dostępu fizycznego; dzienniki lub zapisy dotyczące kontroli dostępu fizycznego do obszarów, w których znajdują się urządzenia wyjścia i związane z nimi wyjścia; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka w zakresie ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PE-05(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci; programiści systemu]. |
| | **PE-05(02)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | |
|---|---|
| **PE-05(03)** | **KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA \| OZNACZANIE URZĄDZEŃ WEJŚCIA - WYJŚCIA** |
| | [WYCOFANE: Włączone do PE-22]. |

| | | |
|---|---|---|
| **PE-06** | **MONITOROWANIE DOSTĘPU FIZYCZNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-06_ODP[01]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu dzienników dostępu fizycznego;*** |
| | **PE-06_ODP[02]** | ***określono zdarzenia lub przesłanki wskazujące na wystąpienie zdarzeń wymagających przeglądu dzienników dostępu fizycznego;*** |
| | **PE-06a.** | fizyczny dostęp do obiektu, w którym znajduje się system, jest monitorowany w celu wykrywania i reagowania na incydenty związane z bezpieczeństwem fizycznym; |
| | **PE-06b.[01]** | dzienniki dostępu fizycznego są przeglądane z ***<częstotliwością PE-06_ODP[01]>***; |
| | **PE-06b.[02]** | dzienniki dostępu fizycznego są przeglądane po wystąpieniu***<zdarzeń PE-06_ODP[02]>***; |
| | **PE-06c.[01]** | wyniki przeglądów są koordynowane z możliwościami organizacji w zakresie reagowania na incydenty; |
| | **PE-06c.[02]** | wyniki dochodzeń są koordynowane z możliwościami organizacji w zakresie reagowania na incydenty; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące monitorowania dostępu fizycznego; dzienniki lub rejestry dostępu fizycznego; rejestry monitorowania dostępu fizycznego; przeglądy dzienników dostępu fizycznego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PE-06** | **MONITOROWANIE DOSTĘPU FIZYCZNEGO** | |
| | **PE-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacyjny odpowiedzialny za reagowanie na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania dostępu fizycznego; mechanizmy wspierające lub wdrażające monitorowanie dostępu fizycznego; mechanizmy wspierające lub wdrażające przegląd dzienników dostępu fizycznego]. |

| | | |
|---|---|---|
| **PE-06(01)** | **MONITOROWANIE DOSTĘPU FIZYCZNEGO \| ALARMY WŁAMANIOWE I URZĄDZENIA NADZORUJĄCE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-06(01)[01]** | fizyczny dostęp do obiektu, w którym znajduje się system, jest monitorowany za pomocą fizycznych systemów antywłamaniowych; |
| | **PE-06(01)[02]** | fizyczny dostęp do obiektu, w którym znajduje się system, jest monitorowany za pomocą fizycznych urządzeń nadzorujących; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-06(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące monitorowania dostępu fizycznego; dzienniki lub zapisy dotyczące dostępu fizycznego; zapisy dotyczące monitorowania dostępu fizycznego; przeglądy dzienników dostępu fizycznego; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka w zakresie ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PE-06(01)** | **MONITOROWANIE DOSTĘPU FIZYCZNEGO \| ALARMY WŁAMANIOWE I URZĄDZENIA NADZORUJĄCE** | |
| | **PE-06(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacyjny odpowiedzialny za reagowanie na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PE-06(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania fizycznych alarmów antywłamaniowych i urządzeń nadzorujących; mechanizmy wspierające lub wdrażające monitorowanie dostępu fizycznego; mechanizmy wspierające lub wdrażające fizyczne alarmy włamaniowe i urządzenia nadzorujące]. |

| | | |
|---|---|---|
| **PE-06(02)** | **MONITOROWANIE DOSTĘPU FIZYCZNEGO \| AUTOMATYCZNE ROZPOZNAWANIE WŁAMANIA/INFORMOWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-06(02)_ODP[01]** | ***określono klasy lub rodzaje włamań, które mają być rozpoznawane przez automatyczne mechanizmy;*** |
| | **PE-06(02)_ODP[02]** | ***określono reakcje, które mają być inicjowane przez automatyczne mechanizmy w przypadku rozpoznania zdefiniowanych przez organizację klas lub rodzajów włamań;*** |
| | **PE-06(02)_ODP[03]** | ***określono automatyczne mechanizmy służące do rozpoznawania klas lub rodzajów włamań i inicjowania reakcji (zdefiniowanych w PE-06(02)_ODP);*** |
| | **PE-06(02)[01]** | ***<klasy lub rodzaje włamań PE-06(02)_ODP[01]>*** są rozpoznawane; |
| | **PE-06(02)[02]** | ***<reakcje PE-06(02)_ODP[02]>*** są inicjowane przy użyciu ***<mechanizmów automatycznych PE-06(02)_ODP[03]>***. |

| | | |
|---|---|---|
| **PE-06(02)** | **MONITOROWANIE DOSTĘPU FIZYCZNEGO \| AUTOMATYCZNE ROZPOZNAWANIE WŁAMANIA/INFORMOWANIE** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-06(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące monitorowania dostępu fizycznego; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; lista reakcji, które zostaną podjęte w przypadku rozpoznania określonych klas lub rodzajów włamań; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PE-06(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PE-06(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne monitorowania dostępu fizycznego; automatyczne mechanizmy wspierające lub wdrażające monitorowanie dostępu fizycznego; automatyczne mechanizmy wspierające lub wdrażające rozpoznawanie klas lub rodzajów włamań i inicjowanie reakcji]. |

| | | |
|---|---|---|
| **PE-06(03)** | **MONITOROWANIE DOSTĘPU FIZYCZNEGO \| MONITORING WIZYJNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-06(03)_ODP[01]** | ***określono obszary operacyjne, w których ma być stosowany monitoring wizyjny;*** |
| | **PE-06(03)_ODP[02]** | ***określono częstotliwość przeglądania nagrań wideo;*** |

| | | |
|---|---|---|
| **PE-06(03)** | **MONITOROWANIE DOSTĘPU FIZYCZNEGO \| MONITORING WIZYJNY** | |
| | **PE-06(03)_ODP[03]** | ***określono okres przechowywania nagrań wideo;*** |
| | **PE-06(03)(a)** | stosuje się monitoring wizyjny ***<obszarów operacyjnych PE-06(03)_ODP[01]>***; |
| | **PE-06(03)(b)** | nagrania wideo są przeglądane z ***<częstotliwością PE-06(03)_ODP[02]>***; |
| | **PE-06(03)(c)** | nagrania wideo są przechowywane przez ***<okres PE-06(03)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-06(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące fizycznego monitorowania dostępu; sprzęt do monitoringu wizyjnego wykorzystywany do monitorowania obszarów operacyjnych; nagrania wideo z obszarów operacyjnych, w których stosowany jest monitoring wizyjny; dzienniki lub zapisy dotyczące sprzętu do monitoringu wizyjnego; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka w zakresie ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PE-06(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PE-06(03)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PE-06(04)** | **MONITOROWANIE DOSTĘPU FIZYCZNEGO \| MONITOROWANIE DOSTĘPU FIZYCZNEGO DO SYSTEMÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-06(04)_ODP** | ***określono fizyczne przestrzenie zawierające jeden lub więcej komponentów systemu;*** |
| | **PE-06(04)** | fizyczny dostęp do systemu jest monitorowany w uzupełnieniu do monitoringu fizycznego dostępu do obiektu w ***<przestrzeniach fizycznych PE-06(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-06(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące monitorowania dostępu fizycznego; dzienniki lub zapisy dotyczące kontroli dostępu fizycznego; urządzenia kontroli dostępu fizycznego; upoważnienia dostępu; dane uwierzytelniające; lista obszarów w obiekcie, w których skoncentrowano komponenty systemu, lub lista komponentów systemu wymagających dodatkowego monitorowania dostępu fizycznego; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PE-06(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PE-06(04)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | |
|---|---|
| **PE-07** | **KONTROLA GOŚCI** |
| | [WYCOFANE: Włączone do PE-02, PE-03]. |

| | | |
|---|---|---|
| **PE-08** | **REJESTRACJA DOSTĘPU GOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-08_ODP[01]** | ***określono okres przechowywania ewidencji dostępu gości do obiektu, w którym znajduje się system;*** |
| | **PE-08_ODP[02]** | ***określono częstotliwość przeglądu ewidencji dostępu gości do obiektu;*** |
| | **PE-08_ODP[03]** | ***określono personel, któremu zgłasza się nieprawidłowości w ewidencji dostępu gości do obiektu;*** |
| | **PE-08a.** | ewidencja dostępu gości do obiektu, w którym znajduje się system jest przechowywana przez ***<okres PE-08_ODP[01]>***; |
| | **PE-08b.** | ewidencja dostępu gości do obiektu jest sprawdzana z ***<częstotliwością PE-08_ODP[02]>***; |
| | **PE-08c.** | nieprawidłowości w ewidencji dostępu gości do obiektu zgłaszane są do ***<personelu PE-08_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące ewidencji dostępu gości do obiektu; dzienniki lub zapisy dotyczące kontroli dostępu gości do obiektu; przeglądy dzienników lub zapisów dotyczących dostępu gości do obiektu; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka w zakresie ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PE-08** | **REJESTRACJA DOSTĘPU GOŚCI** | |
| | **PE-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ewidencję dostępu gościu do obiektu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PE-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące prowadzenia i przeglądu dokumentacji związanej z dostępem gości do obiektu; mechanizmy wspierające lub wdrażające prowadzenie i przegląd dokumentacji związanej z dostępem gości do obiektu]. |

| | | |
|---|---|---|
| **PE-08(01)** | **REJESTRACJA DOSTĘPU GOŚCI \| AUTOMATYCZNA REJESTRACJA/PRZEGLĄD** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-08(01)_ODP[01]** | ***określono automatyczne mechanizmy stosowane do prowadzenia ewidencji dostępu gości do obiektu;*** |
| | **PE-08(01)_ODP[02]** | ***określono automatyczne mechanizmy stosowane do przeglądu ewidencji dostępu gości do obiektu;*** |
| | **PE-08(01)[01]** | ewidencja dostępu gości do obiektu prowadzona jest przy użyciu ***<automatycznych mechanizmów PE-08(01)_ODP[01]>***; |
| | **PE-08(01)[02]** | zapisy dotyczące dostępu gości do obiektu są weryfikowane przy użyciu ***<automatycznych mechanizmów PE-08(01)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **PE-08(01)** | **REJESTRACJA DOSTĘPU GOŚCI \| AUTOMATYCZNA REJESTRACJA/PRZEGLĄD** | |
|---|---|---|
| | **PE-08(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące zapisów dotyczących dostępu odwiedzających; automatyczne mechanizmy wspierające zarządzanie zapisami dotyczącymi dostępu odwiedzających; dzienniki lub zapisy kontroli dostępu odwiedzających; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PE-08(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ewidencję dostępu gościu do obiektu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PE-08(01)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ewidencję dostępu gości do obiektu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| **PE-08(02)** | **REJESTRACJA DOSTĘPU GOŚCI \| EWIDENCJA DOSTĘPU FIZYCZNEGO** |
|---|---|
| | [WYCOFANE: Włączone do PE-02]. |

| **PE-08(03)** | **REJESTRACJA DOSTĘPU GOŚCI \| OGRANICZANIE ELEMENTÓW DANYCH OSOBOWYCH UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-08(03)_ODP** | ***określono elementy zidentyfikowane w ocenie ryzyka w zakresie prywatności w celu ograniczenia zakresu danych identyfikacyjnych zawartych w ewidencji dostępu gości do obiektu;*** |
| | **PE-08(03)** | dane identyfikacyjne zawarte w ewidencji dostępu gości do obiektu są ograniczone do ***<elementów PE-08(03)_ODP>*** zidentyfikowanych w ocenie ryzyka dla prywatności. |

| | | |
|---|---|---|
| **PE-08(03)** | **REJESTRACJA DOSTĘPU GOŚCI \| OGRANICZANIE ELEMENTÓW DANYCH OSOBOWYCH UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-08(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; polityka przetwarzania danych identyfikacyjnych; dokumentacja oceny ryzyka związanego z prywatnością; ocena wpływu na prywatność; zapisy dotyczące dostępu gości do obiektu; spis danych identyfikacyjnych; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PE-08(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ewidencję dostępu gości do obiektu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PE-08(03)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ewidencję dostępu gości do obiektu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PE-09** | **WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-09[01]** | urządzenia zasilające system są chronione przed uszkodzeniem i zniszczeniem; |
| | **PE-09[02]** | okablowanie zasilające system jest zabezpieczone przed uszkodzeniem i zniszczeniem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PE-09** | **WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE** | |
| | **PE-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące ochrony urządzeń zasilających/okablowania; obiekty, w których znajdują się urządzenia zasilające/okablowanie; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę urządzeń zasilających/okablowania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-09-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające ochronę urządzeń zasilających/okablowania]. |

| | | |
|---|---|---|
| **PE-09(01)** | **WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE \| REDUNDANCJA OKABLOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-09(01)_ODP** | ***określono odległość fizycznego odseparowania torów redundantnego okablowania zasilającego;*** |
| | **PE-09(01)** | zastosowano redundantne tory okablowania zasilającego, które są fizycznie odseparowane i umieszczone w ***<odległości PE-09(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-09(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące ochrony urządzeń zasilających/okablowania; obiekty, w których znajdują się urządzenia zasilające/okablowanie; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-09(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę urządzeń zasilających/okablowania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **PE-09(01)** | **WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE \| REDUNDANCJA OKABLOWANIA** | |
| | **PE-09(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające ochronę urządzeń zasilających/okablowania]. |

| | | |
|---|---|---|
| **PE-09(02)** | **WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE \| AUTOMATYCZNA KONTROLA JAKOŚCI NAPIĘCIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-09(02)_ODP** | ***określono kluczowe komponenty systemu, które wymagają automatycznej kontroli jakości napięcia;*** |
| | **PE-09(02)** | zastosowano automatyczną kontrolę jakości napięcia dla ***<kluczowych komponentów systemu PE-09(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-09(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące kontroli jakości napięcia; plan bezpieczeństwa; lista kluczowych komponentów systemu wymagających automatycznej kontroli jakości napięcia; mechanizmy automatycznej kontroli jakości napięcia i związane z nimi konfiguracje; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-09(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę środowiska komponentów systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-09(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające automatyczną kontrolę jakości napięcia]. |

| | | |
|---|---|---|
| **PE-10** | **WYŁĄCZENIE AWARYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-10_ODP[01]** | ***określono system lub poszczególne komponenty systemu, które wymagają możliwości odcięcia zasilania w sytuacjach awaryjnych;*** |
| | **PE-10_ODP[02]** | ***określono lokalizację awaryjnych wyłączników lub urządzeń odcinających według systemu lub komponentu systemu;*** |
| | **PE-10a.** | zapewniono możliwość wyłączenia zasilania ***<systemu lub komponentów systemu PE-10_ODP[01]>*** w sytuacjach awaryjnych; |
| | **PE-10b.** | awaryjne wyłączniki lub urządzenia odcinające są umieszczone w ***<lokalizacji PE-10_ODP[02]>*** w celu zapewnienia łatwiejszego dostępu uprawnionemu personelowi; |
| | **PE-10c.** | funkcja awaryjnego wyłączenia zasilania posiada zabezpieczenia chroniące przed nieuprawnioną aktywacją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące awaryjnego wyłączenia zasilania; awaryjne wyłączniki lub przełączniki; lokalizacje, w których znajdują się awaryjne wyłączniki i inne urządzenia; zabezpieczenia chroniące funkcję awaryjnego wyłączenia przed nieuprawnioną aktywacją; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-10-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za funkcję awaryjnego wyłączenia zasilania (zarówno wdrażający, jak i korzystający z tej funkcji); personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-10-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające funkcję awaryjnego wyłączenia zasilania]. |

| | |
|---|---|
| **PE-10(01)** | **WYŁĄCZENIE AWARYJNE \| PRZYPADKOWA I NIEAUTORYZOWANA AKTYWACJA** |
| | [WYCOFANE: Włączone do PE-10]. |

| | | |
|---|---|---|
| **PE-11** | **ZASILANIE AWARYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-11_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {zorganizowane wyłączenie systemu; przejście systemu na długoterminowe alternatywne źródło zasilania};*** |
| | **PE-11** | zapewniono bezprzerwowe zasilanie w celu ułatwienia ***<WYBRANA WARTOŚĆ PARAMETRU PE-11_ODP>*** w przypadku utraty podstawowego źródła zasilania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-11-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące zasilania awaryjnego; zasilanie bezprzerwowe; dokumentacja dotycząca zasilania bezprzerwowego; zapisy dotyczące testów zasilania bezprzerwowego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-11-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zasilanie lub planowanie awaryjne; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-11-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające bezprzerwowe zasilanie; bezprzerwowe zasilanie]. |

| | | |
|---|---|---|
| **PE-11(01)** | **ZASILANIE AWARYJNE \| ALTERNATYWNE ZASILANIE - MINIMALNA ZDOLNOŚĆ OPERACYJNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-11(01)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {ręcznie; automatycznie};*** |
| | **PE-11(01)[01]** | aktywowane jest alternatywne źródło zasilania przewidziane dla systemu ***<WYBRANA WARTOŚĆ PARAMETRU PE-11(01)_ODP>***; |
| | **PE-11(01)[02]** | alternatywne źródło zasilania przewidziane dla systemu może utrzymać minimalną wymaganą zdolność operacyjną w przypadku długotrwałej niedostępności podstawowego źródła zasilania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-11(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące zasilania awaryjnego; alternatywne źródło zasilania; dokumentacja dotycząca alternatywnego źródła zasilania; zapisy dotyczące testów alternatywnego źródła zasilania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-11(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zasilanie lub planowanie awaryjne; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-11(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające alternatywne źródło zasilania; alternatywne źródło zasilania]. |

| | | |
|---|---|---|
| **PE-11(02)** | **ZASILANIE AWARYJNE \| ALTERNATYWNE SAMOOBSŁUGOWE ŹRÓDŁO ZASILANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-11(02)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {ręcznie; automatycznie};*** |
| | **PE-11(02)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {minimalna wymagana zdolność operacyjna; pełna zdolność operacyjna};*** |
| | **PE-11(02)** | aktywowane jest alternatywne źródło zasilania przewidziane dla systemu ***<WYBRANA WARTOŚĆ PARAMETRU PE-11(02)_ODP[01]>***; |
| | **PE-11(02)(a)** | alternatywne źródło zasilania przewidziane dla systemu jest samoobsługowe (autostart); |
| | **PE-11(02)(b)** | alternatywne źródło zasilania przewidziane dla systemu nie jest zależne od zewnętrznego źródła energii; |
| | **PE-11(02)(c)** | alternatywne źródło zasilania przewidziane dla systemu jest w stanie utrzymać ***<WYBRANA WARTOŚĆ PARAMETRU PE-11(02)_ODP[02]>*** w przypadku długotrwałej niedostępności podstawowego źródła zasilania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-11(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące zasilania awaryjnego; alternatywne źródło zasilania; dokumentacja dotycząca alternatywnego źródła zasilania; zapisy dotyczące testów alternatywnego źródła zasilania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-11(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zasilanie lub planowanie awaryjne; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **PE-11(02)** | **ZASILANIE AWARYJNE \| ALTERNATYWNE SAMOOBSŁUGOWE ŹRÓDŁO ZASILANIA** | |
| | **PE-11(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające alternatywne źródło zasilania; alternatywne źródło zasilania]. |

| | | |
|---|---|---|
| **PE-12** | **OŚWIETLENIE AWARYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-12[01]** | w systemie zastosowano automatyczne oświetlenie awaryjne, które aktywuje się w przypadku przerw lub zakłóceń w dostawie prądu; |
| | **PE-12[02]** | w systemie utrzymywane jest automatyczne oświetlenie awaryjne, które uruchamia się w przypadku przerw lub zakłóceń w dostawie prądu; |
| | **PE-12[03]** | automatyczne oświetlenie awaryjne oświetla wyjścia awaryjne na terenie obiektu; |
| | **PE-12[04]** | automatyczne oświetlenie awaryjne oświetla drogi ewakuacyjne w obiekcie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-12-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące oświetlenia awaryjnego; dokumentacja oświetlenia awaryjnego; zapisy testów oświetlenia awaryjnego; wyjścia awaryjne i drogi ewakuacyjne; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-12-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oświetlenie lub planowanie awaryjne; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-12-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające oświetlenie awaryjne]. |

| | | |
|---|---|---|
| **PE-12(01)** | **OŚWIETLENIE AWARYJNE \| ZASADNICZE DZIAŁANIA/FUNKCJE BIZNESOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-12(01)** | we wszystkich miejscach w obiekcie, które wspierają zasadnicze działania i funkcje biznesowe, zapewnione jest oświetlenie awaryjne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-12(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące oświetlenia awaryjnego; dokumentacja oświetlenia awaryjnego; zapisy dotyczące testów oświetlenia awaryjnego; wyjścia awaryjne i drogi ewakuacyjne; obszary/lokalizacje w obrębie obiektu wspierające zasadnicze działania i funkcje biznesowe; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-12(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oświetlenie lub planowanie awaryjne; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-12(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające oświetlenie awaryjne]. |

| | | |
|---|---|---|
| **PE-13** | **OCHRONA PRZECIWPOŻAROWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-13[01]** | zastosowano systemy sygnalizacji pożarowej; |
| | **PE-13[02]** | zastosowane systemy sygnalizacji pożarowej są zasilane przez niezależne źródło energii; |

| | | |
|---|---|---|
| **PE-13** | **OCHRONA PRZECIWPOŻAROWA** | |
| | **PE-13[03]** | zastosowane systemy sygnalizacji pożarowej są utrzymywane w dobrym stanie; |
| | **PE-13[04]** | zastosowano systemy gaśnicze; |
| | **PE-13[05]** | zastosowane systemy gaśnicze są zasilane przez niezależne źródło energii; |
| | **PE-13[06]** | zastosowane systemy gaśnicze są utrzymywane w dobrym stanie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-13-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące ochrony przeciwpożarowej; urządzenia/systemy wykrywania i gaszenia ognia; dokumentacja urządzeń/systemów wykrywania i gaszenia ognia; zapisy dotyczące testów urządzeń/systemów wykrywania i gaszenia ognia; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-13-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za urządzenia/systemy sygnalizacji pożarowej oraz gaśnicze; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-13-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające urządzenia/systemy wykrywania i gaszenia ognia]. |

| | | |
|---|---|---|
| **PE-13(01)** | **OCHRONA PRZECIWPOŻAROWA \| SYSTEMY DETEKCJI - AUTOMATYCZNA AKTYWACJA I POWIADAMIANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-13(01)_ODP[01]** | ***określono personel lub role, które należy powiadomić w przypadku pożaru;*** |

| | | |
|---|---|---|
| **PE-13(01)** | **OCHRONA PRZECIWPOŻAROWA \| SYSTEMY DETEKCJI - AUTOMATYCZNA AKTYWACJA I POWIADAMIANIE** | |
| | **PE-13(01)_ODP[02]** | ***określono podmioty odpowiedzialne za reagowanie w sytuacjach kryzysowych, które należy powiadomić w przypadku pożaru;*** |
| | **PE-13(01)[01]** | stosuje się systemy sygnalizacji pożarowej, które aktywują się automatycznie w razie pożaru; |
| | **PE-13(01)[02]** | stosuje się systemy sygnalizacji pożarowej, które automatycznie powiadamiają ***<personel lub role PE-13(01)_ODP[01]> w*** razie wystąpienia pożaru; |
| | **PE-13(01)[03]** | stosuje się systemy sygnalizacji pożarowej, które automatycznie powiadamiają ***<osoby reagujące na sytuacje kryzysowe PE-13(01)_ODP[02]> w*** razie wystąpienia pożaru. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-13(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące ochrony przeciwpożarowej; obiekt, w którym znajduje się system informatyczny; umowy dotyczące poziomu obsługi w zakresie alarmów; protokoły z testów urządzeń/systemów wykrywania i gaszenia ognia; dokumentacja urządzeń/systemów wykrywania i gaszenia ognia; alarmy/powiadomienia o pożarach; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-13(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za urządzenia/systemy wykrywania i gaszenia ognia; personel organizacyjny odpowiedzialny za powiadamianie odpowiedniego personelu, ról i służb ratowniczych o pożarach; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-13(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające urządzenia/systemy wykrywania pożaru; aktywacja urządzeń/systemów wykrywania pożaru (symulowanego); automatyczne powiadomienia]. |

| | | |
|---|---|---|
| **PE-13(02)** | **OCHRONA PRZECIWPOŻAROWA \| SYSTEMY DETEKCJI - AUTOMATYCZNA AKTYWACJA I POWIADAMIANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-13(02)_ODP[01]** | ***określono personel lub role, które należy powiadomić w przypadku pożaru;*** |
| | **PE-13(02)_ODP[02]** | ***określono podmioty odpowiedzialne za reagowanie w sytuacjach kryzysowych, które należy powiadomić w przypadku pożaru;*** |
| | **PE-13(02)(a)[01]** | stosuje się systemy gaszenia ognia, które aktywują się automatycznie; |
| | **PE-13(02)(a)[02]** | stosuje się systemy gaszenia ognia, które powiadamiają ***<personel lub role PE-13(02)_ODP[01]>***<br>w sposób automatyczny; |
| | **PE-13(02)(a)[03]** | stosuje się systemy gaszenia ognia, które powiadamiają ***<osoby reagujące na sytuacje kryzysowe PE-13(02)_ODP[02]>***.<br>w sposób automatyczny; |
| | **PE-13(02)(b)** | jeżeli w obiekcie nie ma stałego personelu, stosuje się automatyczną instalację gaśniczą. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-13(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące ochrony przeciwpożarowej; dokumentacja urządzeń/systemów wykrywania i gaszenia ognia; obiekt, w którym znajduje się system; umowy dotyczące poziomu obsługi w zakresie alarmów; zapisy dotyczące testów urządzeń/systemów wykrywania i gaszenia ognia; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PE-13(02)** | **OCHRONA PRZECIWPOŻAROWA \| SYSTEMY DETEKCJI - AUTOMATYCZNA AKTYWACJA I POWIADAMIANIE** | |
| | **PE-13(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za urządzenia/systemy wykrywania i gaszenia ognia; personel organizacyjny odpowiedzialny za dostarczanie automatycznych powiadomień o każdym uruchomieniu urządzeń/systemów gaszenia ognia odpowiednim osobom, w tym reagującym na sytuacje kryzysowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-13(02)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspomagające lub wdrażające urządzenia/systemy gaszenia ognia; uruchamianie urządzeń/systemów gaszenia ognia (symulowane); automatyczne powiadomienia]. |

| | | |
|---|---|---|
| **PE-13(03)** | **OCHRONA PRZECIWPOŻAROWA \| AUTOMATYCZNE GASZENIE POŻARU** | |
| | [WYCOFANE: Włączone do PE-13(02)]. | |

| | | |
|---|---|---|
| **PE-13(04)** | **OCHRONA PRZECIWPOŻAROWA \| INSPEKCJE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-13(04)_ODP[01]** | ***określono częstotliwość przeprowadzania kontroli stanu ochrony przeciwpożarowej w obiekcie;*** |
| | **PE-13(04)_ODP[02]** | ***określono wymagany termin usunięcia uchybień stwierdzonych w wyniku kontroli ochrony przeciwpożarowej;*** |
| | **PE-13(04)[01]** | obiekt poddawany jest przeglądom ochrony przeciwpożarowej z ***<częstotliwością PE-13(04)_ODP[01]>***, a przeglądów tych dokonują wykwalifikowani inspektorzy z odpowiednimi uprawnieniami; |

| | | |
|---|---|---|
| **PE-13(04)** | **OCHRONA PRZECIWPOŻAROWA \| INSPEKCJE** | |
| | **PE-13(04)[02]** | uchybienia stwierdzone podczas inspekcji ochrony przeciwpożarowej są usuwane w ciągu ***<okresu PE-13(04)_ODP[02]>*.** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-13(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące ochrony przeciwpożarowej; obiekt, w którym znajduje się system; plany inspekcji; wyniki inspekcji; raporty z inspekcji; protokoły z testów urządzeń/systemów wykrywania i gaszenia ognia; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-13(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie, zatwierdzanie i wykonywanie przeglądów przeciwpożarowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **PE-14** | **ZABEZPIECZENIA ŚRODOWISKOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-14_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {temperatura; wilgotność; ciśnienie; promieniowanie; <zabezpieczenie środowiskowe PE-14_ODP[02]>};*** |
| | **PE-14_ODP[02]** | ***określono zabezpieczenie środowiskowe, które musi być utrzymane na należytym poziomie, w obiekcie, w którym znajduje się system (jeśli wybrano);*** |
| | **PE-14_ODP[03]** | ***określono dopuszczalne poziomy zabezpieczeń środowiskowych;*** |
| | **PE-14_ODP[04]** | ***określono częstotliwość, z jaką należy monitorować poziomy zabezpieczeń środowiskowych;*** |

| | | |
|---|---|---|
| **PE-14** | **ZABEZPIECZENIA ŚRODOWISKOWE** | |
| | **PE-14a.** | ***<WYBRANA WARTOŚĆ PARAMETRU PE-14_ODP[01]>*** są utrzymywane na ***<odpowiednich poziomach PE-14_ODP[03]>*** w obiekcie, w którym znajduje się system; |
| | **PE-14b.** | poziomy zabezpieczeń środowiskowych są monitorowane z ***<częstotliwością PE-14_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-14-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące zabezpieczeń w zakresie temperatury i wilgotności; zabezpieczenia w zakresie temperatury i wilgotności; obiekt, w którym znajduje się system; dokumentacja dotycząca zabezpieczeń w zakresie temperatury i wilgotności; zapisy dotyczące temperatury i wilgotności; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-14-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczenia środowiskowe systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-14-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające utrzymanie i monitorowanie poziomu temperatury i wilgotności]. |

| | | |
|---|---|---|
| **PE-14(01)** | **ZABEZPIECZENIA ŚRODOWISKOWE \| ZABEZPIECZENIA AUTOMATYCZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-14(01)_ODP** | ***określono automatyczne zabezpieczenia środowiskowe zapobiegające wahaniom, które są potencjalnie szkodliwe dla systemu;*** |

| | | |
|---|---|---|
| **PE-14(01)** | **ZABEZPIECZENIA ŚRODOWISKOWE \| ZABEZPIECZENIA AUTOMATYCZNE** | |
| | **PE-14(01)** | w obiekcie stosuje się ***<automatyczne zabezpieczenia środowiskowe PE-14(01)_ODP>***, aby zapobiec fluktuacjom, które mogą być szkodliwe dla systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-14(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące zabezpieczeń w zakresie temperatury i wilgotności; obiekt, w którym znajduje się system; automatyczne zabezpieczenia w zakresie temperatury i wilgotności; dokumentacja dotycząca temperatury i wilgotności; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-14(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczenia środowiskowe systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-14(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspierające lub wdrażające utrzymanie poziomu temperatury i wilgotności]. |

| | | |
|---|---|---|
| **PE-14(02)** | **ZABEZPIECZENIA ŚRODOWISKOWE \| MONITOROWANIE, ALARMOWANIE/POWIADOMIENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-14(02)_ODP** | ***określono personel lub role powiadamiane przez zabezpieczenia środowiskowe, gdy zachodzące zmiany w środowisku są potencjalnie szkodliwe dla personelu lub urządzeń;*** |
| | **PE-14(02)[01]** | zabezpieczenia środowiskowe są monitorowane; |

| | | |
|---|---|---|
| **PE-14(02)** | **ZABEZPIECZENIA ŚRODOWISKOWE \| MONITOROWANIE, ALARMOWANIE/POWIADOMIENIA** | |
| | **PE-14(02)[02]** | monitorowanie zabezpieczeń środowiskowych zapewniane jest przez alarm lub powiadomienie dla ***<personelu lub ról PE-14(02)_ODP>***, jeżeli zachodzące zmiany są potencjalnie szkodliwe dla personelu lub sprzętu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-14(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące monitorowania temperatury i wilgotności; obiekt, w którym znajduje się system; dzienniki lub zapisy dotyczące monitorowania temperatury i wilgotności; zapisy dotyczące zmian temperatury i wilgotności, które generują alarmy lub powiadomienia; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-14(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczenia środowiskowe systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-14(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające monitorowanie temperatury i wilgotności]. |

| | | |
|---|---|---|
| **PE-15** | **OCHRONA PRZED ZALANIEM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-15[01]** | system jest zabezpieczony przed uszkodzeniami wynikającymi z zalania poprzez wyposażenie go w główne zawory odcinające lub separujące; |
| | **PE-15[02]** | główne zawory odcinające lub separujące są fizycznie dostępne; |
| | **PE-15[03]** | główne zawory odcinające lub separujące działają prawidłowo; |
| | **PE-15[04]** | kluczowy personel posiada wiedzę na temat głównych zaworów odcinających lub separujących; |

| | | |
|---|---|---|
| **PE-15** | **OCHRONA PRZED ZALANIEM** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-15-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące ochrony przed zalaniem; obiekt, w którym znajduje się system; główne zawory odcinające; lista kluczowego personelu znającego lokalizację i procedury aktywacji głównych zaworów odcinających w systemie hydraulicznym; dokumentacja głównych zaworów odcinających; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-15-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczenia środowiskowe systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-15-Test** | [WYBÓR SPOŚRÓD: Główne zawory odcinające wodę; proces organizacyjny w zakresie dotyczący aktywacji głównych zaworów odcinających wodę]. |

| | | |
|---|---|---|
| **PE-15(01)** | **OCHRONA PRZED ZALANIEM \| AUTOMATYCZNE WYKRYWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-15(01)_ODP[01]** | ***określono personel lub role, które mają być ostrzegane w przypadku wykrycia obecności wody w pobliżu systemu;*** |
| | **PE-15(01)_ODP[02]** | ***określono automatyczne mechanizmy wykorzystywane do wykrywania obecności wody w pobliżu systemu;*** |
| | **PE-15(01)[01]** | obecność wody w pobliżu systemu może być wykrywana automatycznie; |
| | **PE-15(01)[02]** | ***<personel lub role PE-15(01)_ODP[01]>*** są ostrzegane przy użyciu ***<automatycznych mechanizmów PE-15(01)_ODP[02]>.*** |

| | | |
|---|---|---|
| **PE-15(01)** | **OCHRONA PRZED ZALANIEM \| AUTOMATYCZNE WYKRYWANIE** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-15(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące ochrony przed zalaniem; obiekt, w którym znajduje się system; automatyczne mechanizmy dla zaworów odcinających wodę; automatyczne mechanizmy wykrywania obecności wody w pobliżu systemu; alarmy/powiadomienia o wykryciu wody w obiekcie, w którym znajduje się system; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-15(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczenia środowiskowe systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-15(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania wody oraz alarmy w systemie]. |

| | | |
|---|---|---|
| **PE-16** | **DOSTAWA I USUWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-16_ODP[01]** | ***określono rodzaje komponentów systemu, które podlegają zatwierdzeniu i kontroli przy wejściu do obiektu;*** |
| | **PE-16_ODP[02]** | ***określono rodzaje komponentów systemu, które podlegają zatwierdzeniu i kontroli przy wyjściu z obiektu;*** |
| | **PE-16a.[01]** | ***<rodzaje komponentów systemu PE-16_ODP[01]>*** podlegają zatwierdzeniu przy wejściu do obiektu; |
| | **PE-16a.[02]** | ***<rodzaje komponentów systemu PE-16_ODP[01]>*** podlegają kontroli przy wejściu do obiektu; |

| | | |
|---|---|---|
| **PE-16** | **DOSTAWA I USUWANIE** | |
| | **PE-16a.[03]** | ***<rodzaje komponentów systemu PE-16_ODP[02]>*** podlegają zatwierdzeniu przy wyjściu z obiektu; |
| | **PE-16a.[04]** | ***<rodzaje komponentów systemu PE-16_ODP[02]>*** podlegają kontroli przy wyjściu z obiektu; |
| | **PE-16b.** | zapisy dotyczące komponentów systemu są przechowywane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-16-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące wnoszenia i wynoszenia komponentów systemu z obiektu; obiekt, w którym znajduje się system; ewidencja komponentów wnoszonych i wynoszonych z obiektu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-16-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę komponentów systemu wnoszonych i wynoszonych z obiektu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-16-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny zatwierdzania, monitorowania i kontroli elementów związanych z systemem wnoszonych i wynoszonych z obiektu; mechanizmy wspierające lub wdrażające, autoryzację, monitorowanie i kontrolę elementów związanych z systemem wnoszonych i wynoszonych z obiektu]. |

| | | |
|---|---|---|
| **PE-17** | **ZAPASOWE MIEJSCE PRACY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-17_ODP[01]** | ***określono zapasowe miejsca pracy, z których mogą korzystać pracownicy;*** |

| | | |
|---|---|---|
| **PE-17** | **ZAPASOWE MIEJSCE PRACY** | |
| | **PE-17_ODP[02]** | ***określono zabezpieczenia, które mają być stosowane w zapasowych miejscach pracy;*** |
| | **PE-17a.** | określono i udokumentowano ***<zapasowe miejsca pracy PE-17_ODP[01]>***; |
| | **PE-17b.** | w zapasowych miejscach pracy stosuje się ***<zabezpieczenia PE-17_ODP[02]>***; |
| | **PE-17c.** | skuteczność zabezpieczeń stosowanych w zapasowych miejscach pracy jest oceniana; |
| | **PE-17d.** | pracownikom zapewniono środki do komunikacji z personelem odpowiedzialnym za bezpieczeństwo i prywatność informacji w przypadku wystąpienia incydentów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-17-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące zapasowych miejsc pracy dla personelu organizacyjnego; lista zabezpieczeń wymaganych w zapasowych miejscach pracy; oceny zabezpieczeń w zapasowych miejscach pracy; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PE-17-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny zatwierdzający korzystanie z zapasowych miejsc pracy; personel organizacyjny korzystający z zapasowych miejsc pracy; personel organizacyjny oceniający zabezpieczenia w zapasowych miejscach pracy; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PE-17** | **ZAPASOWE MIEJSCE PRACY** | |
| | **PE-17-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące bezpieczeństwa i ochrony prywatności w zapasowych miejscach pracy; mechanizmy wspierające zapasowe miejsca pracy; środki kontroli bezpieczeństwa i ochrony prywatności stosowane w zapasowych miejscach pracy; środki komunikacji między personelem pracującym w zapasowych miejscach pracy a personelem odpowiedzialnym za bezpieczeństwo i ochronę prywatności]. |

| | | |
|---|---|---|
| **PE-18** | **LOKALIZACJA KOMPONENTÓW SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-18_ODP** | ***określono zagrożenia fizyczne i środowiskowe, które mogą spowodować uszkodzenie komponentów systemu w obiekcie;*** |
| | **PE-18** | komponenty systemu są rozmieszczone w obiekcie tak, aby zminimalizować potencjalne uszkodzenia spowodowane ***<zagrożeniami fizycznymi i środowiskowymi PE-18_ODP>*** oraz zminimalizować możliwość nieautoryzowanego dostępu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-18-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące rozmieszczenia komponentów systemu; dokumentacja określająca lokalizację i położenie komponentów systemu w obiekcie; położenie komponentów systemu w obiekcie; lista zagrożeń fizycznych i środowiskowych mogących uszkodzić komponenty systemu w obiekcie; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-18-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za rozmieszczenie komponentów systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **PE-18** | **LOKALIZACJA KOMPONENTÓW SYSTEMU** | |
| | **PE-18-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące rozmieszczenia komponentów systemu]. |

| | |
|---|---|
| **PE-18(01)** | **LOKALIZACJA KOMPONENTÓW SYSTEMU \| LOKALIZACJA OBIEKTU** |
| | [WYCOFANE: Włączone do PE-23]. |

| | | |
|---|---|---|
| **PE-19** | **ULOT INFORMACJI/ELEKTROMAGNETYCZNA EMISJA UJAWNIAJĄCA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-19** | system jest zabezpieczony przed ulotem informacji spowodowanym promieniowaniem sygnałów elektromagnetycznych, tzw. elektromagnetyczną emisją ujawniającą. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-19-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące promieniowania sygnałów elektromagnetycznych; mechanizmy zabezpieczające system przed promieniowaniem sygnałów elektronicznych; obiekt, w którym znajduje się system; zapisy z testów promieniowania sygnałów elektromagnetycznych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-19-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczenia środowiskowe systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-19-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub realizujące ochronę przed ulotem informacji w wyniku promieniowania sygnałów elektromagnetycznych]. |

| | | |
|---|---|---|
| **PE-19(01)** | **ULOT INFORMACJI/ELEKTROMAGNETYCZNA EMISJA UJAWNIAJĄCA\| KRAJOWE POLITYKI I PROCEDURY DOTYCZĄCE EMISJI UJAWNIAJĄCEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-19(01)[01]** | komponenty systemu są chronione zgodnie z krajowymi politykami i procedurami bezpieczeństwa emisji w oparciu o odpowiednią kategorię bezpieczeństwa lub klasyfikację informacji; |
| | **PE-19(01)[02]** | transmisje danych w tym zakresie są chronione zgodnie z krajową polityką i procedurami bezpieczeństwa emisji w oparciu o odpowiednią kategorię bezpieczeństwa lub klasyfikację informacji; |
| | **PE-19(01)[03]** | sieci chronione są zgodnie z krajowymi politykami i procedurami bezpieczeństwa emisji w oparciu o odpowiednią kategorię bezpieczeństwa lub klasyfikację informacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-19(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące ulotu informacji zgodne z krajowymi politykami i procedurami dotyczącymi emisji oraz TEMPEST; dokumentacja projektowa komponentów systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-19(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zabezpieczenia środowiskowe systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-19(01)-Test** | [WYBÓR SPOŚRÓD: Komponenty systemu informatycznego zapewniające zgodność z krajowymi politykami i procedurami dotyczącymi emisji oraz TEMPEST]. |

| | | |
|---|---|---|
| **PE-20** | **MONITOROWANIE I ŚLEDZENIE ZASOBÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-20_ODP[01]** | ***określono technologie lokalizacji zasobów, które mają być stosowane do śledzenia i monitorowania ich lokalizacji i ruchu;*** |
| | **PE-20_ODP[02]** | ***określono zasoby, których położenie i ruch podlega śledzeniu i monitorowaniu;*** |
| | **PE-20_ODP[03]** | ***określono obszary kontrolowane, w których lokalizacja i ruch zasobów podlega śledzeniu i monitorowaniu;*** |
| | **PE-20** | stosuje się ***<technologie lokalizacji zasobów PE-20_ODP[01]>*** do śledzenia i monitorowania lokalizacji i ruchu ***<zasobów PE-20_ODP[02]>*** w obrębie ***<obszarów kontrolowanych PE-20_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-20-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące monitorowania i śledzenia zasobów; dokumentacja wskazująca na zastosowanie technologii lokalizacji zasobów; dokumentacja konfiguracji systemu; lista aktywów organizacyjnych wymagających śledzenia i monitorowania; zapisy dotyczące monitorowania i śledzenia zasobów; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PE-20-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za monitorowanie i śledzenie zasobów; radca prawny; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PE-20-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące śledzenia i monitorowania zasobów; mechanizmy wspierające lub wdrażające śledzenie i monitorowanie zasobów]. |

| | | |
|---|---|---|
| **PE-21** | **OCHRONA PRZED IMPULSEM ELEKTROMAGNETYCZNYM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-21_ODP[01]** | ***określono środki ochrony przed impulsem elektromagnetycznym, które należy stosować;*** |
| | **PE-21_ODP[02]** | ***określono system i komponenty systemu wymagające ochrony przed impulsem elektromagnetycznym;*** |
| | **PE-21** | stosuje się ***<środki ochrony PE-21_ODP[01]>*** przed impulsem elektromagnetycznym dla ***<systemu i komponentów systemu PE-21_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-21-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące środków ochronnych zmniejszających ryzyko uszkodzenia systemów i komponentów przez EMP; dokumentacja zawierająca szczegóły dotyczące środków ochronnych zmniejszających ryzyko uszkodzenia przez EMP; lista lokalizacji, w których wdrożono środki ochronne zmniejszające ryzyko uszkodzenia przez EMP; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-21-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę fizyczną i środowiskową; programiści/integratorzy systemów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-21-Test** | [WYBÓR SPOŚRÓD: Mechanizmy ograniczające ryzyko uszkodzenia przez EMP]. |

| | | |
|---|---|---|
| **PE-22** | **ZNAKOWANIE KOMPONENTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-22_ODP** | ***określono komponenty sprzętowe systemu, których oznakowanie musi wskazywać poziom wpływu lub klasyfikację informacji, które mogą być przechowywane lub przekazywane przez dany komponent sprzętowy;*** |
| | **PE-22** | ***<PE-22_ODP komponenty sprzętowe systemu>*** są oznaczone wraz ze wskazaniem poziomu wpływu lub klasyfikacji informacji, które mogą być przetwarzane, przechowywane lub przekazywane przez komponent sprzętowy. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-22-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; procedury dotyczące oznaczania komponentów; lista atrybutów bezpieczeństwa związanych ze znakowaniem komponentów; spis komponentów; rodzaje informacji i ich wpływ/klasyfikacja; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-22-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za znakowanie komponentów; personel organizacyjny odpowiedzialny za inwentaryzację komponentów; personel organizacyjny odpowiedzialny za kategoryzację/klasyfikację informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-22-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące znakowania komponentów; automatyczne mechanizmy wspierające lub wdrażające znakowanie komponentów]. |

| | | |
|---|---|---|
| **PE-23** | **LOKALIZACJA OBIEKTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PE-23a.** | lokalizacja obiektu, w którym zostanie umieszczony system, jest zaplanowana z uwzględnieniem zagrożeń fizycznych i środowiskowych; |
| | **PE-23b.** | w przypadku istniejących obiektów zagrożenia fizyczne i środowiskowe są uwzględniane w strategii zarządzania ryzykiem organizacyjnym. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PE-23-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony fizycznej i środowiskowej; dokumenty dotyczące planowania fizycznego położenia obiektu; organizacyjna ocena ryzyka; plan awaryjny; dokumentacja strategii ograniczania ryzyka; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PE-23-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za wybór lokalizacji dla obiektu, w którym zostanie umieszczony system; personel organizacyjny odpowiedzialny za ograniczanie ryzyka; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PE-23-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie planowania przestrzennego]. |

## 4.12. KATEGORIA PL - PLANOWANIE

| | | |
|---|---|---|
| **PL-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PL-01_ODP[01]** | ***określono personel lub role, którym należy przekazać politykę planowania;*** |
| | **PL-01_ODP[02]** | ***określono personel lub role, którym należy przekazać procedury planowania;*** |
| | **PL-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **PL-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami planowania;*** |
| | **PL-01_ODP[05]** | ***określono częstotliwość, z jaką polityka planowania jest przeglądana i aktualizowana;*** |
| | **PL-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji polityki planowania;*** |
| | **PL-01_ODP[07]** | ***określono częstotliwość, z jaką aktualne procedury planowania są przeglądane i aktualizowane;*** |
| | **PL-01_ODP[08]** | ***definiowane są zdarzenia skutkujące koniecznością przeprowadzenia przeglądu i aktualizacji procedur;*** |
| | **PL-01a.[01]** | opracowano i udokumentowano politykę planowania. |
| | **PL-01a.[02]** | polityka planowania jest rozpowszechniana wśród ***<personelu lub ról PL-01_ODP[01]>***; |
| | **PL-01a.[03]** | opracowano i udokumentowano procedury planowania ułatwiające realizację polityki planowania i związanych z nią zabezpieczeń; |

| **PL-01** | **POLITYKA I PROCEDURY** | |
|---|---|---|
| | **PL-01a.[04]** | procedury planowania są rozpowszechniane wśród ***<personelu lub ról PL-01_ODP[02]>***; |
| | **PL-01a.01(a)[01]** | ***<WYBRANA WARTOŚĆ PARAMETRU PL-01_ODP[03]>*** polityki planowania odnosi się do celu; |
| | **PL-01a.01(a)[02]** | ***<WYBRANA WARTOŚĆ PARAMETRU PL-01_ODP[03]>*** polityki planowania odnosi się do zakresu; |
| | **PL-01a.01(a)[03]** | ***<WYBRANA WARTOŚĆ PARAMETRU PL-01_ODP[03]>*** polityki planowania odnosi się do ról; |
| | **PL-01a.01(a)[04]** | ***<WYBRANA WARTOŚĆ PARAMETRU PL-01_ODP[03]>*** polityki planowania odnosi się do obowiązków; |
| | **PL-01a.01(a)[05]** | ***<WYBRANA WARTOŚĆ PARAMETRU PL-01_ODP[03]>*** polityki planowania odnosi się do zaangażowania kierownictwa; |
| | **PL-01a.01(a)[06]** | ***<WYBRANA WARTOŚĆ PARAMETRU PL-01_ODP[03]>*** polityki planowania odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **PL-01a.01(a)[07]** | ***<WYBRANA WARTOŚĆ PARAMETRU PL-01_ODP[03]>*** polityki planowania odnosi się do zgodności; |
| | **PL-01a.01(b)** | polityka planowania ***<WYBRANA WARTOŚĆ PARAMETRU PL-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **PL-01b.** | ***<urzędnik PL-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur planowania; |
| | **PL-01c.01[01]** | aktualna polityka planowania jest analizowana i aktualizowana z ***<częstotliwością PL-01_ODP[05]>***; |

| | | |
|---|---|---|
| **PL-01** | **POLITYKA I PROCEDURY** | |
| | **PL-01c.01[02]** | aktualna polityka planowania jest analizowana i aktualizowana po ***<zdarzeniach PL-01_ODP[06]>***; |
| | **PL-01c.02[01]** | aktualne procedury planowania są analizowane i aktualizowane z ***<częstotliwością PL-01_ODP[07]>***; |
| | **PL-01c.02[02]** | aktualne procedury planowania są analizowane i aktualizowane po ***<zdarzeniach PL-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PL-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury planowania; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PL-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PL-02** | **PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PL-02_ODP[01]** | ***wyznaczono osoby lub grupy odpowiedzialne za realizacje zadań związanych z bezpieczeństwem i prywatnością, mających wpływ na system i wymagających planowania i koordynacji;*** |
| | **PL-02_ODP[02]** | ***wyznaczono personel lub role, które mają otrzymać kopie planów bezpieczeństwa i ochrony prywatności systemu;*** |
| | **PL-02_ODP[03]** | ***określono częstotliwość przeglądu planów bezpieczeństwa i ochrony prywatności systemu;*** |

| **PL-02** | **PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI** | |
|---|---|---|
| | **PL-02a.01[01]** | opracowano plan bezpieczeństwa systemu, który jest spójny z architekturą firmową organizacji; |
| | **PL-02a.01[02]** | opracowano plan ochrony prywatności systemu, który jest spójny z architekturą firmową organizacji; |
| | **PL-02a.02[01]** | opracowano plan ochrony prywatności systemu, który jest zgodny z architekturą firmową organizacji; |
| | **PL-02a.02[02]** | opracowano plan ochrony prywatności systemu, który jednoznacznie określa składowe komponenty systemu; |
| | **PL-02a.03[01]** | opracowano plan bezpieczeństwa systemu, który opisuje kontekst operacyjny systemu pod względem misji i procesów biznesowych; |
| | **PL-02a.03[02]** | opracowano plan ochrony prywatności systemu, który opisuje kontekst operacyjny systemu pod względem misji i procesów biznesowych; |
| | **PL-02a.04[01]** | opracowano plan bezpieczeństwa systemu, który określa osoby pełniące role i obowiązki w ramach systemu; |
| | **PL-02a.04[02]** | opracowano plan ochrony prywatności systemu, który określa osoby pełniące role i obowiązki w ramach systemu; |
| | **PL-02a.05[01]** | opracowano plan bezpieczeństwa systemu, który określa rodzaje informacji przetwarzanych, przechowywanych i przekazywanych przez system; |
| | **PL-02a.05[02]** | opracowano plan ochrony prywatności systemu, który określa rodzaje informacji przetwarzanych, przechowywanych i przekazywanych przez system; |
| | **PL-02a.06[01]** | opracowano plan bezpieczeństwa systemu, w którym przedstawiono klasyfikację systemu pod względem bezpieczeństwa, wraz z uzasadnieniem; |

| PL-02 | PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI | |
|---|---|---|
| | **PL-02a.06[02]** | opracowano plan ochrony prywatności systemu, który zawiera kategoryzację bezpieczeństwa systemu wraz z uzasadnieniem; |
| | **PL-02a.07[01]** | opracowano plan bezpieczeństwa systemu, który opisuje wszelkie szczególne zagrożenia dla systemu będące przedmiotem zainteresowania organizacji; |
| | **PL-02a.07[02]** | opracowano plan ochrony prywatności systemu, który opisuje wszelkie szczególne zagrożenia dla systemu będące przedmiotem zainteresowania organizacji; |
| | **PL-02a.08[01]** | opracowano plan bezpieczeństwa systemu, który zawiera wyniki oceny ryzyka w zakresie ochrony prywatności systemów przetwarzających dane identyfikacyjne; |
| | **PL-02a.08[02]** | opracowano plan bezpieczeństwa systemu, który zawiera wyniki oceny ryzyka w zakresie ochrony prywatności systemów przetwarzających dane identyfikacyjne; |
| | **PL-02a.09[01]** | opracowano plan bezpieczeństwa systemu, który opisuje środowisko operacyjne systemu oraz wszelkie zależności i połączenia z innymi systemami lub komponentami systemu; |
| | **PL-02a.09[02]** | opracowano plan ochrony prywatności systemu, który opisuje środowisko operacyjne systemu i wszelkie zależności lub połączenia z innymi systemami lub komponentami systemu; |
| | **PL-02a.10[01]** | opracowano plan bezpieczeństwa systemu, który zawiera przegląd wymagań dotyczących bezpieczeństwa systemu; |
| | **PL-02a.10[02]** | opracowano plan ochrony prywatności systemu, który zawiera przegląd wymagań dotyczących prywatności dla systemu; |
| | **PL-02a.11[01]** | opracowano plan bezpieczeństwa systemu, w którym określono wszelkie istotne zabezpieczenia bazowe lub nakładki, jeśli są stosowane; |

| PL-02 | PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI | |
|---|---|---|
| | **PL-02a.11[02]** | opracowano plan ochrony prywatności systemu, w którym określono wszelkie istotne zabezpieczenia bazowe lub nakładki, jeśli są stosowane; |
| | **PL-02a.12[01]** | opracowano plan bezpieczeństwa systemu, który opisuje istniejące lub planowane środki kontroli w celu spełnienia wymogów bezpieczeństwa, w tym uzasadnienie wszelkich decyzji dotyczących dostosowywania zabezpieczeń; |
| | **PL-02a.12[02]** | opracowano plan ochrony prywatności systemu, który opisuje istniejące lub planowane zabezpieczenia w celu spełnienia wymagań dotyczących ochrony prywatności, w tym uzasadnienie wszelkich decyzji dotyczących dostosowywania zabezpieczeń; |
| | **PL-02a.13[01]** | opracowano plan bezpieczeństwa systemu, który obejmuje określenie ryzyka dla architektury bezpieczeństwa i decyzji projektowych; |
| | **PL-02a.13[02]** | opracowano plan ochrony prywatności systemu, który obejmuje określenie ryzyka dla architektury prywatności i decyzji projektowych; |
| | **PL-02a.14[01]** | opracowano plan bezpieczeństwa systemu, obejmujący działania związane z bezpieczeństwem mające wpływ na system, które wymagają planowania i koordynacji z ***<osobami lub grupami PL-02_ODP[01]>***; |
| | **PL-02a.14[02]** | opracowano plan ochrony prywatności systemu, obejmujący działania związane z prywatnością wpływające na system, które wymagają planowania i koordynacji z ***<osobami lub grupami PL-02_ODP[01]>***; |
| | **PL-02a.15[01]** | opracowano plan bezpieczeństwa systemu, który jest przeglądany i zatwierdzany przez odpowiedniego urzędnika lub wyznaczonego przedstawiciela przed wdrożeniem; |
| | **PL-02a.15[02]** | opracowano plan ochrony prywatności systemu, który jest przeglądany i zatwierdzany przez odpowiedniego urzędnika lub wyznaczonego przedstawiciela przed wdrożeniem; |

| | | |
|---|---|---|
| **PL-02** | **PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI** | |
| | **PL-02b.[01]** | kopie planów są przekazywane ***<personelowi lub rolom PL-02_ODP[02]>***; |
| | **PL-02b.[02]** | kolejne zmiany w planach są przekazywane ***<personelowi lub rolom PL-02_ODP[02]>***; |
| | **PL-02c.** | plany są przeglądane z ***<częstotliwością PL-02_ODP[03]>***; |
| | **PL-02d.[01]** | plany są aktualizowane w celu uwzględnienia zmian w systemie i środowisku działania; |
| | **PL-02d.[02]** | plany są aktualizowane w celu rozwiązania problemów zidentyfikowanych podczas realizacji planu; |
| | **PL-02d.[03]** | plany są aktualizowane w celu rozwiązania problemów zidentyfikowanych podczas ocen kontrolnych; |
| | **PL-02e.[01]** | plany są chronione przed nieuprawnionym ujawnieniem; |
| | **PL-02e.[02]** | plany są chronione przed nieuprawnionymi zmianami; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PL-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania bezpieczeństwa i prywatności; procedury dotyczące opracowywania i wdrażania planu bezpieczeństwa i prywatności systemu; procedury dotyczące przeglądów i aktualizacji planu bezpieczeństwa i prywatności; dokumentacja architektury firmowej; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja przeglądów i aktualizacji planów bezpieczeństwa i prywatności systemu; dokumentacja dotycząca architektury i projektu w zakresie bezpieczeństwa i prywatności; oceny ryzyka; wyniki oceny ryzyka; dokumentacja dotycząca oceny kontroli; inne istotne dokumenty lub zapisy]. |
| | **PL-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację planu bezpieczeństwa i prywatności systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| PL-02 | PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI | |
|---|---|---|
| | **PL-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące opracowywania, przeglądu, aktualizacji i zatwierdzania planu bezpieczeństwa i prywatności systemu; mechanizmy wspierające plan bezpieczeństwa i prywatności systemu]. |

| PL-02(01) | PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI \| KONCEPCJA |
|---|---|
| | [WYCOFANE: Włączone do PL-07]. |

| PL-02(02) | PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI \| ARCHITEKTURA FUNKCJONALNA |
|---|---|
| | [WYCOFANE: Włączone do PL-08]. |

| PL-02(03) | PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI \| PLANOWANIE/KOORDYNACJA Z INNYMI PODMIOTAMI ORGANIZACYJNYMI |
|---|---|
| | [WYCOFANE: Włączone do PL-02]. |

| PL-03 | AKTUALIZACJA PLANU BEZPIECZEŃSTWA SYSTEMU |
|---|---|
| | [WYCOFANE: Włączone do PL-02]. |

| | | |
|---|---|---|
| **PL-04** | **ZASADY POSTĘPOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PL-04_ODP[01]** | ***określono częstotliwość przeglądów i aktualizacji zasad postępowania;*** |
| | **PL-04_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {<częstotliwość PL-04_ODP[03]>; przy zmianie lub aktualizacji przepisów};*** |
| | **PL-04_ODP[03]** | ***określono częstotliwość zapoznawania się przez poszczególne osoby z zasadami postępowania i ponownego ich podpisania (jeśli wybrano);*** |
| | **PL-04a.[01]** | dla osób wymagających dostępu do systemu ustalane są zasady opisujące ich obowiązki i oczekiwane postępowanie w zakresie korzystania z informacji i systemu, a także w zakresie bezpieczeństwa i prywatności; |
| | **PL-04a.[02]** | osobom wymagającym dostępu do systemu przekazuje się zasady opisujące ich obowiązki i oczekiwane postępowanie w zakresie korzystania z informacji i systemu, a także w zakresie bezpieczeństwa i prywatności; |
| | **PL-04b.** | przed udzieleniem dostępu do informacji i systemu od takich osób uzyskuje się udokumentowane potwierdzenie, że przeczytały, zrozumiały i zgadzają się przestrzegać zasad postępowania; |
| | **PL-04c.** | zasady postępowania są przeglądane i aktualizowane z ***<częstotliwością PL-04_ODP[01]>***; |
| | **PL-04d.** | osoby, które podpisały poprzednią wersję zasad postępowania, zobowiązane są do przeczytania i ponownego podpisania ***<WYBRANA WARTOŚĆ PARAMETRU PL-04_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| PL-04 | ZASADY POSTĘPOWANIA | |
|---|---|---|
| | **PL-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania bezpieczeństwa i prywatności; procedury dotyczące zasad postępowania przez użytkowników systemu; zasady postępowania; podpisane potwierdzenia; zapisy dotyczące przeglądów i aktualizacji zasad postępowania; inne istotne dokumenty lub zapisy]. |
| | **PL-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ustanowienie, przegląd i aktualizację zasad postępowania; personel organizacyjny odpowiedzialny za szkolenia w zakresie uświadamiania i bezpieczeństwa oraz szkolenia w zakresie bezpieczeństwa opartego na rolach; personel organizacyjny, który jest autoryzowanym użytkownikiem systemu i podpisał zasady postępowania po raz pierwszy lub po raz kolejny; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PL-04-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie ustanawiania, przeglądu, rozpowszechniania i aktualizacji zasad postępowania; mechanizmy wspierające lub realizujące ustanawianie, przegląd, rozpowszechnianie i aktualizację zasad postępowania]. |

| PL-04(01) | ZASADY POSTĘPOWANIA \| MEDIA SPOŁECZNOŚCIOWE I OGRANICZENIA KORZYSTANIA ZE STRON/APLIKACJI ZEWNĘTRZNYCH | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PL-04(01)(a)** | zasady postępowania obejmują ograniczenia w korzystaniu z mediów społecznościowych, portali społecznościowych oraz zewnętrznych stron/aplikacji; |
| | **PL-04(01)(b)** | zasady postępowania zawierają ograniczenia dotyczące umieszczania informacji organizacyjnych na publicznych stronach internetowych; |

| | | |
|---|---|---|
| **PL-04(01)** | **ZASADY POSTĘPOWANIA \| MEDIA SPOŁECZNOŚCIOWE I OGRANICZENIA KORZYSTANIA ZE STRON/APLIKACJI ZEWNĘTRZNYCH** | |
| | **PL-04(01)(c)** | zasady postępowania obejmują ograniczenia dotyczące wykorzystywania dostarczonych przez organizację identyfikatorów (np. adresów e-mail) i sekretów uwierzytelniania (np. haseł) do tworzenia kont na zewnętrznych stronach/aplikacjach. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PL-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania bezpieczeństwa i prywatności; procedury dotyczące zasad postępowania przez użytkowników systemu; zasady postępowania; polityka szkoleniowa; inne istotne dokumenty lub zapisy]. |
| | **PL-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ustanowienie, przegląd i aktualizację zasad postępowania; personel organizacyjny odpowiedzialny za szkolenia w zakresie uświadamiania i bezpieczeństwa oraz szkolenia w zakresie bezpieczeństwa opartego na rolach; personel organizacyjny, który jest autoryzowanym użytkownikiem systemu i podpisał zasady postępowania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PL-04(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne ustanawiające zasady postępowania; mechanizmy wspierające lub wdrażające ustanawianie zasad postępowania]. |

| | |
|---|---|
| **PL-05** | **OCENA WPŁYWU NA PRYWATNOŚĆ** |
| | [WYCOFANE: Włączone do RA-08]. |

| | |
|---|---|
| **PL-06** | **PLANOWANIE DZIAŁALNOŚCI ZWIĄZANEJ Z BEZPIECZEŃSTWEM** |
| | [WYCOFANE: Włączone do PL-02]. |

| | | |
|---|---|---|
| **PL-07** | **KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PL-07_ODP** | ***określono częstotliwość przeglądu i aktualizacji koncepcji działań operacyjnych (CONOPS);*** |
| | **PL-07a.** | opracowano koncepcję CONOPS dla systemu opisującą, jak organizacja zamierza eksploatować system z punktu widzenia bezpieczeństwa i prywatności informacji; |
| | **PL-07b.** | CONOPS podlega przeglądowi i aktualizacji z ***<częstotliwością PL-07_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PL-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania bezpieczeństwa i prywatności; procedury dotyczące opracowania CONOPS dot. bezpieczeństwa i prywatności; procedury dotyczące przeglądów i aktualizacji CONOPS dot. bezpieczeństwa i prywatności; CONOPS dot. bezpieczeństwa i prywatności dla systemu; plan bezpieczeństwa systemu; plan prywatności; zapisy przeglądów i aktualizacji CONOPS dot. bezpieczeństwa i prywatności; inne istotne dokumenty lub zapisy]. |
| | **PL-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację planu w zakresie bezpieczeństwa i prywatności; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PL-07-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące opracowywania, przeglądu i aktualizacji CONOPS dot. bezpieczeństwa; mechanizmy wspierające lub wdrażające opracowywanie, przegląd i aktualizację CONOPS dot. bezpieczeństwa]. |

| | | |
|---|---|---|
| **PL-08** | **ARCHITEKTURY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PL-08_ODP** | ***częstotliwość przeglądów i aktualizacji w celu odzwierciedlenia zmian w architekturze organizacyjnej;*** |
| | **PL-08a.01** | architektura bezpieczeństwa systemu opisuje wymagania i podejście, jakie należy przyjąć w celu ochrony poufności, integralności i dostępności informacji organizacyjnych; |
| | **PL-08a.02** | architektura prywatności opisuje wymogi i podejście, jakie należy przyjąć przy przetwarzaniu danych identyfikacyjnych, aby zminimalizować ryzyko utraty prywatności przez osoby fizyczne; |
| | **PL-08a.03[01]** | architektura bezpieczeństwa systemu opisuje sposób, w jaki jest zintegrowana z architekturą organizacyjną oraz jak ją wspiera; |
| | **PL-08a.03[02]** | architektura prywatności systemu opisuje sposób, w jaki jest zintegrowana z architekturą organizacyjną oraz jak ją wspiera; |
| | **PL-08a.04[01]** | architektura bezpieczeństwa systemu opisuje wszelkie założenia dotyczące zewnętrznych systemów i usług oraz zależności od nich; |
| | **PL-08a.04[02]** | architektura prywatności systemu opisuje wszelkie założenia dotyczące zewnętrznych systemów i usług oraz zależności od nich; |
| | **PL-08b.** | zmiany w architekturze organizacji są przeglądane i aktualizowane z ***<częstotliwością PL-08_ODP>*** w celu odzwierciedlenia zmian w jej architekturze; |
| | **PL-08c.[01]** | planowane zmiany architektury są odzwierciedlone w planie bezpieczeństwa; |
| | **PL-08c.[02]** | planowane zmiany architektury są odzwierciedlone w planie prywatności; |
| | **PL-08c.[03]** | planowane zmiany architektury są odzwierciedlone w CONOPS; |

| | | |
|---|---|---|
| **PL-08** | **ARCHITEKTURY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **PL-08c.[04]** | planowane zmiany architektury są odzwierciedlone w analizie krytyczności; |
| | **PL-08c.[05]** | planowane zmiany architektury są odzwierciedlone w procedurach organizacyjnych; |
| | **PL-08c.[06]** | planowane zmiany architektury są odzwierciedlone w zamówieniach i zakupach organizacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PL-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania bezpieczeństwa i prywatności; procedury dotyczące rozwoju architektury bezpieczeństwa i prywatności informacji; procedury dotyczące przeglądów i aktualizacji architektury bezpieczeństwa informacji i prywatności; dokumentacja architektury organizacyjnej; dokumentacja architektury bezpieczeństwa i prywatności informacji; plan bezpieczeństwa systemu; plan ochrony prywatności; CONOPS dla systemu; zapisy dotyczące przeglądów i aktualizacji architektury bezpieczeństwa i prywatności informacji; inne istotne dokumenty lub zapisy]. |
| | **PL-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację planu bezpieczeństwa i prywatności; personel organizacyjny odpowiedzialny za rozwój architektury bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PL-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące opracowywania, przeglądu i aktualizacji architektury bezpieczeństwa i prywatności informacji; mechanizmy wspierające lub wdrażające opracowywanie, przegląd i aktualizację architektury bezpieczeństwa i prywatności informacji]. |

| | | |
|---|---|---|
| **PL-08(01)** | **ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZABEZPIECZENIE WIELOSTOPNIOWE (OCHRONA WARSTWOWA)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PL-08(01)_ODP[01]** | ***określono zabezpieczenia, które mają być przydzielone;*** |
| | **PL-08(01)_ODP[02]** | ***określono lokalizacje i warstwy architektury;*** |
| | **PL-08(01)(a)[01]** | architektura bezpieczeństwa systemu jest zaprojektowana z wykorzystaniem podejścia opartego na ochronie warstwowej, które przypisuje ***<zabezpieczenia PL-08(01)_ODP[01]>*** do ***<lokalizacji i warstw architektury PL-08(01)_ODP[02]>***; |
| | **PL-08(01)(a)[02]** | architektura prywatności systemu jest zaprojektowana z wykorzystaniem podejścia opartego na ochronie warstwowej, które przypisuje ***<zabezpieczenia PL-08(01)_ODP[01]>*** do ***<lokalizacji i warstw architektury PL-08(01)_ODP[02]>***; |
| | **PL-08(01)(b)[01]** | architektura bezpieczeństwa systemu jest zaprojektowana z wykorzystaniem podejścia ochrony warstwowej, które zapewnia, że przydzielone zabezpieczenia działają w sposób skoordynowany i wzajemnie się uzupełniają; |
| | **PL-08(01)(b)[02]** | architektura prywatności systemu jest zaprojektowana z wykorzystaniem podejścia ochrony warstwowej, które zapewnia, że przydzielone zabezpieczenia działają w sposób skoordynowany i wzajemnie się uzupełniają. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PL-08(01)** | **ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZABEZPIECZENIE WIELOSTOPNIOWE (OCHRONA WARSTWOWA)** | |
| | **PL-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania bezpieczeństwa i prywatności; procedury dotyczące rozwoju architektury bezpieczeństwa i prywatności informacji; dokumentacja architektury organizacyjnej; dokumentacja architektury bezpieczeństwa i prywatności informacji; plan bezpieczeństwa systemu; plan ochrony prywatności; CONOPS dla systemu dot. bezpieczeństwa i prywatności; inne istotne dokumenty lub zapisy]. |
| | **PL-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację planu bezpieczeństwa i prywatności; personel organizacyjny odpowiedzialny za rozwój architektury bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PL-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne związane z projektowaniem architektury bezpieczeństwa i prywatności informacji; mechanizmy wspierające lub wdrażające projekt architektury bezpieczeństwa i prywatności informacji]. |

| | | |
|---|---|---|
| **PL-08(02)** | **ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| DYWERSYFIKACJA DOSTAWCY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PL-08(02)_ODP[01]** | ***określono zabezpieczenia, które mają być przydzielone;*** |
| | **PL-08(02)_ODP[02]** | ***określono lokalizacje i warstwy architektury;*** |

| | | |
|---|---|---|
| **PL-08(02)** | **ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| DYWERSYFIKACJA DOSTAWCY** | |
| | **PL-08(02)** | ***<zabezpieczenia PL-08(02)_ODP[01]>***, które są przypisane do ***<lokalizacji i warstw architektury PL-08(02)_ODP[02]>***, muszą być uzyskane od różnych dostawców. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PL-08(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania bezpieczeństwa i prywatności; procedury dotyczące rozwoju architektury bezpieczeństwa i prywatności informacji; dokumentacja architektury organizacyjnej; dokumentacja architektury bezpieczeństwa i prywatności informacji; plan bezpieczeństwa systemu; plan ochrony prywatności; CONOPS dla systemu dot. bezpieczeństwa i prywatności; polityka zakupów w obszarze informatyki; inne istotne dokumenty lub zapisy]. |
| | **PL-08(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację planu bezpieczeństwa i prywatności; personel organizacyjny odpowiedzialny za rozwój architektury bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za pozyskiwanie informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PL-08(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie pozyskiwania zabezpieczeń zapewniających bezpieczeństwo informacji i ochronę prywatności od różnych dostawców]. |

| | | |
|---|---|---|
| **PL-09** | **ZARZĄDZANIE CENTRALNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PL-09_ODP** | ***określono środki kontroli bezpieczeństwa i prywatności oraz powiązane procesy, które mają być zarządzane centralnie;*** |

| | | |
|---|---|---|
| **PL-09** | **ZARZĄDZANIE CENTRALNE** | |
| | **PL-09** | ***<zabezpieczenia i powiązane procesy PL-09_ODP>*** są zarządzane centralnie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PL-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania bezpieczeństwa i prywatności; procedury dotyczące opracowywania i wdrażania planu bezpieczeństwa i prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PL-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację planu w zakresie bezpieczeństwa i prywatności; personel organizacyjny odpowiedzialny za planowanie/wdrażanie centralnego zarządzania zabezpieczeniami i powiązanymi procesami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PL-09-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące centralnego zarządzania zabezpieczeniami i procesami powiązanymi; mechanizmy wspierające lub wdrażające centralne zarządzanie zabezpieczeniami i powiązanymi procesami]. |

| | | |
|---|---|---|
| **PL-10** | **WYBÓR ZABEZPIECZEŃ BAZOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PL-10** | wybrano zabezpieczenia bazowe dla systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PL-10** | **WYBÓR ZABEZPIECZEŃ BAZOWYCH** | |
| | **PL-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania bezpieczeństwa i prywatności; procedury dotyczące opracowania i wdrożenia planu bezpieczeństwa i prywatności systemu; procedury dotyczące przeglądów i aktualizacji planu bezpieczeństwa i prywatności systemu; dokumentacja projektu systemu; dokumentacja architektury i konfiguracji systemu; decyzja o kategoryzacji systemu; rodzaje informacji przechowywanych, przesyłanych i przetwarzanych przez system; informacje o elementach/komponentach systemu; analiza potrzeb zainteresowanych stron; lista wymogów dotyczących bezpieczeństwa i prywatności przypisanych do systemu, elementów systemu i środowiska działania; lista wymogów umownych przypisanych zewnętrznym dostawcom systemu lub jego elementów; analiza wpływu na działalność lub analiza krytyczności; oceny ryzyka; strategia zarządzania ryzykiem; organizacyjna polityka bezpieczeństwa i prywatności; zatwierdzone lub obowiązkowe zabezpieczenia bazowe lub nakładki rządowe bądź organizacyjne; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PL-10-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację planu bezpieczeństwa i prywatności; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za działania w zakresie zarządzania ryzykiem organizacyjnym]. |

| | | |
|---|---|---|
| **PL-11** | **DOSTOSOWYWANIE ZABEZPIECZEŃ BAZOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PL-11** | wybrane zabezpieczenia bazowe są dostosowywane poprzez określone działania dostosowawcze. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **PL-11** | **DOSTOSOWYWANIE ZABEZPIECZEŃ BAZOWYCH** | |
|---|---|---|
| | **PL-11-Badanie** | [WYBÓR SPOŚRÓD: Polityka planowania bezpieczeństwa i prywatności; procedury dotyczące opracowywania i wdrażania planu bezpieczeństwa i prywatności systemu; dokumentacja projektowa systemu; decyzja dotycząca kategoryzacji systemu; rodzaje informacji przechowywanych, przesyłanych i przetwarzanych przez system; informacje o elementach/komponentach systemu;<br><br>analiza potrzeb zainteresowanych stron; lista wymogów dotyczących bezpieczeństwa i prywatności przypisanych do systemu, jego elementów i środowiska działania;<br><br>lista wymogów dotyczących bezpieczeństwa i prywatności przypisanych do systemu, jego elementów i środowiska działania; lista wymogów umownych przypisanych do zewnętrznych dostawców systemu lub elementów systemu; analiza wpływu biznesowego lub analiza krytyczności; oceny ryzyka; strategia zarządzania ryzykiem; organizacyjna polityka bezpieczeństwa i prywatności;<br><br>organizacyjna polityka bezpieczeństwa i prywatności; obowiązkowe lub zatwierdzone przez rząd zabezpieczenia bazowe bądź nakładki; uzasadnienie dostosowania zabezpieczeń bazowych; plan bezpieczeństwa systemu; plan ochrony prywatności; zapisy dotyczące przeglądów i aktualizacji planu bezpieczeństwa i ochrony prywatności systemu; inne istotne dokumenty lub zapisy]. |
| | **PL-11-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację planu w zakresie bezpieczeństwa i prywatności; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

## 4.13. KATEGORIA PM - PROGRAMY ZARZĄDZANIA

| | | |
|---|---|---|
| **PM-01** | **PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-01-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; procedury dotyczące opracowania i realizacji planu programu; procedury dotyczące przeglądów i aktualizacji planu programu; procedury dotyczące koordynacji planu programu z odpowiednimi podmiotami; procedury zatwierdzania planu programu; zapisy dotyczące przeglądów i aktualizacji planu programu; inne istotne dokumenty lub zapisy]. |
| | **PM-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PM-01-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące opracowywania, przeglądu, aktualizacji i zatwierdzania planu programu bezpieczeństwa informacji; mechanizmy wspierające lub wdrażające plan programu bezpieczeństwa informacji]. |

| | | |
|---|---|---|
| **PM-02** | **ROLE KIEROWNICZE PROGRAMU BEZPIECZEŃSTWA INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-02[01]** | mianowany jest wyższy urzędnik ds. bezpieczeństwa informacji; |
| | **PM-02[02]** | wyższy urzędnik ds. bezpieczeństwa informacji otrzymuje zadanie koordynowania programu bezpieczeństwa informacji w całej organizacji oraz odpowiednie zasoby do tego celu; |

| PM-02 | ROLE KIEROWNICZE PROGRAMU BEZPIECZEŃSTWA INFORMACJI | |
|---|---|---|
| | **PM-02[03]** | wyższy urzędnik ds. bezpieczeństwa informacji otrzymuje zadanie opracowania programu bezpieczeństwa informacji w całej organizacji oraz odpowiednie zasoby do tego celu; |
| | **PM-02[04]** | wyższy urzędnik ds. bezpieczeństwa informacji otrzymuje zadanie wdrożenia programu bezpieczeństwa informacji w całej organizacji oraz odpowiednie zasoby do tego celu; |
| | **PM-02[05]** | wyższy urzędnik ds. bezpieczeństwa informacji otrzymuje zadanie utrzymania programu bezpieczeństwa informacji w całej organizacji oraz odpowiednie zasoby do tego celu; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-02-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; procedury dotyczące opracowania i wdrożenia planu programu; procedury dotyczące przeglądów i aktualizacji planu programu; procedury dotyczące koordynacji planu programu z odpowiednimi podmiotami; inne istotne dokumenty lub zapisy]. |
| | **PM-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa informacji; wyższy urzędnik ds. bezpieczeństwa informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| PM-03 | ZASOBY W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI I OCHRONY PRYWATNOŚCI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-03a.[01]** | zasoby potrzebne do wdrożenia programu bezpieczeństwa informacji są uwzględniane w planowaniu kapitałowym i wnioskach inwestycyjnych, a wszystkie wyjątki są dokumentowane; |

| | | |
|---|---|---|
| **PM-03** | **ZASOBY W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI I OCHRONY PRYWATNOŚCI** | |
| | **PM-03a.[02]** | zasoby potrzebne do wdrożenia programu ochrony prywatności są uwzględniane w planowaniu kapitałowym i wnioskach inwestycyjnych, a wszystkie wyjątki są dokumentowane; |
| | **PM-03b.[01]** | dokumentacja wymagana do uwzględnienia programu bezpieczeństwa informacji w planowaniu kapitałowym i wnioskach inwestycyjnych jest sporządzania zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami i normami; |
| | **PM-03b.[02]** | dokumentacja wymagana do uwzględnienia programu ochrony prywatności w planowaniu kapitałowym i wnioskach inwestycyjnych jest sporządzania zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami i normami; |
| | **PM-03c.[01]** | środki na zapewnienie bezpieczeństwa informacji są udostępniane do wydatkowania zgodnie z planem; |
| | **PM-03c.[02]** | środki na zapewnienie prywatności są udostępniane do wydatkowania zgodnie z planem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-03-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; Załącznik 300; Załącznik 53; analizy przypadków dla planowania i inwestycji kapitałowych; procedury planowania i inwestycji kapitałowych; dokumentacja wyjątków od wymogów w zakresie planowania kapitałowego; inne istotne dokumenty lub zapisy]. |

| PM-03 | ZASOBY W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI I OCHRONY PRYWATNOŚCI | |
|---|---|---|
| | **PM-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie programu bezpieczeństwa informacji; personel organizacyjny odpowiedzialny za planowanie programu ochrony prywatności; personel organizacyjny odpowiedzialny za planowanie i inwestycje kapitałowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę prywatności]. |
| | **PM-03-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie planowania i inwestowania kapitałowego; procesy organizacyjne w zakresie analiz przypadków, Załącznik 300, Załącznik 53; mechanizmy wspierające proces planowania i inwestowania kapitałowego]. |

| PM-04 | PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-04a.01[01]** | istnieje proces zapewniający opracowanie planów działania i etapów wprowadzania zabezpieczeń dla programu bezpieczeństwa informacji i powiązanych systemów organizacyjnych; |
| | **PM-04a.01[02]** | istnieje proces zapewniający utrzymanie planów działania i etapów wprowadzania zabezpieczeń dla programu bezpieczeństwa informacji i powiązanych systemów organizacyjnych; |
| | **PM-04a.01[03]** | istnieje proces zapewniający opracowanie planów działania i etapów wprowadzania zabezpieczeń dla programu ochrony prywatności i powiązanych systemów organizacyjnych; |
| | **PM-04a.01[04]** | istnieje proces zapewniający utrzymanie planów działania i etapów wprowadzania zabezpieczeń dla programu ochrony prywatności i powiązanych systemów organizacyjnych; |

| PM-04 | PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ | |
|---|---|---|
| | **PM-04a.01[05]** | istnieje proces zapewniający opracowanie planów działania i etapów wprowadzania zabezpieczeń w zakresie ryzyka w łańcuchach dostaw i powiązanych systemów organizacyjnych; |
| | **PM-04a.01[06]** | istnieje proces zapewniający utrzymanie planów działania i etapów wprowadzania zabezpieczeń w zakresie ryzyka w łańcuchach dostaw i powiązanych systemów organizacyjnych; |
| | **PM-04a.02[01]** | istnieje proces zapewniający, że plany działania i etapy wprowadzania zabezpieczeń dla programu bezpieczeństwa informacji i powiązanych systemów organizacyjnych dokumentują działania zaradcze w zakresie zarządzania ryzykiem dot. bezpieczeństwa informacji w celu odpowiedniego reagowania na zagrożenia dla działań i aktywów organizacyjnych, osób, innych organizacji i bezpieczeństwa narodowego; |
| | **PM-04a.02[02]** | istnieje proces zapewniający, że plany działania i etapy wprowadzania zabezpieczeń dla programu bezpieczeństwa informacji i powiązanych systemów organizacyjnych dokumentują działania zaradcze w zakresie zarządzania ryzykiem dot. ochrony prywatności w celu odpowiedniego reagowania na zagrożenia dla działań i aktywów organizacyjnych, osób, innych organizacji i bezpieczeństwa narodowego; |
| | **PM-04a.02[03]** | istnieje proces zapewniający, że plany działania i etapy wprowadzania zabezpieczeń dla programu zarządzania ryzykiem łańcucha dostaw i powiązanych systemów organizacyjnych dokumentują działania naprawcze w zakresie zarządzania ryzykiem łańcucha dostaw w celu odpowiedniego reagowania na zagrożenia dla działań i aktywów organizacji, osób, innych organizacji i bezpieczeństwa narodowego; |
| | **PM-04a.03[01]** | istnieje proces zapewniający, że plany działania i etapy wprowadzania zabezpieczeń dla programów zarządzania ryzykiem w zakresie bezpieczeństwa informacji i powiązanych systemów organizacyjnych są zgłaszane zgodnie z ustalonymi wymogami sprawozdawczymi; |

| | | |
|---|---|---|
| **PM-04** | **PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ** | |
| | **PM-04a.03[02]** | istnieje proces zapewniający, że plany działania i etapy wprowadzania zabezpieczeń dla programów zarządzania ryzykiem łańcucha dostaw i powiązanych systemach organizacyjnych są zgłaszane zgodnie z ustalonymi wymogami sprawozdawczymi; |
| | **PM-04a.03[03]** | istnieje proces zapewniający, że plany działania i etapy wprowadzania zabezpieczeń dla programów zarządzania ryzykiem łańcucha dostaw i powiązanych systemach organizacyjnych są zgłaszane zgodnie z ustalonymi wymogami sprawozdawczymi; |
| | **PM-04b.[01]** | plany działania i etapy wprowadzania zabezpieczeń są weryfikowane pod kątem spójności z organizacyjną strategią reagowania na ryzyko. |
| | **PM-04b.[02]** | plany działania i etapy wprowadzania zabezpieczeń są weryfikowane pod kątem spójności z priorytetami działań organizacji w obszarze reagowania na ryzyko. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-04-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plany działań i etapy wprowadzania zabezpieczeń; procedury dotyczące opracowywania i utrzymywania planów działań i etapów wprowadzania zabezpieczeń; procedury dotyczące sprawozdawczości z planów działań i etapów wprowadzania zabezpieczeń; procedury przeglądu planów działań i etapów wprowadzania zabezpieczeń pod kątem spójności ze strategią zarządzania ryzykiem i priorytetami w zakresie reagowania na ryzyko;<br><br>wyniki ocen ryzyka związanych z planami działań i etapami wprowadzania zabezpieczeń; krajowe wymogi dotyczące sprawozdawczości w zakresie bezpieczeństwa systemów informatycznych; inne istotne dokumenty lub zapisy]. |
| | **PM-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za opracowanie, utrzymanie, przegląd i sprawozdawczość w zakresie planów działania i etapów wprowadzania zabezpieczeń; personel |

| | | |
|---|---|---|
| **PM-04** | **PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ** | |
| | | organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PM-04-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dot. opracowywania, utrzymywania, przeglądu i sprawozdawczości w zakresie planów działania i etapów wprowadzania zabezpieczeń; mechanizmy wspierające plany działania i etapy wprowadzania zabezpieczeń]. |

| | | |
|---|---|---|
| **PM-05** | **INWENTARYZACJA SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-05_ODP** | ***określono częstotliwość, z jaką należy aktualizować spis systemów organizacyjnych;*** |
| | **PM-05[01]** | opracowano wykaz systemów organizacyjnych; |
| | **PM-05[02]** | wykaz systemów organizacyjnych jest aktualizowany z ***<częstotliwością PM-05_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-05-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; wykaz systemów; procedury dotyczące opracowywania i utrzymywania wykazu systemów; krajowe wytyczne dotyczące sprawozdawczości w zakresie bezpieczeństwa systemów informatycznych; inne istotne dokumenty lub zapisy]. |
| | **PM-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa informacji; personel organizacyjny odpowiedzialny za opracowanie i utrzymanie wykazu systemów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **PM-05** | **INWENTARYZACJA SYSTEMU** | |
| | **PM-05-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie rozwoju i prowadzenia wykazu systemów; mechanizmy wspierające prowadzenie wykazu systemów]. |

| | | |
|---|---|---|
| **PM-05(01)** | **INWENTARYZACJA SYSTEMU \| SPIS DANYCH OSOBOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-05(01)_ODP** | ***określono częstotliwość aktualizacji wykazu systemów, aplikacji i projektów, w których przetwarzane są dane identyfikacyjne;*** |
| | **PM-05(01)[01]** | sporządzono wykaz wszystkich systemów, aplikacji i projektów, które przetwarzają dane identyfikacyjne; |
| | **PM-05(01)[02]** | prowadzony jest wykaz wszystkich systemów, aplikacji i projektów, które przetwarzają dane identyfikacyjne; |
| | **PM-05(01)[03]** | wykaz wszystkich systemów, aplikacji i projektów, w których przetwarzane są dane identyfikacyjne, jest aktualizowany z ***<częstotliwością PM-05(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-05(01)-Badanie** | [WYBÓR SPOŚRÓD: Procedury dotyczące wykazu systemów, ich utrzymania i aktualizacji; krajowe wytyczne dotyczące sprawozdawczości w zakresie bezpieczeństwa systemów informatycznych; plan programu ochrony prywatności; plan programu bezpieczeństwa informacji; polityka przetwarzania danych identyfikacyjnych; wykaz systemów; wykaz danych identyfikacyjnych; dokumentacja dotycząca mapowania danych; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PM-05(01)** | **INWENTARYZACJA SYSTEMU \| SPIS DANYCH OSOBOWYCH** | |
| | **PM-05(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu ochrony prywatności; personel organizacyjny odpowiedzialny za opracowanie i utrzymanie wykazu systemów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PM-05(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie opracowywania, utrzymania i aktualizacji wykazu systemów; mechanizmy wspierające prowadzenie wykazu systemów]. |

| | | |
|---|---|---|
| **PM-06** | **MIARY SKUTECZNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-06[01]** | opracowano miary skuteczności w zakresie bezpieczeństwa informacji; |
| | **PM-06[02]** | monitorowane są miary skuteczności w zakresie bezpieczeństwa informacji; |
| | **PM-06[03]** | podawane są wyniki dot. miar skuteczności w zakresie bezpieczeństwa informacji; |
| | **PM-06[04]** | opracowano miary skuteczności w zakresie ochrony prywatności; |
| | **PM-06[05]** | monitorowane są miary skuteczności w zakresie ochrony prywatności; |
| | **PM-06[06]** | podawane są wyniki dot. miar skuteczności w zakresie ochrony prywatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **PM-06** | **MIARY SKUTECZNOŚCI** | |
|---|---|---|
| | **PM-06-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; miary skuteczności w zakresie bezpieczeństwa informacji; miary skuteczności w zakresie ochrony prywatności; procedury dotyczące opracowywania, monitorowania i raportowania miar skuteczności w zakresie bezpieczeństwa informacji i ochrony prywatności; strategia zarządzania ryzykiem; inne istotne dokumenty lub zapisy]. |
| | **PM-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie programu bezpieczeństwa i prywatności informacji oraz realizację planu; personel organizacyjny odpowiedzialny za opracowanie, monitorowanie i raportowanie miar skuteczności działania w zakresie bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PM-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące opracowywania, monitorowania i raportowania miar skuteczności działania w zakresie bezpieczeństwa i prywatności informacji;<br>mechanizmy wspierające opracowywanie, monitorowanie i raportowanie miar skuteczności działania w zakresie bezpieczeństwa i prywatności informacji]. |

| **PM-07** | **STRUKTURA ORGANIZACYJNA** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-07[01]** | architekturę organizacyjną opracowano z uwzględnieniem kwestii bezpieczeństwa informacji; |
| | **PM-07[02]** | utrzymuje się architekturę organizacyjną uwzględniającą kwestię bezpieczeństwa informacji; |

| | | |
|---|---|---|
| **PM-07** | **STRUKTURA ORGANIZACYJNA** | |
| | **PM-07[03]** | architekturę organizacyjną opracowano z uwzględnieniem kwestii prywatności; |
| | **PM-07[04]** | utrzymuje się architekturę organizacyjną uwzględniającą kwestię prywatności; |
| | **PM-07[05]** | architekturę organizacyjną opracowano z uwzględnieniem wynikającego z niej ryzyka dla działań i majątku samej organizacji, osób, innych organizacji i bezpieczeństwa narodowego; |
| | **PM-07[06]** | architektura organizacyjna jest utrzymywana z uwzględnieniem wynikającego z niej ryzyka dla działań i aktywów samej organizacji, osób, innych organizacji i bezpieczeństwa narodowego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-07-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; dokumentacja architektury organizacyjnej; procedury dotyczące rozwoju architektury organizacyjnej; wyniki ocen ryzyka architektury organizacyjnej; inne istotne dokumenty lub zapisy]. |
| | **PM-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za rozwój architektury organizacyjnej; personel organizacyjny odpowiedzialny za ocenę ryzyka dla architektury organizacyjnej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PM-07-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie rozwoju architektury organizacyjnej; mechanizmy wspierające architekturę organizacyjną i jej rozwój]. |

| | | |
|---|---|---|
| **PM-07(01)** | **ARCHITEKTURA PRZEDSIĘBIORSTWA \| ODCIĄŻENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-07(01)_ODP** | ***określono niekrytyczne funkcje lub usługi, które mają być przeniesione do innego systemu w ramach odciążania;*** |
| | **PM-07(01)** | ***<niekrytyczne funkcje lub usługi PM-07(01)_ODP >*** zostały przeniesione do innego systemu, komponentów systemu lub zewnętrznego dostawcy w ramach odciążania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-07(01)-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; dokumentacja architektury organizacyjnej; procedury dotyczące rozwoju architektury organizacyjnej; procedury identyfikacji i przeniesienia funkcji lub usług do innego systemu w ramach odciążania; wyniki ocen ryzyka dla architektury organizacyjnej; inne istotne dokumenty lub zapisy]. |
| | **PM-07(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za rozwój architektury organizacyjnej; personel organizacyjny odpowiedzialny za ocenę ryzyka dla architektury organizacyjnej; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PM-07(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie rozwoju architektury organizacyjnej; mechanizmy wspierające architekturę organizacyjną i jej rozwój; mechanizmy służące do przenoszenia funkcji i usług do innego systemu w ramach odciążania]. |

| | | |
|---|---|---|
| **PM-08** | **PLAN INFRASTRUKTURY KRYTYCZNEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-08[01]** | opracowany plan ochrony infrastruktury krytycznej i kluczowych zasobów odnosi się do kwestii bezpieczeństwa informacji; |
| | **PM-08[02]** | dokumentacja planu ochrony infrastruktury krytycznej i kluczowych zasobów uwzględnia kwestie bezpieczeństwa informacji; |
| | **PM-08[03]** | aktualizacja planu ochrony infrastruktury krytycznej i kluczowych zasobów odnosi się do kwestii bezpieczeństwa informacji; |
| | **PM-08[04]** | podczas opracowywania planu ochrony infrastruktury krytycznej i kluczowych zasobów uwzględniane są kwestie ochrony prywatności; |
| | **PM-08[05]** | dokumentacja planu ochrony infrastruktury krytycznej i kluczowych zasobów uwzględnia kwestie ochrony prywatności; |
| | **PM-08[06]** | aktualizacja planu ochrony infrastruktury krytycznej i kluczowych zasobów odnosi się do kwestii ochrony prywatności; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-08-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; plan ochrony infrastruktury krytycznej i kluczowych zasobów; procedury dotyczące opracowywania, dokumentowania i aktualizacji planu ochrony infrastruktury krytycznej i kluczowych zasobów; krajowe przepisy dotyczące ochrony infrastruktury krytycznej; krajowy plan ochrony infrastruktury; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PM-08** | **PLAN INFRASTRUKTURY KRYTYCZNEJ** | |
| | **PM-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za opracowywanie, dokumentowanie i aktualizację planu ochrony infrastruktury krytycznej i kluczowych zasobów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PM-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące opracowywania, dokumentowania i aktualizacji planu ochrony infrastruktury krytycznej i kluczowych zasobów; mechanizmy wspierające opracowywanie, dokumentowanie i aktualizację planu ochrony infrastruktury krytycznej i kluczowych zasobów]. |

| | | |
|---|---|---|
| **PM-09** | **STRATEGIA ZARZĄDZANIA RYZYKIEM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-09_ODP** | ***określono częstotliwość przeglądu i aktualizacji strategii zarządzania ryzykiem;*** |
| | **PM-09a.01** | opracowano kompleksową strategię zarządzania ryzykiem dla bezpieczeństwa działań i aktywów samej organizacji, osób, innych organizacji i bezpieczeństwa narodowego w związku z funkcjonowaniem i eksploatacją systemów organizacji; |
| | **PM-09a.02** | opracowano kompleksową strategię zarządzania ryzykiem dla prywatności osób fizycznych w związku z autoryzowanym przetwarzaniem danych identyfikacyjnych; |
| | **PM-09b.** | strategia zarządzania ryzykiem jest konsekwentnie wdrażana w całej organizacji; |

| | | |
|---|---|---|
| **PM-09** | **STRATEGIA ZARZĄDZANIA RYZYKIEM** | |
| | **PM-09c.** | strategia zarządzania ryzykiem jest poddawana przeglądowi i aktualizowana z ***<częstotliwością MP-09_ODP>*** bądź w razie potrzeby w celu uwzględnienia zmian w organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-09-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; strategia zarządzania ryzykiem; strategia zarządzania ryzykiem w łańcuchu dostaw; procedury dotyczące opracowywania, wdrażania, przeglądu i aktualizacji strategii zarządzania ryzykiem; wyniki oceny ryzyka istotne dla strategii zarządzania ryzykiem; inne istotne dokumenty lub zapisy]. |
| | **PM-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za opracowywanie, wdrażanie, przegląd i aktualizację strategii zarządzania ryzykiem; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PM-09-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące opracowywania, wdrażania, przeglądu i aktualizacji strategii zarządzania ryzykiem; mechanizmy wspierające opracowywanie, wdrażanie, przegląd i aktualizację strategii zarządzania ryzykiem]. |

| | | |
|---|---|---|
| **PM-10** | **PROCES AUTORYZACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-10a.[01]** | zarządzanie stanem bezpieczeństwa systemów organizacyjnych i ich środowisk funkcjonowania odbywa się poprzez procesy autoryzacji; |

| | | |
|---|---|---|
| **PM-10** | **PROCES AUTORYZACJI** | |
| | **PM-10a.[02]** | zarządzanie stanem prywatności systemów organizacyjnych i ich środowisk funkcjonowania odbywa się poprzez procesy autoryzacji; |
| | **PM-10b.** | do pełnienia określonych ról i obowiązków w ramach procesu zarządzania ryzykiem organizacyjnym wyznaczono konkretne osoby; |
| | **PM-10c.** | procesy autoryzacji są zintegrowane z organizacyjnym programem zarządzania ryzykiem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-10-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; procedury dotyczące zarządzania procesem autoryzacji (tj. dokumentacja, śledzenie i raportowanie); polityka oceny, autoryzacji i monitorowania; procedury oceny, autoryzacji i monitorowania; dokumentacja dotycząca autoryzacji systemu; listy lub inna dokumentacja dotycząca ról i obowiązków w procesie autoryzacji; wyniki oceny ryzyka istotne dla procesu autoryzacji i programu zarządzania ryzykiem w organizacji; strategia zarządzania ryzykiem organizacyjnym; inne istotne dokumenty lub zapisy]. |
| | **PM-10-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za zarządzanie procesem autoryzacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PM-10-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące autoryzacji; mechanizmy wspierające proces autoryzacji]. |

| | | |
|---|---|---|
| **PM-11** | **DEFINICJA MISJI I PROCESU BIZNESOWEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-11_ODP** | ***określono częstotliwość przeglądu i aktualizacji misji i procesów biznesowych;*** |
| | **PM-11a.[01]** | misję i procesy biznesowe organizacji zdefiniowano z uwzględnieniem kwestii bezpieczeństwa informacji; |
| | **PM-11a.[02]** | misję i procesy biznesowe organizacji zdefiniowano z uwzględnieniem kwestii ochrony prywatności; |
| | **PM-11a.[03]** | misję i procesy biznesowe organizacji zdefiniowano z uwzględnieniem wynikającego z nich ryzyka dla działań i aktywów samej organizacji, osób, innych organizacji i bezpieczeństwa narodowego; |
| | **PM-11b.[01]** | określono potrzeby w zakresie ochrony informacji wynikające ze zdefiniowanej misji i procesów biznesowych; |
| | **PM-11b.[02]** | określono potrzeby w zakresie przetwarzania danych identyfikacyjnych, wynikające z określonej misji i procesów biznesowych; |
| | **PM-11c.** | misja i procesy biznesowe są poddawane przeglądowi i aktualizacji z ***<częstotliwością MPM-11_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PM-11** | **DEFINICJA MISJI I PROCESU BIZNESOWEGO** | |
| | **PM-11-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; strategia zarządzania ryzykiem; procedury określania potrzeb w zakresie ochrony misji i działalności biznesowej; wyniki oceny ryzyka w zakresie bezpieczeństwa informacji i ochrony prywatności, istotne dla określenia potrzeb w zakresie ochrony misji i działalności gospodarczej; polityka przetwarzania danych identyfikacyjnych; wykaz danych identyfikacyjnych; inne istotne dokumenty lub zapisy]. |
| | **PM-11-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem w przedsiębiorstwie; personel organizacyjny odpowiedzialny za określenie potrzeb w zakresie ochrony informacji dot. misji i procesów biznesowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PM-11-Test** | [WYBÓR SPOŚRÓD: Organizacyjne procesy dot. definiowania misji i procesów biznesowych oraz związanych z nimi potrzeb w zakresie ochrony informacji]. |

| | | |
|---|---|---|
| **PM-12** | **ZAGROŻENIA WEWNĘTRZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-12** | wdrożono program dotyczący zagrożeń wewnętrznych, który obejmuje interdyscyplinarny zespół zajmujący się incydentami w tym zakresie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PM-12** | **ZAGROŻENIA WEWNĘTRZNE** | |
| | **PM-12-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za program zagrożeń wewnętrznych; członkowie interdyscyplinarnego zespołu ds. incydentów związanych z zagrożeniami wewnętrznymi; radca prawny; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PM-12-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wdrażania programu zagrożeń wewnętrznych oraz interdyscyplinarnego zespołu ds. incydentów związanych z zagrożeniami wewnętrznymi; mechanizmy wspierające lub wdrażające program zagrożeń wewnętrznych oraz interdyscyplinarny zespół ds. incydentów związanych z zagrożeniami wewnętrznymi]. |

| | | |
|---|---|---|
| **PM-13** | **PERSONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-13[01]** | opracowano program rozwoju i doskonalenia dla personelu bezpieczeństwa; |
| | **PM-13[02]** | opracowano program rozwoju i doskonalenia dla personelu ds. ochrony prywatności; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| PM-13 | PERSONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | |
|---|---|---|
| | **PM-13-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; dokumentacja programu rozwoju i doskonalenia personelu ds. bezpieczeństwa i ochrony prywatności informacji; procedury programu rozwoju i doskonalenia pracowników ds. bezpieczeństwa i ochrony prywatności informacji; dokumentacja programu szkoleniowego w zakresie bezpieczeństwa i ochrony prywatności informacji opartego na rolach; inne istotne dokumenty lub zapisy]. |
| | **PM-13-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i ochrony prywatności informacji; personel organizacyjny odpowiedzialny za program rozwoju i doskonalenia personelu ds. bezpieczeństwa i ochrony prywatności informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PM-13-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wdrażania programu rozwoju i doskonalenia personelu ds. bezpieczeństwa i ochrony prywatności informacji; mechanizmy wspierające lub wdrażające program rozwoju i doskonalenia personelu ds. bezpieczeństwa i ochrony prywatności informacji]. |

| PM-14 | TESTOWANIE, SZKOLENIA I MONITOROWANIE | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-14a.01[01]** | wdrożono proces zapewniający opracowanie planów dotyczących prowadzenia testów bezpieczeństwa, szkoleń i działań monitorujących związanych z systemami organizacyjnymi; |

| PM-14 | TESTOWANIE, SZKOLENIA I MONITOROWANIE | |
|---|---|---|
| | **PM-14a.01[02]** | wdrożono proces zapewniający utrzymanie planów dotyczących prowadzenia testów bezpieczeństwa, szkoleń i działań monitorujących związanych z systemami organizacyjnymi; |
| | **PM-14a.01[03]** | wdrożono proces zapewniający opracowanie planów dotyczących prowadzenia testów prywatności, szkoleń i działań monitorujących związanych z systemami organizacyjnymi; |
| | **PM-14a.01[04]** | wdrożono proces zapewniający utrzymanie planów dotyczących prowadzenia testów prywatności, szkoleń i działań monitorujących związanych z systemami organizacyjnymi; |
| | **PM-14a.02[01]** | wdrożono proces zapewniający, że plany dotyczące prowadzenia testów bezpieczeństwa, szkoleń i działań monitorujących związanych z systemami organizacyjnymi są realizowane; |
| | **PM-14a.02[02]** | wdrożono proces zapewniający, że plany dotyczące prowadzenia testów prywatności, szkoleń i działań monitorujących związanych z systemami organizacyjnymi są realizowane; |
| | **PM-14b.[01]** | plany dotyczące testowania są weryfikowane pod kątem spójności z organizacyjną strategią reagowania na ryzyko; |
| | **PM-14b.[02]** | plany dotyczące szkoleń są weryfikowane pod kątem spójności z organizacyjną strategią zarządzania ryzykiem; |
| | **PM-14b.[03]** | plany dotyczące monitorowania są weryfikowane pod kątem spójności z organizacyjną strategią zarządzania ryzykiem; |
| | **PM-14b.[04]** | plany dotyczące testowania są weryfikowane pod kątem spójności z priorytetami działań organizacji w obszarze reagowania na ryzyko; |
| | **PM-14b.[05]** | plany szkoleniowe są weryfikowane pod kątem spójności z priorytetami działań organizacji w obszarze reagowania na ryzyko; |

| | | |
|---|---|---|
| **PM-14** | **TESTOWANIE, SZKOLENIA I MONITOROWANIE** | |
| | **PM-14b.[06]** | plany dotyczące monitorowania są weryfikowane pod kątem spójności z priorytetami działań organizacji w obszarze reagowania na ryzyko; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-14-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; plany przeprowadzania testów bezpieczeństwa i prywatności, szkoleń i monitorowania; procedury organizacyjne dotyczące opracowywania i utrzymywania planów dot. przeprowadzania testów bezpieczeństwa i prywatności, szkoleń i monitorowania; strategia zarządzania ryzykiem; procedury przeglądu planów przeprowadzania testów bezpieczeństwa i prywatności, szkoleń i monitorowania pod kątem zgodności ze strategią zarządzania ryzykiem i priorytetami w zakresie reagowania na ryzyko; wyniki ocen ryzyka związanych z przeprowadzaniem testów bezpieczeństwa i prywatności, szkoleń i monitorowania; dokumentacja terminowej realizacji planowanych testów bezpieczeństwa i prywatności, szkoleń i monitorowania; inne istotne dokumenty lub zapisy]. |
| | **PM-14-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za opracowanie i utrzymanie planów prowadzenia działań w zakresie testowania, szkolenia i monitorowania bezpieczeństwa i prywatności; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PM-14-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące opracowywania i utrzymywania planów prowadzenia działań w zakresie testowania, szkolenia i monitorowania bezpieczeństwa i prywatności; mechanizmy wspierające opracowywanie i utrzymywanie planów prowadzenia działań w zakresie testowania, szkolenia i monitorowania bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **PM-15** | **GRUPY I STOWARZYSZENIA ZAJMUJĄCE SIĘ BEZPIECZEŃSTWEM I OCHRONĄ PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-15a.[01]** | nawiązano i zinstytucjonalizowano kontakt z wybranymi grupami i stowarzyszeniami należącymi do społeczności bezpieczeństwa w celu ułatwienia bieżącej edukacji i szkolenia w zakresie bezpieczeństwa dla personelu organizacji; |
| | **PM-15a.[02]** | nawiązano i zinstytucjonalizowano kontakt z wybranymi grupami i stowarzyszeniami należącymi do społeczności bezpieczeństwa w celu ułatwienia bieżącej edukacji i szkolenia w zakresie ochrony prywatności dla personelu organizacji; |
| | **PM-15b.[01]** | nawiązano i zinstytucjonalizowano kontakt z wybranymi grupami i stowarzyszeniami należącymi do społeczności bezpieczeństwa w celu zachowania biegłości w zakresie zalecanych praktyk, technik i technologii bezpieczeństwa; |
| | **PM-15b.[02]** | nawiązano i zinstytucjonalizowano kontakt z wybranymi grupami i stowarzyszeniami należącymi do społeczności ochrony prywatności w celu zachowania biegłości w zakresie zalecanych praktyk, technik i technologii bezpieczeństwa; |
| | **PM-15c.[01]** | nawiązano i zinstytucjonalizowano kontakt z wybranymi grupami i stowarzyszeniami należącymi do społeczności bezpieczeństwa w celu wymiany bieżących informacji dotyczących bezpieczeństwa, w tym zagrożeń, podatności i incydentów; |
| | **PM-15c.[02]** | nawiązano i zinstytucjonalizowano kontakt z wybranymi grupami i stowarzyszeniami należącymi do społeczności ochrony prywatności w celu wymiany bieżących informacji dotyczących bezpieczeństwa, w tym zagrożeń, podatności i incydentów; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PM-15** | **GRUPY I STOWARZYSZENIA ZAJMUJĄCE SIĘ BEZPIECZEŃSTWEM I OCHRONĄ PRYWATNOŚCI** | |
| | **PM-15-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; strategia zarządzania ryzykiem; procedury nawiązywania i instytucjonalizacji kontaktów z grupami i stowarzyszeniami zajmującymi się bezpieczeństwem i prywatnością; wykazy lub inne zapisy dotyczące kontaktów z grupami i stowarzyszeniami zajmującymi się bezpieczeństwem i prywatnością lub członkostwa w nich; inne istotne dokumenty lub zapisy]. |
| | **PM-15-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za nawiązanie i zinstytucjonalizowanie kontaktu z grupami i stowarzyszeniami zajmującymi się bezpieczeństwem i prywatnością informacji; personel wybranych grup i stowarzyszeń, z którymi organizacja nawiązała i zinstytucjonalizowała kontakt]. |
| | **PM-15-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące tworzenia i instytucjonalizacji kontaktów z grupami i stowarzyszeniami zajmującymi się bezpieczeństwem i prywatnością; mechanizmy wspierające kontakty z grupami i stowarzyszeniami zajmującymi się bezpieczeństwem i prywatnością]. |

| | | |
|---|---|---|
| **PM-16** | **OSTRZEGANIE O ZAGROŻENIACH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-16** | wdrożono program uświadamiania zagrożeń, który obejmuje międzyorganizacyjną zdolność do wymiany informacji na temat zagrożeń. |

| | | |
|---|---|---|
| **PM-16** | **OSTRZEGANIE O ZAGROŻENIACH** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-16-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; polityka programu uświadamiania zagrożeń; procedury programu uświadamiania zagrożeń; wyniki oceny ryzyka istotne dla uświadamiania zagrożeń; dokumentacja dotycząca możliwości międzyorganizacyjnej wymiany informacji; inne istotne dokumenty lub zapisy]. |
| | **PM-16-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za program uświadamiania zagrożeń; personel organizacyjny odpowiedzialny za możliwość międzyorganizacyjnej wymiany informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel zewnętrzny, z którym organizacja dzieli się informacjami dotyczącymi świadomości zagrożeń]. |
| | **PM-16-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wdrażania programu uświadamiania zagrożeń; procesy organizacyjne dotyczące wdrażania możliwości międzyorganizacyjnej wymiany informacji; mechanizmy wspierające lub wdrażające program uświadamiania zagrożeń; mechanizmy wspierające lub wdrażające zdolności w zakresie międzyorganizacyjnej wymiany informacji]. |

| | | |
|---|---|---|
| **PM-16(01)** | **OSTRZEGANIE O ZAGROŻENIACH \| ZAUTOMATYZOWANE ŚRODKI WYMIANY INFORMACJI O ZAGROŻENIACH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-16(01)** | stosuje się automatyczne mechanizmy maksymalizujące skuteczność wymiany informacji o zagrożeniach. |

| | | |
|---|---|---|
| **PM-16(01)** | **OSTRZEGANIE O ZAGROŻENIACH \| ZAUTOMATYZOWANE ŚRODKI WYMIANY INFORMACJI O ZAGROŻENIACH** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-16(01)-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; polityka programu uświadamiania zagrożeń; procedury programu uświadamiania zagrożeń; wyniki oceny ryzyka związane z uświadamianiem zagrożeń; dokumentacja dotycząca możliwości międzyorganizacyjnej wymiany informacji; inne istotne dokumenty lub zapisy]. |
| | **PM-16(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za program uświadamiania zagrożeń; personel organizacyjny odpowiedzialny za możliwość międzyorganizacyjnej wymiany informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel zewnętrzny, z którym organizacja dzieli się informacjami dotyczącymi świadomości zagrożeń]. |
| | **PM-16(01)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu bezpieczeństwa i prywatności informacji; personel organizacyjny odpowiedzialny za program uświadamiania zagrożeń; personel organizacyjny odpowiedzialny za międzyorganizacyjną wymianę informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel zewnętrzny, z którym organizacja dzieli się informacjami dotyczącymi świadomości zagrożeń]. |

| | | |
|---|---|---|
| **PM-17** | **OCHRONA NADZOROWANYCH INFORMACJI JAWNYCH PRZETWARZANYCH W SYSTEMACH ZEWNĘTRZNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-17_ODP[01]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji polityki;*** |
| | **PM-17_ODP[02]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji procedur;*** |
| | **PM-17a.[01]** | ustanowiono politykę w celu zapewnienia, że wymagania dotyczące ochrony kontrolowanych informacji jawnych, które są przetwarzane, przechowywane lub przekazywane w systemach zewnętrznych, są wdrażane zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami i normami; |
| | **PM-17a.[02]** | ustanowiono procedury w celu zapewnienia, że wymagania dotyczące ochrony kontrolowanych informacji jawnych, które są przetwarzane, przechowywane lub przekazywane w systemach zewnętrznych, są wdrażane zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami i normami; |
| | **PM-17b.[01]** | polityka jest poddawana przeglądowi i aktualizacji z ***<częstotliwością PM-17_ODP[01]>***. |
| | **PM-17b.[02]** | procedury są poddawane przeglądowi i aktualizacji z ***<częstotliwością PM-17_ODP[02]>*.** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-17-Badanie** | [WYBÓR SPOŚRÓD: Polityka dotycząca kontrolowanych informacji jawnych; procedury dotyczące kontrolowanych informacji jawnych; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PM-17** | **OCHRONA NADZOROWANYCH INFORMACJI JAWNYCH PRZETWARZANYCH W SYSTEMACH ZEWNĘTRZNYCH** | |
| | **PM-17-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolowane informacje jawne; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **PM-18** | **PLAN PROGRAMU OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-18_ODP** | ***określono częstotliwość aktualizacji planu programu ochrony prywatności;*** |
| | **PM-18a.[01]** | opracowano plan programu ochrony prywatności obejmujący całą organizację, który zawiera opis programu ochrony prywatności obowiązującego w organizacji; |
| | **PM-18a.01[01]** | plan programu ochrony prywatności zawiera opis struktury programu ochrony prywatności; |
| | **PM-18a.01[02]** | plan programu ochrony prywatności zawiera opis zasobów przeznaczonych na program ochrony prywatności; |
| | **PM-18a.02[01]** | plan programu ochrony prywatności zawiera opis wymagań dotyczących wspomnianego programu; |
| | **PM-18a.02[02]** | plan programu ochrony prywatności zawiera opis zabezpieczeń w zakresie zarządzania programem, wprowadzonych lub planowanych do wprowadzenia w celu spełnienia wymogów tegoż programu; |
| | **PM-18a.02[03]** | plan programu ochrony prywatności zawiera opis wspólnych zabezpieczeń wprowadzonych lub planowanych do wprowadzenia w celu spełnienia wymogów tegoż programu; |
| | **PM-18a.03[01]** | plan programu ochrony prywatności obejmuje rolę wyższego urzędnika ds. ochrony prywatności; |

| **PM-18** | **PLAN PROGRAMU OCHRONY PRYWATNOŚCI** | |
|---|---|---|
| | **PM-18a.03[02]** | plan programu ochrony prywatności obejmuje identyfikację i przypisanie ról i obowiązków innym urzędnikom i pracownikom zajmującym się ochroną prywatności; |
| | **PM-18a.04[01]** | plan programu ochrony prywatności opisuje kwestię zaangażowania kierownictwa; |
| | **PM-18a.04[02]** | plan programu ochrony prywatności opisuje kwestię zgodności; |
| | **PM-18a.04[03]** | plan programu ochrony prywatności opisuje strategiczne cele i założenia rzeczonego programu; |
| | **PM-18a.05** | plan programu ochrony prywatności odzwierciedla koordynację pomiędzy jednostkami organizacyjnymi odpowiedzialnymi za różne aspekty prywatności; |
| | **PM-18a.06** | plan programu ochrony prywatności jest zatwierdzony przez wyższego urzędnika odpowiedzialnego za ryzyko w zakresie prywatności związane z działaniami organizacji (w tym w odniesieniu do misji, funkcji, wizerunku i reputacji), a także w zakresie majątku samej organizacji, osób, innych organizacji i bezpieczeństwa narodowego; |
| | **PM-18a.[02]** | plan programu ochrony prywatności jest rozpowszechniany; |
| | **PM-18b.[01]** | plan programu ochrony prywatności jest aktualizowany z ***<częstotliwością PM-18_ODP>***; |
| | **PM-18b.[02]** | plan programu ochrony prywatności jest aktualizowany w celu uwzględnienia zmian w krajowych przepisach i politykach dotyczących ochrony prywatności; |
| | **PM-18b.[03]** | plan programu ochrony prywatności jest aktualizowany w celu uwzględnienia zmian w organizacji; |
| | **PM-18b.[04]** | plan programu ochrony prywatności jest aktualizowany w celu rozwiązania problemów zidentyfikowanych podczas jego realizacji lub w trakcie oceny ochrony prywatności. |

| | | |
|---|---|---|
| **PM-18** | **PLAN PROGRAMU OCHRONY PRYWATNOŚCI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-18-Badanie** | [WYBÓR SPOŚRÓD: Plan ochrony prywatności; procedury dotyczące opracowania i realizacji planu programu; procedury dotyczące przeglądów, aktualizacji i zatwierdzania planu programu; procedury dotyczące koordynacji planu programu z odpowiednimi podmiotami; zapisy przeglądów, aktualizacji i zatwierdzeń planu programu; inne istotne dokumenty lub zapisy]. |
| | **PM-18-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację planu programu ochrony prywatności; personel organizacyjny odpowiedzialny za prywatność]. |

| | | |
|---|---|---|
| **PM-19** | **ROLE KIEROWNICZE PROGRAMU OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-19[01]** | wyznaczono wyższego urzędnika ds. prywatności z odpowiednimi uprawnieniami, misją, obowiązkami i zasobami; |
| | **PM-19[02]** | wyższy urzędnik ds. prywatności przeprowadza koordynację obowiązujących wymogów dotyczących prywatności; |
| | **PM-19[03]** | wyższy urzędnik ds. prywatności opracowuje stosowne wymagania dotyczące prywatności; |
| | **PM-19[04]** | wyższy urzędnik ds. prywatności wdraża obowiązujące wymogi dotyczące prywatności; |
| | **PM-19[05]** | wyższy urzędnik ds. prywatności zarządza ryzykiem związanym z prywatnością poprzez organizacyjny program ochrony prywatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PM-19** | **ROLE KIEROWNICZE PROGRAMU OCHRONY PRYWATNOŚCI** | |
| | **PM-19-Badanie** | [WYBÓR SPOŚRÓD: Dokumenty dotyczące programu ochrony prywatności, w tym polityki, procedury, plany i sprawozdania; publiczne informacje o ochronie prywatności, w tym te publikowane w odpowiednim rejestrze krajowym; oceny wpływu na prywatność; oceny ryzyka w zakresie ochrony prywatności; oświadczenia zgodne z ustawą o ochronie danych<br>oświadczenia związane z przepisami o ochronie prywatności; zawiadomienia o ujawnieniu danych z rejestru; umowy i zawiadomienia o komputerowym dopasowaniu danych; umowy, umowy o wymianie informacji i protokoły ustaleń; wymogi regulacyjne, w tym ustawy, rozporządzenia, przepisy, normy i wytyczne; inne istotne dokumenty lub zapisy]. |
| | **PM-19-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie i realizację programu ochrony prywatności; personel organizacyjny odpowiedzialny za prywatność; wyższy urzędnik ds. prywatności; urzędnicy ds. prywatności]. |

| | | |
|---|---|---|
| **PM-20** | **ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-20[01]** | na głównej, publicznej witrynie internetowej organizacji utrzymywana jest centralna strona z zasobami; |
| | **PM-20[02]** | wspomniana strona internetowa służy jako centralne źródło informacji o programie ochrony prywatności organizacji; |
| | **PM-20a.[01]** | strona internetowa umożliwia opinii publicznej dostęp do informacji o działaniach organizacji w zakresie ochrony prywatności; |

| | | |
|---|---|---|
| **PM-20** | **ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI** | |
| | **PM-20a.[02]** | strona internetowa zapewnia opinii publicznej możliwość kontaktu z wyższym urzędnikiem organizacji w związku z kwestiami prywatności; |
| | **PM-20b.[01]** | strona internetowa zapewnia publiczny dostęp do praktyk w zakresie ochrony prywatności stosowanych przez organizację; |
| | **PM-20b.[02]** | strona internetowa zapewnia publiczny dostęp do raportów organizacji dotyczących ochrony prywatności; |
| | **PM-20c.** | strona internetowa wykorzystuje publicznie dostępne adresy e-mail lub numery telefonów, aby umożliwić opinii publicznej przekazywanie informacji zwrotnych lub kierowanie zapytań dotyczących praktyk w zakresie ochrony prywatności do biura ochrony prywatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-20-Badanie** | [WYBÓR SPOŚRÓD: Publiczna strona internetowa; publicznie dostępne dokumenty dotyczące programu ochrony prywatności, w tym polityki, procedury, plany i sprawozdania; opis stanowiska wyższego urzędnika ds. ochrony prywatności; publiczne informacje o ochronie prywatności, w tym te publikowane w odpowiednim rejestrze krajowym; oceny wpływu na prywatność; oceny ryzyka w zakresie ochrony prywatności; oświadczenia związane z przepisami o ochronie prywatności; zawiadomienia o ujawnieniu danych z rejestru; umowy i zawiadomienia o komputerowym dopasowaniu danych; inne istotne dokumenty lub zapisy]. |
| | **PM-20-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za rozpowszechnianie informacji o programie ochrony prywatności; personel organizacyjny odpowiedzialny za ochronę prywatności]. |
| | **PM-20-Test** | [WYBÓR SPOŚRÓD: Lokalizacja, dostępność i funkcjonalność strony internetowej z zasobami dotyczącymi prywatności, a także dostęp do niej]. |

| | | |
|---|---|---|
| **PM-20(01)** | **ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI \| POLITYKI PRYWATNOŚCI PREZENTOWANE NA STRONACH INTERNETOWYCH, W APLIKACJACH I USŁUGACH CYFROWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-20(01)[01]** | opracowano politykę prywatności i zamieszczono ją na wszystkich dostępnych publicznie stronach internetowych; |
| | **PM-20(01)[02]** | opracowano politykę prywatności i zamieszczono ją we wszystkich aplikacjach mobilnych; |
| | **PM-20(01)[03]** | opracowano politykę prywatności i zamieszczono ją we wszystkich innych usługach cyfrowych; |
| | **PM-20(01)(a)[01]** | polityka prywatności jest napisana prostym językiem; |
| | **PM-20(01)(a)[02]** | polityka prywatności jest zorganizowana w sposób intuicyjny i łatwy do nawigacji; |
| | **PM-20(01)(b)[01]** | polityka prywatności dostarcza opinii publicznej informacji potrzebnych do podjęcia świadomej decyzji o ewentualnej interakcji z organizacją; |
| | **PM-20(01)(b)[02]** | polityka prywatności dostarcza opinii publicznej informacji potrzebnych do podjęcia świadomej decyzji o sposobie interakcji z organizacją; |
| | **PM-20(01)(c)[01]** | polityka prywatności jest każdorazowo aktualizowana, gdy organizacja wprowadza istotne zmiany w zakresie opisanych w niej praktyk; |
| | **PM-20(01)(c)[02]** | polityka prywatności zawiera znacznik czasu/daty w celu poinformowania opinii publicznej o terminie wprowadzenia ostatnich zmian. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-20(01)-Badanie** | [WYBÓR SPOŚRÓD: Plan programu ochrony prywatności; polityka prywatności dostępna na stronie internetowej organizacji, w aplikacjach mobilnych lub innych usługach cyfrowych]. |

| | | |
|---|---|---|
| **PM-20(01)** | **ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI \| POLITYKI PRYWATNOŚCI PREZENTOWANE NA STRONACH INTERNETOWYCH, W APLIKACJACH I USŁUGACH CYFROWYCH** | |
| | **PM-20(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za rozpowszechnianie informacji o programie ochrony prywatności; personel organizacyjny odpowiedzialny za ochronę prywatności]. |
| | **PM-20(01)-Test** | [WYBÓR SPOŚRÓD: Procedury i praktyki organizacyjne dotyczące autoryzacji, prowadzenia, zarządzania i przeglądu w zakresie przetwarzania danych identyfikacyjnych; procedury i praktyki organizacyjne w zakresie rozpowszechniania informacji o programie ochrony prywatności; mechanizmy wspierające rozpowszechnianie informacji o programie ochrony prywatności]. |

| | | |
|---|---|---|
| **PM-21** | **REJESTROWANIE UJAWNIEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-21a.** | opracowano i prowadzono dokładną ewidencję ujawnień danych identyfikacyjnych; |
| | **PM-21a.01[01]** | ewidencja obejmuje datę każdego ujawnienia; |
| | **PM-21a.01[02]** | ewidencja obejmuje charakter każdego ujawnienia; |
| | **PM-21a.01[03]** | ewidencja obejmuje cel każdego ujawnienia; |
| | **PM-21a.02[01]** | ewidencja zawiera imię i nazwisko osoby lub organizacji, której ujawniono informacje; |
| | **PM-21a.02[02]** | ewidencja zawiera adres lub inne informacje kontaktowe osoby lub organizacji, której ujawniono informacje; |

| | | |
|---|---|---|
| **PM-21** | **REJESTROWANIE UJAWNIEŃ** | |
| | **PM-21b.** | ewidencja ujawnień jest przechowywana przez okres przechowywania danych identyfikacyjnych lub przez pięć lat po dokonaniu ujawnienia, w zależności od tego, który z tych okresów jest dłuższy; |
| | **PM-21c.** | ewidencja ujawnień jest udostępniana na żądanie osoby, której dotyczą dane identyfikacyjne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-21-Badanie** | [WYBÓR SPOŚRÓD: Plan programu ochrony prywatności; polityka i procedury ujawniania; rejestry ujawnień; zapisy z audytu; polityka i procedury związane z przepisami o ochronie prywatności; zawiadomienia o ujawnieniu danych z rejestru; zasady wyłączenia ze stosowania przepisów o ochronie prywatności]. |
| | **PM-21-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za program ochrony prywatności; personel organizacyjny odpowiedzialny za ochronę prywatności]. |
| | **PM-21-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ujawnień; mechanizmy wspierające ewidencję ujawnień, w tym komercyjne usługi zapewniające powiadomienia i alerty]. |

| | | |
|---|---|---|
| **PM-22** | **ZARZĄDZANIE JAKOŚCIĄ DANYCH OSOBOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-22[01]** | opracowano i udokumentowano organizacyjną politykę zarządzania jakością danych identyfikacyjnych; |
| | **PM-22[02]** | opracowano i udokumentowano organizacyjne procedury zarządzania jakością danych identyfikacyjnych; |

| **PM-22** | **ZARZĄDZANIE JAKOŚCIĄ DANYCH OSOBOWYCH** | |
|---|---|---|
| | **PM-22a.[01]** | polityki uwzględniają sprawdzenie dokładności danych identyfikacyjnych w całym cyklu życia informacji; |
| | **PM-22a.[02]** | polityki uwzględniają sprawdzenie istotności danych identyfikacyjnych w całym cyklu życia informacji; |
| | **PM-22a.[03]** | polityki uwzględniają sprawdzenie aktualności danych identyfikacyjnych w całym cyklu życia informacji; |
| | **PM-22a.[04]** | polityki uwzględniają sprawdzenie kompletności danych identyfikacyjnych w całym cyklu życia informacji; |
| | **PM-22a.[05]** | procedury uwzględniają sprawdzenie dokładności danych identyfikacyjnych w całym cyklu życia informacji; |
| | **PM-22a.[06]** | procedury uwzględniają sprawdzenie istotności danych identyfikacyjnych w całym cyklu życia informacji; |
| | **PM-22a.[07]** | procedury uwzględniają sprawdzenie aktualności danych identyfikacyjnych w całym cyklu życia informacji; |
| | **PM-22a.[08]** | procedury uwzględniają sprawdzenie kompletności danych identyfikacyjnych w całym cyklu życia informacji; |
| | **PM-22b.[01]** | polityki uwzględniają możliwość korekty lub usunięcia nieprawidłowych bądź nieaktualnych danych identyfikacyjnych; |
| | **PM-22b.[02]** | procedury uwzględniają możliwość korekty lub usunięcia nieprawidłowych bądź nieaktualnych danych identyfikacyjnych; |
| | **PM-22c.[01]** | polityki uwzględniają wysyłanie osobom lub innym podmiotom zawiadomień o korekcie lub usunięciu nieprawidłowych bądź nieaktualnych danych identyfikacyjnych; |
| | **PM-22c.[02]** | procedury uwzględniają wysyłanie osobom lub innym podmiotom zawiadomień o korekcie lub usunięciu nieprawidłowych bądź nieaktualnych danych identyfikacyjnych; |

| | | |
|---|---|---|
| **PM-22** | **ZARZĄDZANIE JAKOŚCIĄ DANYCH OSOBOWYCH** | |
| | **PM-22d.[01]** | polityki uwzględniają odwołania od decyzji odmownych w sprawie wniosków o korektę lub usunięcie danych; |
| | **PM-22d.[02]** | procedury uwzględniają odwołania od decyzji odmownych w sprawie wniosków o korektę lub usunięcie danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-22-Badanie** | [WYBÓR SPOŚRÓD: Plan programu ochrony prywatności; polityki i procedury dotyczące zarządzania jakością danych osobowych, dokumentacja cyklu życia informacji oraz przykładowe zawiadomienia o korekcie lub usunięciu danych; zapisy dotyczące monitorowania praktyk zarządzania jakością danych identyfikacyjnych; dokumentacja przeglądów i aktualizacji polityk i procedur]. |
| | **PM-22-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za rozpowszechnianie informacji o programie ochrony prywatności; personel organizacyjny odpowiedzialny za ochronę prywatności]. |
| | **PM-22-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące jakości danych i procedur zarządzania jakością danych identyfikacyjnych; mechanizmy wspierające lub wdrażające wymagania dotyczące zarządzania jakością]. |

| | | |
|---|---|---|
| **PM-23** | **ORGAN ZARZĄDZANIA DANYMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-23_ODP[01]** | ***określono role organu zarządzającego danymi;*** |
| | **PM-23_ODP[02]** | ***określono obowiązki organu zarządzającego danymi;*** |

| **PM-23** | **ORGAN ZARZĄDZANIA DANYMI** | |
|---|---|---|
| | **PM-23** | ustanowiono organ zarządzający danymi, obejmujący ***<role PM-23_ODP[01]>***<br>oraz ***<obowiązki PM-23_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-23-Badanie** | [WYBÓR SPOŚRÓD: Plan programu ochrony prywatności; dokumentacja dotycząca organu zarządzającego danymi, w tym dokumenty ustanawiające taki organ, jego statut oraz wszelkie plany i sprawozdania; protokoły ze spotkań i ewidencja decyzji zarządu; ewidencja wniosków o przegląd danych; polityki, procedury i normy ułatwiające zarządzanie danymi]. |
| | **PM-23-Wywiad** | [WYBÓR SPOŚRÓD: Urzędnicy wchodzący w skład organu ds. zarządzania danymi (np. kierownik ds. informacji, wyższy urzędnik ds. bezpieczeństwa informacji oraz wyższy urzędnik ds. prywatności)]. |

| **PM-24** | **RADA DS. INTEGRALNOŚCI DANYCH** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-24** | powołano radę ds. integralności danych; |
| | **PM-24a.** | rada ds. integralności danych dokonuje przeglądu wniosków o przeprowadzenie lub udział w programie dopasowywania; |
| | **PM-24b.** | rada ds. integralności danych przeprowadza coroczny przegląd wszystkich programów dopasowywania, w których uczestniczyła organizacja. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PM-24** | **RADA DS. INTEGRALNOŚCI DANYCH** | |
| | **PM-24-Badanie** | [WYBÓR SPOŚRÓD: Plan programu ochrony prywatności; dokumenty dotyczące programu ochrony prywatności odnoszące się do rady ds. integralności danych, w tym dokumenty ustanawiające radę, jej statut oraz wszelkie plany i sprawozdania; umowy i zawiadomienia o komputerowym dopasowaniu danych; umowy o wymianie informacji; protokoły ustaleń; zapisy dokumentujące coroczne przeglądy; wymogi regulacyjne, w tym ustawy, rozporządzenia, przepisy, normy i wytyczne]. |
| | **PM-24-Wywiad** | [WYBÓR SPOŚRÓD: Członkowie rady ds. integralności danych (np. kierownik ds. informacji, wyższy urzędnik ds. bezpieczeństwa informacji, wyższy urzędnik ds. prywatności i inspektor generalny organizacji)]. |

| | | |
|---|---|---|
| **PM-25** | **MINIMALIZACJA DANYCH OSOBOWYCH WYKORZYSTYWANYCH W TESTACH, SZKOLENIACH I BADANIACH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-25_ODP[01]** | ***określono częstotliwość przeglądu polityk, które dotyczą wykorzystywania danych identyfikacyjnych do wewnętrznych testów szkoleń i badań;*** |
| | **PM-25_ODP[02]** | ***określono częstotliwość aktualizacji polityk, które dotyczą wykorzystywania danych identyfikacyjnych do wewnętrznych testów szkoleń i badań;*** |
| | **PM-25_ODP[03]** | ***określono częstotliwość przeglądu procedur, które dotyczą wykorzystywania danych identyfikacyjnych do wewnętrznych testów szkoleń i badań;*** |
| | **PM-25_ODP[04]** | ***określono częstotliwość aktualizacji procedur, które dotyczą wykorzystywania danych identyfikacyjnych do wewnętrznych testów szkoleń i badań;*** |

| | | |
|---|---|---|
| **PM-25** | **MINIMALIZACJA DANYCH OSOBOWYCH WYKORZYSTYWANYCH W TESTACH, SZKOLENIACH I BADANIACH** | |
| | **PM-25a.[01]** | opracowano i udokumentowano polityki dotyczące wykorzystania danych identyfikacyjnych do celów testów wewnętrznych; |
| | **PM-25a.[02]** | opracowano i udokumentowano polityki dotyczące wykorzystania danych identyfikacyjnych do celów szkoleń wewnętrznych; |
| | **PM-25a.[03]** | opracowano i udokumentowano polityki dotyczące wykorzystania danych identyfikacyjnych do celów badań wewnętrznych; |
| | **PM-25a.[04]** | opracowano i udokumentowano procedury dotyczące wykorzystania danych identyfikacyjnych do celów testów wewnętrznych; |
| | **PM-25a.[05]** | opracowano i udokumentowano procedury dotyczące wykorzystania danych identyfikacyjnych do celów szkoleń wewnętrznych; |
| | **PM-25a.[06]** | opracowano i udokumentowano procedury dotyczące wykorzystania danych identyfikacyjnych do celów badań wewnętrznych; |
| | **PM-25a.[07]** | wdrożono polityki dotyczące wykorzystania danych identyfikacyjnych do celów testów wewnętrznych; |
| | **PM-25a.[08]** | wdrożono polityki dotyczące wykorzystania danych identyfikacyjnych do celów szkoleń; |
| | **PM-25a.[09]** | wdrożono polityki dotyczące wykorzystania danych identyfikacyjnych do celów badań; |
| | **PM-25a.[10]** | wdrożono procedury dotyczące wykorzystania danych identyfikacyjnych do celów testów wewnętrznych; |
| | **PM-25a.[11]** | wdrożono procedury dotyczące wykorzystania danych identyfikacyjnych do celów szkoleń; |
| | **PM-25a.[12]** | wdrożono procedury dotyczące wykorzystania danych identyfikacyjnych do celów badań; |

| | | |
|---|---|---|
| **PM-25** | **MINIMALIZACJA DANYCH OSOBOWYCH WYKORZYSTYWANYCH W TESTACH, SZKOLENIACH I BADANIACH** | |
| | **PM-25b.[01]** | ilość danych identyfikacyjnych wykorzystywanych do celów testów wewnętrznych jest ograniczona lub zminimalizowana; |
| | **PM-25b.[02]** | ilość danych identyfikacyjnych wykorzystywanych do celów szkoleń wewnętrznych jest ograniczona lub zminimalizowana; |
| | **PM-25b.[03]** | ilość danych identyfikacyjnych wykorzystywanych do celów badań wewnętrznych jest ograniczona lub zminimalizowana; |
| | **PM-25c.[01]** | wykorzystanie danych identyfikacyjnych jest dozwolone, gdy jest to wymagane do testów wewnętrznych; |
| | **PM-25c.[02]** | wykorzystanie danych identyfikacyjnych jest dozwolone, gdy jest to wymagane do szkoleń wewnętrznych; |
| | **PM-25c.[03]** | wykorzystanie danych identyfikacyjnych jest dozwolone, gdy jest to wymagane do badań wewnętrznych; |
| | **PM-25d.[01]** | polityki są poddawane przeglądowi z ***<częstotliwością PM-25_ODP[01]>***; |
| | **PM-25d.[02]** | polityki są poddawane aktualizacji z ***<częstotliwością PM-25_ODP[02]>***; |
| | **PM-25d.[03]** | procedury są poddawane przeglądowi i aktualizacji z ***<częstotliwością MP-25_ODP[03]>***; |
| | **PM-25d.[04]** | procedury są poddawane aktualizacji z ***<częstotliwością PM-25_ODP[04]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-25-Badanie** | [WYBÓR SPOŚRÓD: Plan programu ochrony prywatności; polityka i procedury minimalizacji wykorzystania danych identyfikacyjnych w testach, szkoleniach i badaniach; dokumentacja wspierająca realizację polityki (np. szablony testów, szkoleń i badań; analiza progu ochrony prywatności; ocena ryzyka dla ochrony prywatności); zbiory danych wykorzystywane w testach, szkoleniach i badaniach]. |

| | | |
|---|---|---|
| **PM-25** | **MINIMALIZACJA DANYCH OSOBOWYCH WYKORZYSTYWANYCH W TESTACH, SZKOLENIACH I BADANIACH** | |
| | **PM-25-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za program ochrony prywatności; personel organizacyjny odpowiedzialny za ochronę prywatności; programiści systemu; personel odpowiedzialny za Niezależne Komisje Etyczne]. |
| | **PM-25-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zarządzania jakością danych, w tym danych identyfikacyjnych; mechanizmy wspierające zarządzanie jakością danych, w tym danych identyfikacyjnych, w celu minimalizacji wykorzystania danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **PM-26** | **ZARZĄDZANIE SKARGAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-26_ODP[01]** | ***określono okres na przegląd skargi (w tym zastrzeżenia lub zapytania) od osoby fizycznej;*** |
| | **PM-26_ODP[02]** | ***określono okres na rozpatrzenie skargi (w tym zastrzeżenia lub zapytania) od osoby fizycznej;*** |
| | **PM-26_ODP[03]** | ***określono okres na potwierdzenie przyjęcia złożonej skargi;*** |
| | **PM-26_ODP[04]** | ***określono okres na udzielenie odpowiedzi na złożoną skargę;*** |
| | **PM-26[01]** | wdrożono proces przyjmowania skarg, zastrzeżeń lub zapytań od osób fizycznych dotyczących praktyk organizacji w zakresie bezpieczeństwa i prywatności; |
| | **PM-26[02]** | wdrożono proces odpowiadania na skargi, zastrzeżenia lub zapytania od osób fizycznych dotyczące praktyk organizacji w zakresie bezpieczeństwa i prywatności; |

| | | |
|---|---|---|
| **PM-26** | **ZARZĄDZANIE SKARGAMI** | |
| | **PM-26a.[01]** | proces obsługi skarg obejmuje mechanizmy, które są łatwe do wykorzystania przez obywateli; |
| | **PM-26a.[02]** | proces zarządzania skargami obejmuje mechanizmy, które są bez trudu dostępne dla obywateli; |
| | **PM-26b.** | proces zarządzania skargami obejmuje wszystkie informacje niezbędne do skutecznego składania skarg; |
| | **PM-26c.[01]** | proces zarządzania skargami obejmuje mechanizmy śledzenia w celu zapewnienia, że wszystkie skargi są przyjmowane w ***<okresie PM-26_ODP[01]>***; |
| | **PM-26c.[02]** | proces zarządzania skargami obejmuje mechanizmy śledzenia w celu zapewnienia, że wszystkie skargi są rozpatrywane w ***<okresie PM-26_ODP[01]>***; |
| | **PM-26d.** | proces zarządzania skargami obejmuje potwierdzenie przyjęcia skarg, zastrzeżeń lub zapytań od osób fizycznych w ***<okresie PM-26_ODP[03]>***; |
| | **PM-26e.** | proces zarządzania skargami obejmuje udzielanie odpowiedzi na skargi, zastrzeżenia lub zapytania osób fizycznych w ***<okresie PM-26_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-26-Badanie** | [WYBÓR SPOŚRÓD: Plan programu ochrony prywatności; procedury dotyczące zarządzania skargami; dokumentacja skarg; procedury dotyczące przeglądów skarg; inne istotne dokumenty lub zapisy]. |
| | **PM-26-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za program ochrony prywatności; personel organizacyjny odpowiedzialny za ochronę prywatności]. |
| | **PM-26-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zarządzania skargami; mechanizmy wspierające zarządzanie skargami; narzędzia wykorzystywane przez obywateli do składania skarg, zastrzeżeń i zapytań (np. telefon, infolinia, e-mail lub formularze internetowe). |

| | | |
|---|---|---|
| **PM-27** | **SPRAWOZDAWCZOŚĆ W ZAKRESIE OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-27_ODP[01]** | ***określono raporty dotyczące ochrony prywatności;*** |
| | **PM-27_ODP[02]** | ***określono organy nadzorujące ochronę prywatności;*** |
| | **PM-27_ODP[03]** | ***określono urzędników odpowiedzialnych za monitorowanie zgodności z programem ochrony prywatności;*** |
| | **PM-27_ODP[04]** | ***określono częstotliwość przeglądów i aktualizacji raportów dotyczących ochrony prywatności;*** |
| | **PM-27a.** | opracowywane są ***<raporty dotyczące ochrony prywatności PM-27_ODP[01]>***; |
| | **PM-27a.01** | raporty dotyczące ochrony prywatności są przekazywane ***<organom nadzorczym PM-27_ODP[02]>*** w celu wykazania zgodności z wymogami w zakresie ochrony prywatności, określonymi w przepisach prawa i polityce; |
| | **PM-27a.02[01]** | raporty dotyczące ochrony prywatności są rozpowszechniane wśród ***<urzędników PM-27_ODP[03]>***; |
| | **PM-27a.02[02]** | raporty dotyczące ochrony prywatności są rozpowszechniane wśród innego personelu odpowiedzialnego za monitorowanie zgodności z programem ochrony prywatności; |
| | **PM-27b.** | raporty dotyczące ochrony prywatności są przeglądane i aktualizowane z ***<częstotliwością MPM-27_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PM-27** | **SPRAWOZDAWCZOŚĆ W ZAKRESIE OCHRONY PRYWATNOŚCI** | |
| | **PM-27-Badanie** | [WYBÓR SPOŚRÓD: Plan programu ochrony prywatności; wewnętrzne i zewnętrzne raporty dotyczące ochrony prywatności; plan programu ochrony prywatności; roczne sprawozdania dotyczące ochrony prywatności przekazywane przez wyższego urzędnika organizacji do odpowiedniego organu;<br>sprawozdania dla parlamentu wymagane przez przepisy prawa lub polityki, w tym polityki wewnętrzne; zapisy dokumentujące przedkładanie sprawozdań organom nadzoru i urzędnikom odpowiedzialnym za monitorowanie zgodności z programem ochrony prywatności; zapisy przeglądów i aktualizacji raportów dotyczących ochrony prywatności]. |
| | **PM-27-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za program ochrony prywatności; personel organizacyjny odpowiedzialny za ochronę prywatności; radca prawny]. |

| | | |
|---|---|---|
| **PM-28** | **OPRACOWYWANIE RAM RYZYKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-28_ODP[01]** | ***określono personel otrzymujący wyniki działań w zakresie opracowywania ram ryzyka;*** |
| | **PM-28_ODP[02]** | ***określono częstotliwość przeglądu i aktualizacji działań w zakresie opracowywania ram ryzyka;*** |
| | **PM-28a.01[01]** | założenia wpływające na ocenę ryzyka są identyfikowane i dokumentowane; |
| | **PM-28a.01[02]** | założenia wpływające na reakcje na ryzyko są identyfikowane i dokumentowane; |

| | | |
|---|---|---|
| **PM-28** | **OPRACOWYWANIE RAM RYZYKA** | |
| | **PM-28a.01[03]** | założenia mające wpływ na monitorowanie ryzyka są identyfikowane i dokumentowane; |
| | **PM-28a.02[01]** | ograniczenia wpływające na ocenę ryzyka są identyfikowane i dokumentowane; |
| | **PM-28a.02[02]** | ograniczenia wpływające na reakcje na ryzyko są identyfikowane i dokumentowane; |
| | **PM-28a.02[03]** | ograniczenia wpływające na monitorowanie ryzyka są identyfikowane i dokumentowane; |
| | **PM-28a.03[01]** | priorytety uwzględniane przez organizację w zarządzaniu ryzykiem są identyfikowane i dokumentowane; |
| | **PM-28a.03[02]** | kompromisy uwzględniane przez organizację przy zarządzaniu ryzykiem są identyfikowane i dokumentowane; |
| | **PM-28a.04** | tolerancja ryzyka przez organizację jest identyfikowana i dokumentowana; |
| | **PM-28b.** | wyniki działań w zakresie opracowywania ram ryzyka są przekazywane ***<personelowi PM-28_ODP[01]>***; |
| | **PM-28c.** | zagadnienia związane z opracowywaniem ram ryzyka są poddawane przeglądowi i aktualizowane z ***<częstotliwością PM-28_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-28-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; strategia zarządzania ryzykiem łańcucha dostaw; dokumentacja działań związanych z opracowywaniem ram ryzyka; polityka i procedury dotyczące działań związanych z opracowywaniem ram ryzyka; strategia zarządzania ryzykiem]. |

| **PM-28** | **OPRACOWYWANIE RAM RYZYKA** | |
|---|---|---|
| | **PM-28-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny (w tym właściciele lub osoby zarządzające misją, działalnością i systemem; urzędnicy zatwierdzający; wyższy urzędnik ds. bezpieczeństwa informacji; wyższy urzędnik ds. ochrony prywatności; oraz wyższy urzędnik odpowiedzialny za zarządzanie ryzykiem)]. |
| | **PM-28-Test** | [WYBÓR SPOŚRÓD: Procedury i praktyki organizacyjne dotyczące autoryzacji, prowadzenia, zarządzania i przeglądu procesu przetwarzania danych identyfikacyjnych; procesy organizacyjne dotyczące opracowywania ram ryzyka; mechanizmy wspierające opracowywanie, przegląd, aktualizację i zatwierdzanie ram ryzyka]. |

| **PM-29** | **ROLE KIEROWNICZE PROGRAMU ZARZĄDZANIA RYZYKIEM** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-29a.[01]** | powołano wyższego urzędnika ds. zarządzania ryzykiem; |
| | **PM-29a.[02]** | wyższy urzędnik ds. zarządzania ryzykiem dostosowuje procesy zarządzania bezpieczeństwem informacji i prywatnością do procesów planowania strategicznego, operacyjnego i budżetowego; |
| | **PM-29b.[01]** | ustanowiono stanowisko (funkcję) dyrektora ds. ryzyka; |
| | **PM-29b.[02]** | dyrektor ds. ryzyka (funkcja) bada i analizuje ryzyko z perspektywy całej organizacji; |
| | **PM-29b.[03]** | dyrektor ds. ryzyka (funkcja) zapewnia, że zarządzanie ryzykiem jest spójne w całej organizacji; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PM-29** | **ROLE KIEROWNICZE PROGRAMU ZARZĄDZANIA RYZYKIEM** | |
| | **PM-29-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; strategia zarządzania ryzykiem; strategia zarządzania ryzykiem w łańcuchu dostaw; dokumentacja dotycząca powołania, ról i obowiązków wyższego urzędnika ds. zarządzania ryzykiem; dokumentacja działań podjętych przez wspomnianego urzędnika; dokumentacja dotycząca ustanowienia stanowiska (funkcji) kierownika ds. ryzyka oraz powiązanych polityk i procedur]. |
| | **PM-29-Wywiad** | [WYBÓR SPOŚRÓD: Wyższy urzędnik ds. zarządzania ryzykiem; kierownik ds. informacji; wyższy urzędnik ds. bezpieczeństwa informacji; wyższy urzędnik ds. prywatności; personel organizacyjny odpowiedzialny za program bezpieczeństwa informacji i prywatności]. |

| | | |
|---|---|---|
| **PM-30** | **STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-30_ODP** | ***określono częstotliwość przeglądu i aktualizacji strategii zarządzania ryzykiem łańcucha dostaw;*** |
| | **PM-30a.[01]** | opracowano organizacyjną strategię zarządzania ryzykiem w łańcuchu dostaw; |
| | **PM-30a.[02]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z rozwojem systemów; |
| | **PM-30a.[03]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z rozwojem komponentów systemu; |
| | **PM-30a.[04]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z rozwojem usług systemowych; |

| | | |
|---|---|---|
| **PM-30** | **STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW** | |
| | **PM-30a.[05]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z pozyskiwaniem systemów; |
| | **PM-30a.[06]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z pozyskiwaniem komponentów systemu; |
| | **PM-30a.[07]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z pozyskiwaniem usług systemowych; |
| | **PM-30a.[08]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z utrzymaniem systemów; |
| | **PM-30a.[09]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z utrzymaniem komponentów systemu; |
| | **PM-30a.[10]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z utrzymaniem usług systemowych; |
| | **PM-30a.[11]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z utylizacją systemów; |
| | **PM-30a.[12]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z utylizacją komponentów systemu; |
| | **PM-30a.[13]** | strategia zarządzania ryzykiem łańcucha dostaw odnosi się do ryzyka związanego z utylizacją usług systemowych; |
| | **PM-30b.** | strategię zarządzania ryzykiem łańcucha dostaw wdrożono konsekwentnie w całej organizacji; |
| | **PM-30c.** | strategia zarządzania ryzykiem łańcucha dostaw jest poddawana przeglądowi i aktualizacji z ***<częstotliwością MPM-30_ODP>*** lub w miarę potrzeb w celu uwzględnienia zmian w organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PM-30** | **STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW** | |
| | **PM-30-Badanie** | [WYBÓR SPOŚRÓD: Strategia zarządzania ryzykiem łańcucha dostaw; strategia zarządzania ryzykiem organizacyjnym; dokumenty dotyczące zarządzania ryzykiem w organizacji; inne istotne dokumenty lub zapisy]. |
| | **PM-30-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem w organizacji]. |

| | | |
|---|---|---|
| **PM-30(01)** | **STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW \| DOSTAWCY ELEMENTÓW KRYTYCZNYCH LUB ISTOTNYCH Z PUNKTU WIDZENIA MISJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-30(01)[01]** | określono dostawców technologii, produktów i usług krytycznych lub istotnych z punktu widzenia misji; |
| | **PM-30(01)[02]** | ustala się priorytet dostawców technologii, produktów i usług krytycznych lub istotnych z punktu widzenia misji; |
| | **PM-30(01)[03]** | dokonuje się oceny dostawców technologii, produktów i usług krytycznych lub istotnych z punktu widzenia misji; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-30(01)-Badanie** | [WYBÓR SPOŚRÓD: Strategia zarządzania ryzykiem łańcucha dostaw; strategia zarządzania ryzykiem w całej organizacji; dokumenty dotyczące zarządzania ryzykiem w organizacji; dokumentacja dotycząca zapasów lub dostawców; dokumentacja dotycząca oceny i ustalania priorytetów; dokumenty lub zapisy dotyczące technologii, produktów i usług krytycznych lub istotnych z punktu widzenia misji; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PM-30(01)** | **STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW \| DOSTAWCY ELEMENTÓW KRYTYCZNYCH LUB ISTOTNYCH Z PUNKTU WIDZENIA MISJI** | |
| | **PM-30(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem w organizacji]. |
| | **PM-30(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne służące identyfikacji, ustalaniu priorytetów i ocenie technologii, produktów i usług krytycznych lub istotnych z punktu widzenia misji; procesy organizacyjne służące prowadzeniu rejestru dostawców; proces organizacyjny służący kojarzeniu dostawców z technologiami, produktami i usługami z krytycznymi lub istotnymi z punktu widzenia misji]. |

| | | |
|---|---|---|
| **PM-31** | **STRATEGIA CIĄGŁEGO MONITOROWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-31_ODP[01]** | ***określono wskaźniki dla całej organizacji, które będą monitorowane;*** |
| | **PM-31_ODP[02]** | ***określono częstotliwość monitorowania;*** |
| | **PM-31_ODP[03]** | ***określono częstotliwość oceny skuteczności zabezpieczeń;*** |
| | **PM-31_ODP[04]** | ***określono personel lub role odpowiedzialne za informowanie o stanie bezpieczeństwa systemów organizacji;*** |
| | **PM-31_ODP[05]** | ***określono personel lub role odpowiedzialne za informowanie o stanie prywatności systemów organizacji;*** |
| | **PM-31_ODP[06]** | ***określono częstotliwość informowania o stanie bezpieczeństwa systemów organizacji;*** |

| PM-31 | STRATEGIA CIĄGŁEGO MONITOROWANIA | |
|---|---|---|
| | **PM-31_ODP[07]** | ***określono częstotliwość informowania o stanie prywatności systemów organizacji;*** |
| | **PM-31** | opracowano strategię ciągłego monitorowania w całej organizacji; |
| | **PM-31a.** | wdrożono programy ciągłego monitorowania, obejmujące ustanowienie ***<wskaźników PM-31_ODP[01]>*** podlegających monitorowaniu; |
| | **PM-31b.[01]** | wdrożono programy ciągłego monitorowania określające ***<częstotliwość PM-31_ODP[02]>*** monitorowania; |
| | **PM-31b.[02]** | wdrożono programy ciągłego monitorowania określające ***<częstotliwość PM-31_ODP[03]>*** oceny skuteczności zabezpieczeń; |
| | **PM-31c.** | wdrożono programy ciągłego monitorowania, obejmujące bieżące monitorowanie ***<wskaźników PM-31_ODP[01]>*** zgodnie ze strategią ciągłego monitorowania; |
| | **PM-31d.[01]** | wdrożono programy ciągłego monitorowania, które obejmują korelację informacji generowanych w ramach ocen zabezpieczeń i monitorowania; |
| | **PM-31d.[02]** | wdrożono programy ciągłego monitorowania, które obejmują analizę informacji generowanych w ramach ocen zabezpieczeń i monitorowania; |
| | **PM-31e.[01]** | wdrożono programy ciągłego monitorowania, które obejmują reakcje podejmowane w wyniku analizy informacji z oceny zabezpieczeń; |
| | **PM-31e.[02]** | wdrożono programy ciągłego monitorowania, które obejmują reakcje podejmowane w wyniku analizy informacji z monitorowania; |
| | **PM-31f.[01]** | wdrożono programy ciągłego monitorowania, które obejmują informowanie ***<personelu lub ról PM-31_ODP[04]> o*** stanie bezpieczeństwa systemów organizacji z ***<częstotliwością PM-31_ODP[06]>***; |

| | | |
|---|---|---|
| **PM-31** | **STRATEGIA CIĄGŁEGO MONITOROWANIA** | |
| | **PM-31f.[02]** | wdrożono programy ciągłego monitorowania, które obejmują informowanie ***<personelu lub ról PM-31_ODP[05]> o*** stanie prywatności systemów organizacji z ***<częstotliwością PM-31_ODP[07]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-31-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; plan zarządzania ryzykiem łańcucha dostaw; strategia ciągłego monitorowania; strategia zarządzania ryzykiem; dokumentacja, sprawozdawczość, wskaźniki i artefakty programu ciągłego monitorowania bezpieczeństwa informacji; dokumentacja, sprawozdawczość, wskaźniki i artefakty programu ciągłego monitorowania bezpieczeństwa informacji; polityka oceny i autoryzacji; procedury dotyczące ciągłego monitorowania zabezpieczeń; dokumentacja, sprawozdawczość, wskaźniki i artefakty programu ochrony prywatności; zapisy dotyczące programu ciągłego monitorowania, analizy wpływu na bezpieczeństwo i prywatność; raporty o stanie bezpieczeństwa i prywatności; dokumentacja dotycząca reakcji na ryzyko; inne istotne dokumenty lub zapisy]. |
| | **PM-31-Wywiad** | [WYBÓR SPOŚRÓD: Wyższy urzędnik ds. zarządzania ryzykiem; kierownik ds. informacji; wyższy urzędnik ds. bezpieczeństwa informacji; wyższy urzędnik ds. prywatności; personel organizacyjny odpowiedzialny za program bezpieczeństwa informacji, prywatności i zarządzania ryzykiem w łańcuchu dostaw]. |
| | **PM-31-Test** | [WYBÓR SPOŚRÓD: Procedury i mechanizmy organizacyjne stosowane w celu zapewnienia bezpieczeństwa informacji, prywatności i ciągłego monitorowania łańcucha dostaw]. |

| | | |
|---|---|---|
| **PM-32** | **PRZEZNACZENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PM-32_ODP** | ***określono systemy lub komponenty systemu wspierające usługi lub funkcje istotne z punktu widzenia misji;*** |
| | **PM-32** | ***<systemy lub komponenty systemu PM-32_ODP>*** wspierające usługi lub funkcje istotne z punktu widzenia misji są analizowane w celu zapewnienia, że zasoby informacyjne są wykorzystywane w sposób zgodny z ich przeznaczeniem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PM-32-Badanie** | [WYBÓR SPOŚRÓD: Plan programu bezpieczeństwa informacji; plan programu ochrony prywatności; lista podstawowych usług i funkcji; organizacyjna analiza zasobów informacyjnych; strategia zarządzania ryzykiem; inne istotne dokumenty lub zapisy]. |
| | **PM-32-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za programy bezpieczeństwa informacji, prywatności i zarządzania ryzykiem łańcucha dostaw]. |

## 4.14. KATEGORIA PS - BEZPIECZEŃSTWO OSOBOWE

| | | |
|---|---|---|
| **PS-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-01_ODP[01]** | ***określono personel lub role, wśród których ma być rozpowszechniana polityka bezpieczeństwa osobowego;*** |
| | **PS-01_ODP[02]** | ***określono personel lub role, wśród których mają być rozpowszechniane procedury bezpieczeństwa osobowego;*** |
| | **PS-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **PS-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami bezpieczeństwa osobowego;*** |
| | **PS-01_ODP[05]** | ***określono częstotliwość przeglądu i aktualizacji obowiązującej polityki bezpieczeństwa osobowego;*** |
| | **PS-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji obowiązującej polityki bezpieczeństwa osobowego;*** |
| | **PS-01_ODP[07]** | ***określono częstotliwość przeglądu i aktualizacji obowiązujących procedur bezpieczeństwa osobowego;*** |
| | **PS-01_ODP[08]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji procedur bezpieczeństwa osobowego;*** |
| | **PS-01a.[01]** | opracowano i udokumentowano politykę bezpieczeństwa osobowego; |
| | **PS-01a.[02]** | polityka bezpieczeństwa osobowego jest rozpowszechniana wśród ***<personelu lub ról PS-01_ODP[01]>***; |
| | **PS-01a.[03]** | opracowano i udokumentowano procedury bezpieczeństwa osobowego ułatwiające wdrożenie polityki i powiązanych zabezpieczeń w tym zakresie; |

| **PS-01** | **POLITYKA I PROCEDURY** | |
|---|---|---|
| | **PS-01a.[04]** | procedury bezpieczeństwa osobowego są rozpowszechniane wśród ***<personelu lub ról PS-01_ODP[02]>***; |
| | **PS-01a.01(a)[01]** | polityka bezpieczeństwa osobowego ***<WYBRANA WARTOŚĆ PARAMETRU PS-01_ODP[03]>*** odnosi się do celu; |
| | **PS-01a.01(a)[02]** | polityka bezpieczeństwa osobowego ***<WYBRANA WARTOŚĆ PARAMETRU PS-01_ODP[03]>*** odnosi się do zakresu; |
| | **PS-01a.01(a)[03]** | polityka bezpieczeństwa osobowego ***<WYBRANA WARTOŚĆ PARAMETRU PS-01_ODP[03]>*** odnosi się do ról; |
| | **PS-01a.01(a)[04]** | polityka bezpieczeństwa osobowego ***<WYBRANA WARTOŚĆ PARAMETRU PS-01_ODP[03]>*** odnosi się do obowiązków ; |
| | **PS-01a.01(a)[05]** | polityka bezpieczeństwa osobowego ***<WYBRANA WARTOŚĆ PARAMETRU PS-01_ODP[03]>*** odnosi się do zaangażowania kierownictwa; |
| | **PS-01a.01(a)[06]** | polityka bezpieczeństwa osobowego ***<WYBRANA WARTOŚĆ PARAMETRU PS-01_ODP[03]>*** odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **PS-01a.01(a)[07]** | polityka bezpieczeństwa osobowego ***<WYBRANA WARTOŚĆ PARAMETRU PS-01_ODP[03]>*** odnosi się do zgodności; |
| | **PS-01a.01(b)** | polityka bezpieczeństwa osobowego ***<WYBRANA WARTOŚĆ PARAMETRU PS-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **PS-01b.** | ***<urzędnik PS-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur bezpieczeństwa osobowego; |
| | **PS-01c.01[01]** | aktualna polityka bezpieczeństwa osobowego jest przeglądana i aktualizowana z ***<częstotliwością PS-01_ODP[05]>***; |

| | | |
|---|---|---|
| **PS-01** | **POLITYKA I PROCEDURY** | |
| | **PS-01c.01[02]** | aktualna polityka bezpieczeństwa osobowego jest przeglądana i aktualizowana po ***<zdarzeniach PS-01_ODP[06]>***; |
| | **PS-01c.02[01]** | przegląd i aktualizacja procedur bezpieczeństwa osobowego odbywa się z ***<częstotliwością PS-01_ODP[07]>***; |
| | **PS-01c.02[02]** | aktualne procedury bezpieczeństwa osobowego są przeglądane i aktualizowane po ***<zdarzeniach PS-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury bezpieczeństwa osobowego; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja strategii zarządzania ryzykiem; wyniki audytu; inne istotne dokumenty lub zapisy]. |
| | **PS-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **PS-02** | **OKREŚLANIE RYZYKA DLA STANOWISKA PRACY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-02_ODP** | ***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji oznaczeń ryzyka dla stanowisk;*** |
| | **PS-02a.** | do wszystkich stanowisk w organizacji przypisane jest oznaczenie ryzyka; |
| | **PS-02b.** | ustalono kryteria sprawdzania osób obsadzających stanowiska w organizacji; |

| | | |
|---|---|---|
| **PS-02** | **OKREŚLANIE RYZYKA DLA STANOWISKA PRACY** | |
| | **PS-02c.** | oznaczenie ryzyka dla stanowiska jest przeglądane i aktualizowane z ***<częstotliwością PS-02_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury dotyczące kategoryzacji stanowisk; odpowiednie przepisy krajowe; lista oznaczeń ryzyka dla stanowisk organizacyjnych; zapisy dotyczące przeglądów i aktualizacji oznaczeń ryzyka dla stanowisk; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące nadawania, przeglądu i aktualizacji oznaczeń ryzyka dla stanowisk; procesy organizacyjne dotyczące ustanawiania kryteriów sprawdzania osób]. |

| | | |
|---|---|---|
| **PS-03** | **DOBÓR PERSONELU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-03_ODP[01]** | ***określono warunki, w których wymagane jest ponowne sprawdzenie poszczególnych osób;*** |
| | **PS-03_ODP[02]** | ***określono częstotliwość ponownego sprawdzania osób, w przypadku których jest to wskazane;*** |
| | **PS-03a.** | osoby są sprawdzane przed przyznaniem dostępu do systemu; |
| | **PS-03b.[01]** | osoby są ponownie sprawdzane zgodnie z ***<warunkami, w których wymagane jest ponowne sprawdzenie PS-03_ODP[01]>***; |

| | | |
|---|---|---|
| **PS-03** | **DOBÓR PERSONELU** | |
| | **PS-03b.[02]** | w przypadku gdy wskazane jest ponowne sprawdzenie, osoby są ponownie sprawdzane z ***<częstotliwością PS-03_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury dotyczące sprawdzania personelu; ewidencja sprawdzanego personelu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-03-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie sprawdzania personelu]. |

| | | |
|---|---|---|
| **PS-03(01)** | **DOBÓR PERSONELU \| INFORMACJE NIEJAWNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-03(01)[01]** | osoby mające dostęp do systemu przetwarzającego, przechowującego lub przekazującego informacje niejawne są sprawdzane; |
| | **PS-03(01)[02]** | osoby mające dostęp do systemu przetwarzającego, przechowującego lub przekazującego informacje niejawne posiadają poświadczenia bezpieczeństwa do najwyższego poziomu klasyfikacji informacji, do których mają dostęp w systemie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury dotyczące sprawdzania personelu; ewidencja sprawdzanego personelu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PS-03(01)** | **DOBÓR PERSONELU \| INFORMACJE NIEJAWNE** | |
| | **PS-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-03(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące sprawdzania personelu i przyznawania mu uprawnień dostępu do informacji niejawnych]. |

| | | |
|---|---|---|
| **PS-03(02)** | **DOBÓR PERSONELU \| POSTĘPOWANIA SPRAWDZAJĄCE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-03(02)** | osoby mające dostęp do systemu przetwarzającego, przechowującego lub przekazującego informacje niejawne, które wymagały przeprowadzenia postępowania sprawdzającego, posiadają poświadczenia bezpieczeństwa do najwyższego poziomu klasyfikacji informacji, do których mają dostęp w systemie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury dotyczące sprawdzania personelu; dokumenty dotyczące poświadczeń bezpieczeństwa; zapisy dotyczące sprawdzanego personelu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-03(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące postępowania sprawdzającego w zakresie wszystkich istotnych rodzajów informacji, do których personel ma dostęp]. |

| | | |
|---|---|---|
| **PS-03(03)** | **DOBÓR PERSONELU \| INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-03(03)_ODP** | ***określono dodatkowe kryteria sprawdzania personelu, które muszą być spełnione w przypadku osób mających dostęp do systemu przetwarzającego, przechowującego lub przekazującego informacje wymagające szczególnej ochrony;*** |
| | **PS-03(03)(a)** | osoby mające dostęp do systemu przetwarzającego, przechowującego lub przekazującego informacje wymagające szczególnej ochrony posiadają ważne uprawnienia dostępu, które wynikają z przydzielonych im oficjalnych obowiązków rządowych; |
| | **PS-03(03)(b)** | osoby mające dostęp do systemu przetwarzającego, przechowującego lub przekazującego informacje wymagające szczególnej ochrony spełniają ***<dodatkowe kryteria sprawdzania personelu PS-03(03)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; polityka kontroli dostępu, procedury dotyczące sprawdzania personelu; ewidencja sprawdzanego personelu; kryteria sprawdzania personelu; ewidencja upoważnień dostępu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-03(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zapewniające ważne upoważnienia dostępu do informacji wymagających szczególnej ochrony; proces organizacyjny dotyczący dodatkowego sprawdzania personelu mającego dostęp do informacji wymagających szczególnej ochrony]. |

| | | |
|---|---|---|
| **PS-03(04)** | **DOBÓR PERSONELU \| WYMAGANIA DOTYCZĄCE OBYWATELSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-03(04)_ODP[01]** | ***określono rodzaje informacji przetwarzanych, przechowywanych lub przekazywanych przez system, w przypadku których wymaga się spełnienia <wymogów dotyczących obywatelstwa PS-03(04)_ODP[02]> przez osoby mające dostęp do takich treści;*** |
| | **PS-03(04)_ODP[02]** | ***określono wymagania dotyczące obywatelstwa, które muszą spełniać osoby mające dostęp do systemu przetwarzającego, przechowującego lub przekazującego informacje;*** |
| | **PS-03(04)** | osoby mające dostęp do systemu przetwarzającego, przechowującego lub przekazującego<br>***<rodzaje informacje PS-03(04)_ODP[01]>*** spełniają ***<wymogi dotyczące obywatelstwa PS-03(04)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-03(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; polityka kontroli dostępu, procedury dotyczące sprawdzania personelu; ewidencja sprawdzanego personelu; kryteria sprawdzania personelu; ewidencja upoważnień dostępu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-03(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-03(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zapewniające upoważnienia dostępu do informacji wymagających posiadania obywatelstwa; proces organizacyjny dotyczący dodatkowego sprawdzania personelu pod kątem informacji wymagających posiadania obywatelstwa]. |

| **PS-04** | **ZAKOŃCZENIE ZATRUDNIENIA** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-04_ODP[01]** | ***określono okres, w którym należy zablokować osobie dostęp do systemu;*** |
| | **PS-04_ODP[02]** | ***określono tematy dotyczące bezpieczeństwa informacji, które należy omówić podczas przeprowadzania rozmów końcowych;*** |
| | **PS-04a.** | po zakończeniu zatrudnienia osoby fizycznej, jej dostęp do systemu zostaje zablokowany w ciągu ***<okresu PS-04_ODP[01]>***; |
| | **PS-04b.** | po zakończeniu zatrudnienia osoby fizycznej, wszelkie przyznane jej środki uwierzytelniania i poświadczenia zostają unieważnione lub cofnięte; |
| | **PS-04c.** | po zakończeniu zatrudnienia osoby fizycznej przeprowadza się rozmowę końcową, obejmującą omówienie ***<tematów związanych z bezpieczeństwem informacji PS-04_ODP[02]>***; |
| | **PS-04d.** | po zakończeniu zatrudnienia osoby fizycznej odzyskiwane są wszystkie aktywa związane z bezpieczeństwem systemu; |
| | **PS-04e.** | po zakończeniu zatrudnienia osoby fizycznej organizacja zachowuje się dostęp do informacji i systemów, które wcześniej były nadzorowane przez tę osobę. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **PS-04** | **ZAKOŃCZENIE ZATRUDNIENIA** | |
|---|---|---|
| | **PS-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury dotyczące zakończenia zatrudnienia personelu; ewidencja działań związanych z zakończeniem zatrudnienia personelu; lista kont systemowych; ewidencja unieważnionych lub cofniętych środków uwierzytelniania/poświadczeń; ewidencja rozmów końcowych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-04-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zakończenia zatrudnienia personelu; mechanizmy wspierające lub wdrażające powiadomienia o zakończeniu zatrudnienia personelu; mechanizmy wyłączania dostępu do systemu/unieważniania środków uwierzytelniania]. |

| **PS-04(01)** | **ZAKOŃCZENIE ZATRUDNIENIA \| ZOBOWIĄZANIA PO ZAKOŃCZENIU ZATRUDNIENIA** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-04(01)(a)** | osoby, z którymi rozwiązano stosunek pracy, są informowane o prawnie wiążących zobowiązaniach po zakończeniu zatrudnienia, dotyczących ochrony informacji organizacji; |
| | **PS-04(01)(b)** | w ramach procesu zakończenia zatrudnienia osoby, z którymi rozwiązano stosunek pracy, są zobowiązane do podpisania oświadczenia dotyczącego zobowiązań po zakończeniu zatrudnienia. |

| | | |
|---|---|---|
| **PS-04(01)** | **ZAKOŃCZENIE ZATRUDNIENIA \| ZOBOWIĄZANIA PO ZAKOŃCZENIU ZATRUDNIENIA** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury dotyczące rozwiązania stosunku pracy z personelem; podpisane oświadczenia dotyczące zobowiązań po zakończeniu zatrudnienia; lista prawnie wiążących zobowiązań po zakończeniu zatrudnienia; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-04(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zobowiązań po zakończeniu zatrudnienia]. |

| | | |
|---|---|---|
| **PS-04(02)** | **ZAKOŃCZENIE ZATRUDNIENIA \| AUTOMATYCZNE POWIADAMIANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-04(02)_ODP[01]** | ***określono automatyczne mechanizmy powiadamiania personelu lub ról o poszczególnych działaniach związanych z zakończeniem zatrudnienia osoby lub zablokowaniem dostępu do zasobów systemowych;*** |
| | **PS-04(02)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {powiadomienie <personelu lub ról PS-04(02)_ODP[03]> o działaniach związanych z zakończeniem zatrudnienia osoby; zablokowanie dostępu do zasobów systemowych};*** |
| | **PS-04(02)_ODP[03]** | ***określono personel lub role, które należy powiadomić o zakończeniu zatrudnienia danej osoby (jeśli wybrano);*** |

| | | |
|---|---|---|
| **PS-04(02)** | **ZAKOŃCZENIE ZATRUDNIENIA \| AUTOMATYCZNE POWIADAMIANIE** | |
| | **PS-04(02)** | stosuje się ***<mechanizmy automatyczne PS-04(02)_ODP[01]>*** do ***<WYBRANA WARTOŚĆ PARAMETRU PS-04(02)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-04(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury dotyczące zakończenia zatrudnienia personelu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; ewidencja działań związanych z zakończeniem zatrudnienia personelu; automatyczne powiadomienia o zakończeniu zatrudnienia personelu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-04(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-04(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zakończenia zatrudnienia personelu; automatyczne mechanizmy wspierające lub wdrażające powiadomienia o zakończenia zatrudnienia personelu]. |

| | | |
|---|---|---|
| **PS-05** | **OBSADZENIE LUB PRZENIESIENIE STANOWISKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-05_ODP[01]** | ***określono działania podejmowane po przeniesieniu pracownika lub ponownym obsadzeniu stanowiska;*** |
| | **PS-05_ODP[02]** | ***określono okres, w którym muszą nastąpić działania związane z przeniesieniem pracownika lub ponownym obsadzeniem stanowiska;*** |

| | | |
|---|---|---|
| **PS-05** | **OBSADZENIE LUB PRZENIESIENIE STANOWISKA** | |
| | **PS-05_ODP[03]** | ***określono personel lub role, które mają być powiadamiane o przeniesieniu osób bądź ponownym obsadzeniu stanowisk w ramach organizacji;*** |
| | **PS-05_ODP[04]** | ***określono okres, w którym należy powiadomić zdefiniowany przez organizację personel lub role o przeniesieniu osób bądź ponownym obsadzeniu stanowisk w ramach organizacji;*** |
| | **PS-05a.** | bieżące potrzeby operacyjne w zakresie aktualnych uprawnień do logicznego i fizycznego dostępu do systemów i obiektów są poddawane przeglądowi i zatwierdzane, gdy osoby są przenoszone lub następuje ponowne obsadzenie stanowisk w ramach organizacji; |
| | **PS-05b.** | ***<czynności związane z przeniesieniem pracownika lub ponownym obsadzeniem stanowiska PS-05_ODP[01]>*** są inicjowane w ciągu ***<okresu po formalnym rozpoczęciu procedury PS-05_ODP[02]>***; |
| | **PS-05c.** | uprawnienia dostępu są modyfikowane w miarę potrzeb, aby odpowiadały wszelkim zmianom w zakresie potrzeb operacyjnych, wynikającym z przeniesienia pracownika lub ponownego obsadzenia stanowiska; |
| | **PS-05d.** | ***<personel lub role PS-05_ODP[03]>*** są powiadamiane w ciągu***<okresu PS-05_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury dotyczące przenoszenia personelu; rejestry działań związanych z przenoszeniem personelu; wykaz uprawnień do dostępu do systemu i obiektów; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **PS-05** | **OBSADZENIE LUB PRZENIESIENIE STANOWISKA** | |
| | **PS-05-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **PS-06** | **UMOWY DOSTĘPU/WSPÓŁPRACY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-06_ODP[01]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji umów o dostępie;*** |
| | **PS-06_ODP[02]** | ***określono częstotliwość ponownego podpisywania umów o dostępie w celu zachowania dostępu do informacji organizacyjnych;*** |
| | **PS-06a.** | opracowano i udokumentowano umowy o dostępie do systemów organizacyjnych; |
| | **PS-06b.** | umowy o dostępie są poddawane przeglądowi i aktualizowane z ***<częstotliwością PS-06_ODP[01]>***; |
| | **PS-06c.01** | osoby wymagające dostępu do informacji i systemów organizacji podpisują odpowiednie umowy o dostępie przed uzyskaniem dostępu; |
| | **PS-06c.02** | w celu zachowania dostępu do informacji i systemów organizacji osoby wymagające takiego dostępu ponownie podpisują umowy o dostępie w przypadku aktualizacji ich treści lub co ***<częstotliwość PS-06_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **PS-06** | **UMOWY DOSTĘPU/WSPÓŁPRACY** | |
|---|---|---|
| | **PS-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury bezpieczeństwa personelu; procedury dotyczące umów o dostępie do informacji i systemów organizacyjnych; polityka kontroli dostępu; procedury kontroli dostępu; umowy o dostępie (w tym umowy o zachowaniu poufności, umowy o dopuszczalnym użytkowaniu, zasady postępowania oraz umowy dotyczące konfliktu interesów); dokumentacja przeglądów, aktualizacji i ponownego podpisywania umów o dostępie; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PS-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny, który zawarł umowy o dostępie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PS-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przeglądu, aktualizacji i ponownego podpisywania umów o dostępie; mechanizmy wspierające przegląd, aktualizację i ponowne podpisywanie umów o dostępie]. |

| **PS-06(01)** | **UMOWY DOSTEPU/WSPÓŁPRACY \| INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY** |
|---|---|
| | [WYCOFANE: Włączone do PS-03]. |

| | | |
|---|---|---|
| **PS-06(02)** | **UMOWY DOSTEPU/WSPÓŁPRACY \| INFORMACJE NIEJAWNE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-06(02)(a)** | dostęp do informacji niejawnych wymagających szczególnej ochrony przysługuje wyłącznie osobom, które posiadają ważne uprawnienia dostępu, zgodnie z przydzielonymi obowiązkami państwowymi; |
| | **PS-06(02)(b)** | dostęp do informacji niejawnych wymagających szczególnej ochrony przyznaje się wyłącznie osobom, które spełniają związane z tym kryteria bezpieczeństwa osobowego; |
| | **PS-06(02)(c)** | dostęp do informacji niejawnych wymagających szczególnej ochrony jest przyznawany wyłącznie osobom, które przeczytały, zrozumiały i podpisały umowę o zachowaniu poufności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-06(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury dotyczące umów o dostępie do informacji i systemów organizacyjnych; umowy o dostępie; upoważnienia dostępu; kryteria bezpieczeństwa osobowego; zawarte umowy o zachowaniu poufności; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-06(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny, który zawarł umowy o zachowaniu poufności; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-06(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące dostępu do informacji niejawnych wymagających szczególnej ochrony]. |

| | | |
|---|---|---|
| **PS-06(03)** | **UMOWY DOSTEPU/WSPÓŁPRACY \| WYMOGI PO ZAKOŃCZENIU ZATRUDNIENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-06(03)(a)** | osoby fizyczne są informowane o obowiązujących zobowiązaniach po zakończeniu zatrudnienia dotyczących ochrony informacji organizacyjnych; |
| | **PS-06(03)(b)** | od osób fizycznych wymaga się podpisania oświadczenia dotyczącego zobowiązań po zakończeniu zatrudnienia w ramach przyznawania pierwszego dostępu do informacji objętych ochroną. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-06(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury dotyczące umów o dostępie do informacji i systemów organizacyjnych; podpisane oświadczenia dotyczące zobowiązań po zakończeniu zatrudnienia; umowy o dostępie; lista prawnie wiążących zobowiązań po zakończeniu zatrudnienia; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-06(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny z umowami o dostępie do informacji; personel organizacyjny, który podpisał umowy o dostępie zawierające zobowiązania po zakończeniu zatrudnienia; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-06(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zobowiązań po zakończeniu zatrudnienia; mechanizmy wspierające powiadomienia i indywidualne oświadczenia dotyczące zobowiązań po zakończeniu zatrudnienia]. |

| | | |
|---|---|---|
| **PS-07** | **BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-07_ODP[01]** | ***określono personel lub role, które mają być powiadamiane o wszelkich przypadkach przeniesienia lub rozwiązania stosunku pracy z personelem zewnętrznym posiadającym poświadczenia lub identyfikatory organizacyjne lub uprawnienia systemowe;*** |
| | **PS-07_ODP[02]** | ***określono okres, w którym dostawcy zewnętrzni są zobowiązani do powiadomienia personelu lub ról określonych przez organizację o wszelkich przypadkach przeniesienia lub zakończenia stosunku pracy personelu zewnętrznego, który posiada poświadczenia lub identyfikatory organizacyjne lub uprawnienia systemowe;*** |
| | **PS-07a.** | ustanowiono wymogi bezpieczeństwa osobowego, w tym role i obowiązki w zakresie bezpieczeństwa dla dostawców zewnętrznych; |
| | **PS-07b.** | dostawcy zewnętrzni są zobowiązani do przestrzegania zasad i procedur bezpieczeństwa osobowego ustanowionych przez organizację; |
| | **PS-07c.** | wymogi dotyczące bezpieczeństwa osobowego są udokumentowane; |
| | **PS-07d.** | dostawcy zewnętrzni są zobowiązani do powiadomienia ***<personelu lub ról PS-07_ODP[01]> o*** wszelkich przypadkach przeniesienia lub zakończenia stosunku pracy personelu zewnętrznego, który posiada poświadczenia lub identyfikatory organizacyjne lub uprawnienia systemowe w ciągu ***<okresu PS-07_ODP[02]>***; |
| | **PS-07e.** | Monitoruje się przestrzeganie wymogów bezpieczeństwa osobowego przez dostawcę. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PS-07** | **BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH** | |
| | **PS-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury bezpieczeństwa dotyczące personelu zewnętrznego; wykaz wymogów bezpieczeństwa osobowego; dokumenty dotyczące zakupów; umowy o poziomie usług; proces monitorowania zgodności; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **PS-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; dostawcy zewnętrzni; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za zarządzanie kontami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **PS-07-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zarządzania i monitorowania bezpieczeństwa osobowego personelu zewnętrznego; mechanizmy wspierające lub wdrażające monitorowanie przestrzeganie wymogów przez dostawców]. |

| | | |
|---|---|---|
| **PS-08** | **SANKCJE PERSONALNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-08_ODP[01]** | ***określono personel lub role, które mają być powiadamiane o wszczęciu formalnego postępowania w sprawie sankcji wobec pracowników;*** |
| | **PS-08_ODP[02]** | ***określono okres, w którym zdefiniowany przez organizację personel lub role muszą otrzymać informację o wszczęciu formalnego postępowania w sprawie sankcji wobec pracowników;*** |
| | **PS-08a.** | stosuje się formalny proces sankcji wobec osób, które nie przestrzegają ustalonych polityk i procedur dotyczących bezpieczeństwa informacji i prywatności; |

| | | |
|---|---|---|
| **PS-08** | **SANKCJE PERSONALNE** | |
| | **PS-08b.** | ***<personel lub role PS-08_ODP[01]>*** są powiadamiane w ciągu ***<okresu PS-08_ODP[02]>*** o wszczęciu formalnego postępowania w sprawie sankcji, wraz ze wskazaniem osoby nimi objętej oraz przyczyn ich nałożenia. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury bezpieczeństwa osobowego; procedury dotyczące sankcji wobec pracowników; umowy o dostępie (w tym umowy o zachowaniu poufności, umowy o dopuszczalnym użytkowaniu, zasady postępowania oraz umowy dotyczące konfliktu interesów); wykaz personelu lub ról, które należy powiadomić o formalnych sankcjach wobec pracowników; zapisy lub powiadomienia dotyczące formalnych sankcji wobec pracowników; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka przetwarzania informacji umożliwiających identyfikację osób; inne istotne dokumenty lub zapisy]. |
| | **PS-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; radca prawny; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PS-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zarządzania formalnymi sankcjami wobec pracowników; mechanizmy wspierające lub wdrażające formalne powiadomienia o sankcjach wobec pracowników]. |

| | | |
|---|---|---|
| **PS-09** | **OPISY STANOWISK PRACY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PS-09[01]** | role i obowiązki w zakresie bezpieczeństwa są włączone do opisów stanowisk organizacyjnych; |

| | | |
|---|---|---|
| **PS-09** | **OPISY STANOWISK PRACY** | |
| | **PS-09[02]** | role i obowiązki w zakresie prywatności są włączone do opisów stanowisk organizacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PS-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka bezpieczeństwa osobowego; procedury bezpieczeństwa osobowego; procedury dotyczące opisów stanowisk; opisy stanowisk odpowiedzialnych za bezpieczeństwo i prywatność; plan bezpieczeństwa systemu; plan ochrony prywatności; plan programu ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PS-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo osobowe; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za zarządzanie kapitałem ludzkim]. |
| | **PS-09-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zarządzania opisami stanowisk]. |

## 4.15. KATEGORIA PT - PRZEJRZYSTOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH

| | | |
|---|---|---|
| **PT-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-01_ODP[01]** | ***określono personel lub role, wśród których ma być rozpowszechniana polityka przetwarzania i przejrzystości danych identyfikacyjnych;*** |
| | **PT-01_ODP[02]** | ***określono personel lub role, wśród których mają być rozpowszechniane procedury przetwarzania i przejrzystości danych identyfikacyjnych;*** |
| | **PT-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **PT-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami przetwarzania i przejrzystości danych identyfikacyjnych;*** |
| | **PT-01_ODP[05]** | ***określono częstotliwość przeglądu i aktualizacji obowiązującej polityki przetwarzania i przejrzystości danych identyfikacyjnych;*** |
| | **PT-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji obowiązującej polityki przetwarzania i przejrzystości danych identyfikacyjnych;*** |
| | **PT-01_ODP[07]** | ***określono częstotliwość przeglądu i aktualizacji obowiązujących procedur przetwarzania i przejrzystości danych identyfikacyjnych;*** |
| | **PT-01_ODP[08]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji obowiązujących procedur przetwarzania i przejrzystości danych identyfikacyjnych;*** |
| | **PT-01a.[01]** | opracowano i udokumentowano politykę przetwarzania i przejrzystości danych identyfikacyjnych; |

| **PT-01** | **POLITYKA I PROCEDURY** | |
|---|---|---|
| | **PT-01a.[02]** | polityka przetwarzania i przejrzystości danych identyfikacyjnych jest rozpowszechniana wśród ***<personelu lub ról PT-01_ODP[01]>***; |
| | **PT-01a.[03]** | opracowano i udokumentowano procedury przetwarzania i przejrzystości danych identyfikacyjnych, które ułatwiają wdrożenie polityki przetwarzania i przejrzystości takich danych, a także powiązane zabezpieczenia w zakresie ich przetwarzania i przejrzystości; |
| | **PT-01a.[04]** | procedury przetwarzania i przejrzystości danych identyfikacyjnych są rozpowszechniane wśród ***<personelu lub ról PT-01_ODP[02]>***; |
| | **PT-01a.01(a)[01]** | polityka przetwarzania danych identyfikacyjnych i przejrzystości ***<WYBRANA WARTOŚĆ PARAMETRU PT-01_ODP[03]>*** odnosi się do celu; |
| | **PT-01a.01(a)[02]** | polityka przetwarzania danych identyfikacyjnych i przejrzystości ***<WYBRANA WARTOŚĆ PARAMETRU PT-01_ODP[03]>*** odnosi się do zakresu; |
| | **PT-01a.01(a)[03]** | polityka przetwarzania danych identyfikacyjnych i przejrzystości ***<WYBRANA WARTOŚĆ PARAMETRU PT-01_ODP[03]>*** odnosi się do ról; |
| | **PT-01a.01(a)[04]** | polityka przetwarzania danych identyfikacyjnych i przejrzystości ***<WYBRANA WARTOŚĆ PARAMETRU PT-01_ODP[03]>*** odnosi się do obowiązków; |
| | **PT-01a.01(a)[05]** | polityka przetwarzania danych identyfikacyjnych i przejrzystości ***<WYBRANA WARTOŚĆ PARAMETRU PT-01_ODP[03]>*** odnosi się do zaangażowania kierownictwa; |
| | **PT-01a.01(a)[06]** | polityka przetwarzania danych identyfikacyjnych i przejrzystości ***<WYBRANA WARTOŚĆ PARAMETRU PT-01_ODP[03]>*** odnosi się do koordynacji pomiędzy podmiotami organizacji; |

| | | |
|---|---|---|
| **PT-01** | **POLITYKA I PROCEDURY** | |
| | **PT-01a.01(a)[07]** | polityka przetwarzania danych identyfikacyjnych i przejrzystości ***<WYBRANA WARTOŚĆ PARAMETRU PT-01_ODP[03]>*** odnosi się do zgodności; |
| | **PT-01a.01(b)** | polityka przetwarzania danych identyfikacyjnych i przejrzystości ***<WYBRANA WARTOŚĆ PARAMETRU PT-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **PT-01b.** | ***<urzędnik PT-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur przetwarzania danych identyfikacyjnych i przejrzystości; |
| | **PT-01c.01[01]** | polityka przetwarzania i przejrzystości danych identyfikacyjnych jest poddawana przeglądowi i aktualizowana z ***<częstotliwością PT-01_ODP[05]>;*** |
| | **PT-01c.01[02]** | polityka przetwarzania i przejrzystości danych identyfikacyjnych jest poddawana przeglądowi i aktualizowana po***<zdarzeniach PT-01_ODP[06]>;*** |
| | **PT-01c.02[01]** | procedury przetwarzania i przejrzystości danych identyfikacyjnych są poddawane przeglądowi i aktualizowane z ***<częstotliwością PT-01_ODP[07]>;*** |
| | **PT-01c.02[02]** | procedury przetwarzania i przejrzystości danych identyfikacyjnych są poddawane przeglądowi i aktualizowane po ***<zdarzeniach PT-01_ODP[08]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; plan ochrony prywatności; plan programu ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PT-01** | **POLITYKA I PROCEDURY** | |
| | **PT-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PT-02** | **UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-02_ODP[01]** | ***określono uprawnienia do zezwalania na przetwarzanie (zdefiniowane w PT-02_ODP[02]) danych identyfikacyjnych;*** |
| | **PT-02_ODP[02]** | ***określono sposób przetwarzania danych identyfikacyjnych;*** |
| | **PT-02_ODP[03]** | ***określono sposób przetwarzania danych identyfikacyjnych, który ma zostać ograniczony;*** |
| | **PT-02a.** | określono i udokumentowano ***<uprawnienia PT-02_ODP[01]>***, które pozwalają na ***<przetwarzanie PT-02_ODP[02]>*** danych identyfikacyjnych; |
| | **PT-02b.** | ***<przetwarzanie PT-02_ODP[03]>*** danych identyfikacyjnych obejmuje wyłącznie zatwierdzone sposoby przetwarzania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PT-02** | **UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH** | |
| | **PT-02-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i prywatność]. |

| | | |
|---|---|---|
| **PT-02(01)** | **UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH \| OZNACZANIE DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-02(01)_ODP[01]** | ***określono autoryzowane sposoby przetwarzania danych identyfikacyjnych;*** |
| | **PT-02(01)_ODP[02]** | ***określono elementy danych identyfikacyjnych, które mają być oznakowane;*** |
| | **PT-02(01)** | znaczniki danych zawierające ***<autoryzowane sposoby przetwarzania PT-02(01)_ODP[01]>*** są dołączone do ***<elementów danych identyfikacyjnych PT-02(01)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-02(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych, w tym procedury dotyczące oznaczania danych; definicje oznaczania danych; udokumentowane wymagania dotyczące stosowania i monitorowania oznaczania danych; fragmenty danych z odpowiadającymi im oznaczeniami danych; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-02(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PT-02(01)** | **UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH \| OZNACZANIE DANYCH** | |
| | **PT-02(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące autoryzacji przetwarzania danych identyfikacyjnych; procesy organizacyjne dotyczące znakowania danych; mechanizmy stosowania i monitorowania znakowania danych; mechanizmy wspierające lub wdrażające ograniczenie przetwarzania danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **PT-02(02)** | **UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH \| AUTOMATYZACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-02(02)_ODP** | ***określono automatyczne mechanizmy stosowane do zarządzania egzekwowaniem upoważnień do przetwarzania danych identyfikacyjnych;*** |
| | **PT-02(02)** | egzekwowaniem upoważnień do przetwarzania danych identyfikacyjnych zarządza się przy użyciu ***<automatycznych mechanizmów PT-02(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-02(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące upoważnień do przetwarzania danych identyfikacyjnych; automatyczne mechanizmy wspierające lub wdrażające zarządzanie autoryzowanym przetwarzaniem danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **PT-03** | **CELE PRZETWARZANIA DANYCH OSOBOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-03_ODP[01]** | ***określono cel(e) przetwarzania danych identyfikacyjnych;*** |
| | **PT-03_ODP[02]** | ***określono sposoby przetwarzania danych identyfikacyjnych, które mają zostać ograniczone;*** |
| | **PT-03_ODP[03]** | ***określono mechanizmy, które mają zostać wdrożone w celu zapewnienia, że wszelkie zmiany w przetwarzaniu danych identyfikacyjnych są dokonywane zgodnie z wymogami;*** |
| | **PT-03_ODP[04]** | ***określono wymagania dotyczące zmiany sposobów przetwarzania danych identyfikacyjnych;*** |
| | **PT-03a.** | zidentyfikowano i udokumentowano ***<PT-03_ODP[01] cel(e)>*** przetwarzania danych identyfikacyjnych; |
| | **PT-03b.[01]** | cel(e) opisano w polityce ochrony prywatności organizacji; |
| | **PT-03b.[02].** | cel(e) opisano w polityce organizacji; |
| | **PT-03c.** | ***<przetwarzanie PT-03_ODP[02]>*** danych identyfikacyjnych jest ograniczone tylko do tych danych, które są zgodne z określonym celem (celami); |
| | **PT-03d.[01]** | monitorowane są zmiany w przetwarzaniu danych identyfikacyjnych; |
| | **PT-03d.[02]** | wdrożono ***<PT-03_ODP[03] mechanizmy>*** w celu zapewnienia, że wszelkie zmiany są dokonywane zgodnie z ***<wymaganiami PT-03_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| PT-03 | CELE PRZETWARZANIA DANYCH OSOBOWYCH | |
|---|---|---|
| | **PT-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; plan zarządzania konfiguracją; organizacyjna polityka ochrony prywatności; polityka organizacji; oświadczenia zgodne z ustawą o ochronie danych; zawiadomienia o komputerowym dopasowaniu danych; stosowne informacje publikowane w odpowiednim rejestrze krajowym; udokumentowane wymagania dotyczące egzekwowania i monitorowania przetwarzania danych identyfikacyjnych; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-03-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące autoryzacji przetwarzania danych identyfikacyjnych; mechanizmy wspierające lub wdrażające zarządzanie autoryzowanym przetwarzaniem danych identyfikacyjnych; procesy organizacyjne dotyczące monitorowania zmian w przetwarzaniu danych identyfikacyjnych]. |

| PT-03(01) | CELE PRZETWARZANIA DANYCH OSOBOWYCH \|OZNACZANIE DANYCH | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-03(01)_ODP[01]** | ***określono cele przetwarzania, które mają być zawarte w znacznikach danych;*** |
| | **PT-03(01)_ODP[02]** | ***określono elementy danych identyfikacyjnych, które mają być oznakowane;*** |

| **PT-03(01)** | **CELE PRZETWARZANIA DANYCH OSOBOWYCH \|OZNACZANIE DANYCH** | |
|---|---|---|
| | **PT-03(01)** | znaczniki danych określające ***<cele przetwarzania PT-03(01)_ODP[01]>*** są dołączane do ***<elementów danych identyfikacyjnych PT-03(01)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; udokumentowany opis sposobu wykorzystania znaczników danych do identyfikacji elementów informacji identyfikacyjnych oraz ich dozwolonych zastosowań; schemat znaczników danych; fragmenty danych z odpowiadającymi im znacznikami danych; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie i przejrzystość danych identyfikacyjnych; personel organizacyjny odpowiedzialny za znakowanie danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-03(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące autoryzacji przetwarzania danych identyfikacyjnych; mechanizmy wspierające lub wdrażające znakowanie danych]. |

| **PT-03(02)** | **CELE PRZETWARZANIA DANYCH OSOBOWYCH \| AUTOMATYZACJA** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-03(02)_ODP** | ***określono automatyczne mechanizmy monitorowania celów przetwarzania danych identyfikacyjnych;*** |

| | | |
|---|---|---|
| **PT-03(02)** | **CELE PRZETWARZANIA DANYCH OSOBOWYCH \| AUTOMATYZACJA** | |
| | **PT-03(02)** | cele przetwarzania danych identyfikacyjnych są monitorowane przy użyciu<br>***<automatycznych mechanizmów PT-03(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; fragmenty danych z odpowiednimi znacznikami danych; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-03(02)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie i przejrzystość danych identyfikacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PT-04** | **ZGODY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-04_ODP** | ***określono narzędzia lub mechanizmy, które należy wdrożyć, aby osoby fizyczne mogły wyrazić zgodę na przetwarzanie swoich danych identyfikacyjnych;*** |
| | **PT-04** | wdrożono ***<narzędzia lub mechanizmy PT-04_ODP>*** umożliwiające osobom fizycznym wyrażenie zgody na przetwarzanie takich danych przed ich zebraniem, które ułatwiają osobom fizycznym podejmowanie świadomych decyzji. |

| | | |
|---|---|---|
| **PT-04** | **ZGODY** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka i procedury wyrażania zgody; narzędzia i mechanizmy wyrażania zgody; prezentacja lub wyświetlanie zgody (interfejs użytkownika); dowody wyrażenia zgody przez osoby fizyczne; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-04-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące gromadzenia danych identyfikacyjnych; narzędzia lub mechanizmy do wyrażania zgody przez użytkowników na przetwarzanie ich danych identyfikacyjnych; mechanizmy wdrażania zgody]. |

| | | |
|---|---|---|
| **PT-04(01)** | **ZGODY \| ZGODA NA PODSTAWIE ART. 6 UST. 1 RODO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-04(01)_ODP** | ***określono mechanizmy dostosowawcze do przetwarzania wybranych elementów uprawnień umożliwiających dostęp do danych identyfikacyjnych;*** |
| | **PT-04(01)** | zapewniono ***<mechanizmy PT-04(01)_ODP>*** umożliwiające osobom fizycznym dostosowanie uprawnień do przetwarzania wybranych elementów danych identyfikacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **PT-04(01)** | **ZGODY \| ZGODA NA PODSTAWIE ART. 6 UST. 1 RODO** | |
|---|---|---|
| | **PT-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka i procedury wyrażania zgody; narzędzia i mechanizmy wyrażania zgody; prezentacja lub wyświetlanie zgody (interfejs użytkownika); plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie i przejrzystość danych identyfikacyjnych; personel organizacyjny odpowiedzialny za interfejs użytkownika lub doświadczenia użytkownika;<br>personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-04(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wyrażania zgody na przetwarzanie danych identyfikacyjnych; narzędzia lub mechanizmy do wyrażania zgody; mechanizmy wdrażające wyrażanie zgody]. |

| **PT-04(02)** | **ZGODY \| ZGODA TYPU „JUST-IN-TIME”** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-04(02)_ODP[01]** | ***określono mechanizmy wyrażania zgody, o których należy informować osoby fizyczne;*** |
| | **PT-04(02)_ODP[02]** | ***określono częstotliwość, z jaką należy informować osoby fizyczne o mechanizmach wyrażania zgody;*** |
| | **PT-04(02)_ODP[03]** | ***określono sposoby przetwarzania danych identyfikacyjnych, o których należy informować w połączeniu z mechanizmami wyrażania zgody zdefiniowanymi przez organizację;*** |

| **PT-04(02)** | **ZGODY \| ZGODA TYPU „JUST-IN-TIME”** | |
|---|---|---|
| | **PT-04(02)** | osoby fizyczne są informowane o ***<mechanizmach wyrażania zgody PT-04(02)_ODP[01]>***<br>z ***<częstotliwością PT-04(02)_ODP[02]> oraz w*** związku z ***<przetwarzaniem danych identyfikacyjnych PT-04(02)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-04(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka i procedury udzielania zgody; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-04(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie i przejrzystość danych identyfikacyjnych; personel organizacyjny odpowiedzialny za interfejs użytkownika lub doświadczenia użytkownika;<br>personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-04(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące gromadzenia danych identyfikacyjnych; mechanizmy uzyskiwania od użytkowników zgody typu „just-in-time” na przetwarzanie ich danych identyfikacyjnych; mechanizmy wyrażania zgody typu „just-in-time”]. |

| **PT-04(03)** | **ZGODY \| WYCOFANIE ZGODY** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-04(03)_ODP** | ***określono narzędzia lub mechanizmy, które należy wdrożyć, aby osoby fizyczne mogły wycofać wyrażoną zgodę na przetwarzanie swoich danych identyfikacyjnych;*** |

| | | |
|---|---|---|
| **PT-04(03)** | **ZGODY \| WYCOFANIE ZGODY** | |
| | **PT-04(03)** | wdrożono ***<narzędzia lub mechanizmy PT-04(03)_ODP>*** umożliwiające osobom fizycznym wycofanie wyrażonej zgody na przetwarzanie danych identyfikacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-04(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka i procedury cofnięcia zgody; interfejs użytkownika lub doświadczenia użytkownika związane z wycofaniem zgody; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-04(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie i przejrzystość danych identyfikacyjnych; personel organizacyjny odpowiedzialny za interfejs użytkownika lub doświadczenia użytkownika;<br>personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-04(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wyrażania zgody na przetwarzanie danych identyfikacyjnych; narzędzia lub mechanizmy służące do wycofania zgody]. |

| | | |
|---|---|---|
| **PT-05** | **INFORMACJA O OCHRONIE PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-05_ODP[01]** | ***określono częstotliwość, z jaką osobom fizycznym dostarczane jest powiadomienie po pierwszej interakcji z organizacją;*** |
| | **PT-05_ODP[02]** | ***określono informacje, które należy zamieścić w powiadomieniu o przetwarzaniu danych identyfikacyjnych;*** |

| | | |
|---|---|---|
| **PT-05** | **INFORMACJA O OCHRONIE PRYWATNOŚCI** | |
| | **PT-05a.[01]** | powiadomienie dla osób fizycznych o przetwarzaniu danych identyfikacyjnych jest dostarczane w taki sposób, że jest ono dostępna dla osób fizycznych przy pierwszej interakcji z organizacją; |
| | **PT-05a.[02]** | powiadomienie dla osób fizycznych o przetwarzaniu danych identyfikacyjnych jest przekazywane w taki sposób, że w późniejszym czasie jest ono dostępne dla takich osób z ***<częstotliwością PT-05_ODP[01]>***; |
| | **PT-05b.** | przekazywane powiadomienie dla osób fizycznych o przetwarzaniu danych identyfikacyjnych jest sformułowane w sposób jasny i łatwy do zrozumienia, a zawarte w nim informacje o przetwarzaniu danych identyfikacyjnych są napisane prostym językiem; |
| | **PT-05c.** | przekazywane powiadomienie dla osób fizycznych o przetwarzaniu danych identyfikacyjnych wskazuje organ upoważniający do przetwarzania danych identyfikacyjnych; |
| | **PT-05d.** | przekazywane powiadomienie dla osób fizycznych o przetwarzaniu danych identyfikacyjnych określa cel przetwarzania takich danych; |
| | **PT-05e.** | przekazywane powiadomienie dla osób fizycznych o przetwarzaniu danych identyfikacyjnych zawiera ***<informacje PT-05_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka prywatności; oświadczenia zgodne z ustawą o ochronie danych; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PT-05** | **INFORMACJA O OCHRONIE PRYWATNOŚCI** | |
| | **PT-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie i przejrzystość danych identyfikacyjnych; personel organizacyjny odpowiedzialny za interfejs użytkownika lub doświadczenia użytkownika;<br>personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-05-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie i przejrzystość danych identyfikacyjnych; personel organizacyjny odpowiedzialny za interfejs użytkownika lub doświadczenia użytkownika; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PT-05(01)** | **INFORMACJA O OCHRONIE PRYWATNOŚCI \| INFORMACJA NA ŻĄDANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-05(01)_ODP** | ***określono częstotliwość, z jaką należy przedstawiać powiadomienie o przetwarzaniu danych identyfikacyjnych;*** |
| | **PT-05(01)** | powiadomienie o przetwarzaniu danych identyfikacyjnych jest przedstawiane osobom fizycznym w czasie i miejscu, w którym osoby te podają takie dane, w związku z działaniem na danych lub z ***<częstotliwością PT-05(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-05(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka ochrony prywatności; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PT-05(01)** | **INFORMACJA O OCHRONIE PRYWATNOŚCI \| INFORMACJA NA ŻĄDANIE** | |
| | **PT-05(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie i przejrzystość danych identyfikacyjnych; personel organizacyjny odpowiedzialny za interfejs użytkownika lub doświadczenia użytkownika;<br>personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-05(01)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie i przejrzystość danych identyfikacyjnych; personel organizacyjny odpowiedzialny za interfejs użytkownika lub doświadczenia użytkownika; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PT-05(02)** | **INFORMACJA O OCHRONIE PRYWATNOŚCI \| OŚWIADCZENIE O OCHRONIE PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-05(02)** | Oświadczenia zgodne z przepisami o ochronie prywatności są zawarte w formularzach do zbierania informacji, które będą przechowywane w rejestrze zgodnym z tymi przepisami, lub oświadczenia zgodne z przepisami o ochronie prywatności są dostarczane na odrębnych formularzach, które mogą być przechowywane przez osoby fizyczne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-05(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka ochrony prywatności; system rejestrów zgodny z ustawą o ochronie danych; formularze zawierające oświadczenia zgodne z przepisami o ochronie prywatności; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **PT-05(02)** | **INFORMACJA O OCHRONIE PRYWATNOŚCI \| OŚWIADCZENIE O OCHRONIE PRYWATNOŚCI** | |
| | **PT-05(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-05(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące umieszczania oświadczeń zgodnych z ustawą o ochronie danych w formularzach zbierających informacje lub na oddzielnych formularzach, które mogą być przechowywane przez osoby fizyczne]. |

| | | |
|---|---|---|
| **PT-06** | **SYSTEM ZAWIADOMIEŃ O REJESTRACH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-06a.[01]** | zawiadomienia o systemie rejestrów sporządzane są zgodnie z wytycznymi odpowiedniego organu dla systemów przetwarzających informacje przechowywane w systemie rejestrów zgodnym z ustawą o ochronie danych; |
| | **PT-06a.[02]** | nowe i znacząco zmodyfikowane zawiadomienia o systemie rejestrów są przedkładane odpowiedniemu organowi i właściwym komisjom parlamentarnym w celu dokonania wcześniejszego przeglądu systemów przetwarzających informacje przechowywane w systemie rejestrów zgodnym z ustawą o ochronie danych; |
| | **PT-06b.** | zawiadomienia o systemie rejestrów, dotyczące systemów przetwarzających informacje przechowywane w systemie rejestrów zgodnym z ustawą o ochronie danych, są publikowane w odpowiednim rejestrze krajowym; |

| | | |
|---|---|---|
| **PT-06** | **SYSTEM ZAWIADOMIEŃ O REJESTRACH** | |
| | **PT-06c.** | zawiadomienia o systemie rejestrów są dokładne, aktualne i obejmują zakres zgodny z polityką obowiązującą w odniesieniu do systemów przetwarzających informacje przechowywane w systemie rejestrów zgodnym z ustawą o ochronie danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka ochrony prywatności; system rejestrów zgodny z ustawą o ochronie danych; zawiadomienia o odpowiednim rejestrze krajowym; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne służące utrzymaniu rejestru zgodnego z ustawą o ochronie danych]. |

| | | |
|---|---|---|
| **PT-06(01)** | **SYSTEM ZAWIADOMIEŃ O REJESTRACH \| RUTYNOWE ZASTOSOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-06(01)_ODP** | ***określono częstotliwość, z jaką należy dokonywać przeglądu wszystkich rutynowych zastosowań określonych w zawiadomieniu o systemie rejestrów;*** |

| | | |
|---|---|---|
| **PT-06(01)** | **SYSTEM ZAWIADOMIEŃ O REJESTRACH \| RUTYNOWE ZASTOSOWANIA** | |
| | **PT-06(01)** | wszystkie rutynowe zastosowania określone w zawiadomieniu o systemie rejestrów są poddawane przeglądowi z ***<częstotliwością PT-06(01)_ODP>*** w celu zapewnienia ciągłej dokładności, a także zapewnienia, że zastosowania te pozostają zgodne z celem gromadzenia informacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-06(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka ochrony prywatności; system rejestrów zgodny z ustawą o ochronie danych; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-06(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-06(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przeglądania zawiadomień o systemie rejestrów]. |

| | | |
|---|---|---|
| **PT-06(02)** | **SYSTEM ZAWIADOMIEŃ O REJESTRACH \| ZASADY WYŁĄCZENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-06(02)_ODP** | ***określono częstotliwość, z jaką należy dokonywać przeglądu wszystkich zwolnień ze stosowania przepisów ustawy o ochronie danych, zgłaszanych w odniesieniu do systemu rejestrów;*** |
| | **PT-06(02)[01]** | wszystkie zwolnienia ze stosowania przepisów o ochronie prywatności zgłoszone w odniesieniu do systemu rejestrów są poddawane przeglądowi z ***<częstotliwością PT-06(02)_ODP>*** w celu zapewnienia, że są one odpowiednie i niezbędne zgodnie z prawem; |

| | | |
|---|---|---|
| **PT-06(02)** | **SYSTEM ZAWIADOMIEŃ O REJESTRACH \| ZASADY WYŁĄCZENIA** | |
| | **PT-06(02)[02]** | wszystkie zwolnienia ze stosowania przepisów o ochronie prywatności zgłoszone w odniesieniu do systemu rejestrów są poddawane przeglądowi z ***<częstotliwością PT-06(02)_ODP w*** celu zapewnienia, że zostały ogłoszone jako regulacje; |
| | **PT-06(02)[03]** | wszystkie zwolnienia ze stosowania przepisów o ochronie prywatności zgłoszone w odniesieniu do systemu rejestrów są poddawane przeglądowi z ***<częstotliwością PT-06(02)_ODP w*** celu zapewnienia, że zostały dokładnie opisane w zawiadomieniu o systemie rejestrów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-06(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka ochrony prywatności; system rejestrów zgodny z ustawą o ochronie danych; wyłączenia ze stosowania przepisów o ochronie prywatności; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-06(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-06(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne służące utrzymaniu rejestru zgodnego z ustawą o ochronie danych]. |

| | | |
|---|---|---|
| **PT-07** | **SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-07_ODP** | ***określono warunki przetwarzania, które mają być stosowane w odniesieniu do konkretnych kategorii danych identyfikacyjnych;*** |

| | | |
|---|---|---|
| **PT-07** | **SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH** | |
| | **PT-07** | ***<warunki przetwarzania PT-07_ODP>*** są stosowane w przypadku określonych kategorii danych identyfikacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; dane dotyczące prywatności; system rejestrów zgodny z ustawą o ochronie danych; umowy i zawiadomienia o komputerowym dopasowaniu danych; umowy; umowy o udostępnianiu informacji dotyczących prywatności; protokoły ustaleń; wymogi regulacyjne; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-07-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne wspierające lub wdrażające przetwarzanie danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **PT-07(01)** | **SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH \| IDENTYFIKATOR OSOBY - NP. NUMER PESEL** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-07(01)(a)[01]** | jeżeli system przetwarza identyfikatory osób, to eliminuje się niepotrzebne gromadzenie, utrzymywanie i wykorzystywanie takich identyfikatorów; |
| | **PT-07(01)(a)[02]** | jeżeli system przetwarza identyfikatory osób, to wówczas bada się alternatywy dla stosowania takich identyfikatorów; |

| | | |
|---|---|---|
| **PT-07(01)** | **SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH \| IDENTYFIKATOR OSOBY - NP. NUMER PESEL** | |
| | **PT-07(01)(b)** | jeżeli system przetwarza identyfikatory osób, nie uniemożliwia się osobie skorzystania z indywidualnych praw, świadczeń lub przywilejów przewidzianych prawem z powodu odmowy ujawnienia identyfikatora; |
| | **PT-07(01)(c)[01]** | jeżeli system przetwarza identyfikatory osób, każda osoba poproszona o ujawnienie swojego identyfikatora jest informowana o tym, czy ujawnienie to jest obowiązkowe czy dobrowolne, na podstawie jakich przepisów lub innych uprawnień jest on pozyskiwany oraz w jaki sposób będzie wykorzystywany; |
| | **PT-07(01)(c)[02]** | jeżeli system przetwarza identyfikatory osób, każda osoba, która jest proszona o ujawnienie swojego identyfikatora, jest informowana o tym, na podstawie jakich przepisów lub innych uprawnień jest on pozyskiwany; |
| | **PT-07(01)(c)[03]** | jeżeli system przetwarza numery identyfikatorów osób, każda osoba poproszona o ujawnienie swojego identyfikatora jest informowana o tym, w jaki sposób zostanie on wykorzystany. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-07(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; informacja o ochronie prywatności; system rejestrów zgodny z ustawą o ochronie danych; polityka ochrony prywatności; oddzielna informacja dotycząca korzystania z identyfikatorów osób; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-07(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **PT-07(01)** | **SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH \| IDENTYFIKATOR OSOBY - NP. NUMER PESEL** | |
| | **PT-07(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące identyfikacji, przeglądu i podejmowania działań w celu kontroli zbędnego wykorzystania identyfikatorów osób; wdrożenie alternatywy dla wykorzystywania identyfikatorów osób]. |

| | | |
|---|---|---|
| **PT-07(02)** | **SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH \| PRZETWARZANIE WRAŻLIWYCH DANYCH OSOBOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-07(02)** | przetwarzanie informacji opisujących sposób, w jaki osoba korzysta z przysługujących jej praw, jest zabronione, chyba że jest to wyraźnie dopuszczone przez ustawę lub przez daną osobę, lub też mieści się w zakresie dozwolonych działań organów ścigania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **PT-07(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka ochrony prywatności; system rejestrów zgodny z ustawą o ochronie danych; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-07(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-07(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne wspierające lub wdrażające przetwarzanie danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **PT-08** | **WYMAGANIA DOTYCZĄCE ZGODNOŚCI PRZY PRZETWARZANIU KOMPUTEROWOWYM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **PT-08a.** | rada ds. integralności danych wydała zgodę na przeprowadzenie programu dopasowania, jeżeli system lub organizacja przetwarza informacje w celu zrealizowania programu dopasowania; |
| | **PT-08b.[01]** | sporządzono umowę o komputerowym dopasowaniu danych, jeżeli system lub organizacja przetwarza informacje w celu realizacji programu dopasowania; |
| | **PT-08b.[02]** | zawarto umowę o komputerowym dopasowaniu danych, jeżeli system lub organizacja przetwarza informacje w celu realizacji programu dopasowania; |
| | **PT-08c.** | w rejestrze krajowym opublikowano zawiadomienie o komputerowym dopasowaniu danych, jeżeli system lub organizacja przetwarza informacje w celu realizacji programu dopasowania; |
| | **PT-08d.** | jeśli jest to wymagane, w przypadku gdy system lub organizacja przetwarza informacje w celu realizacji programu dopasowania informacje uzyskane w drodze jego implementacji są niezależnie weryfikowane przed podjęciem niekorzystnych działań wobec osoby fizycznej; |
| | **PT-08e.[01]** | osoby fizyczne otrzymują powiadomienie, gdy system lub organizacja przetwarza informacje w celu realizacji programu dopasowania; |
| | **PT-08e.[02]** | osoby fizyczne mają możliwość zakwestionowania ustaleń przed podjęciem wobec nich niekorzystnych działań, gdy system lub organizacja przetwarza informacje w celu realizacji programu dopasowania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **PT-08** | **WYMAGANIA DOTYCZĄCE ZGODNOŚCI PRZY PRZETWARZANIU KOMPUTEROWOWYM** | |
| | **PT-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury przetwarzania i przejrzystości danych identyfikacyjnych; polityka ochrony prywatności; system rejestrów zgodny z ustawą o ochronie danych; zawiadomienia o odpowiednim rejestrze krajowym; ustalenia rady ds. integralności danych; umowy; umowy o wymianie informacji; protokoły ustaleń; wymogi regulacyjne; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **PT-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przetwarzanie danych identyfikacyjnych i przejrzystość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **PT-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne wspierające lub wdrażające przetwarzanie danych identyfikacyjnych; program dopasowania]. |

## 4.16. KATEGORIA RA - OCENA RYZYKA

| | | |
|---|---|---|
| **RA-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-01_ODP[01]** | ***określono personel lub role, wśród których ma być rozpowszechniana polityka oceny ryzyka;*** |
| | **RA-01_ODP[02]** | ***określono personel lub role, wśród których mają być rozpowszechniane procedury oceny ryzyka;*** |
| | **RA-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **RA-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami oceny ryzyka;*** |
| | **RA-01_ODP[05]** | ***określono częstotliwość, z jaką dokonuje się przeglądu i aktualizacji bieżącej polityki oceny ryzyka;*** |
| | **RA-01_ODP[06]** | ***określono zdarzenia wymagające przeglądu i aktualizacji obecnej polityki oceny ryzyka;*** |
| | **RA-01_ODP[07]** | ***określono częstotliwość, z jaką dokonuje się przeglądu i aktualizacji obecnych procedur oceny ryzyka;*** |
| | **RA-01_ODP[08]** | ***określono zdarzenia wymagające przeglądu i aktualizacji obecnych procedur oceny ryzyka;*** |
| | **RA-01a.[01]** | opracowano i udokumentowano politykę oceny ryzyka; |
| | **RA-01a.[02]** | polityka oceny ryzyka jest rozpowszechniana wśród ***<personelu lub ról RA-01_ODP[01]>***; |
| | **RA-01a.[03]** | opracowano i udokumentowano procedury oceny ryzyka ułatwiające wdrożenie polityki oceny ryzyka i związanych z nią zabezpieczeń w zakresie oceny ryzyka; |

| | | |
|---|---|---|
| **RA-01** | **POLITYKA I PROCEDURY** | |
| | **RA-01a.[04]** | procedury oceny ryzyka są rozpowszechniane wśród ***<personelu lub ról RA-01_ODP[02]>***; |
| | **RA-01a.01(a)[01]** | polityka oceny ryzyka ***<WYBRANA WARTOŚĆ PARAMETRU RA-01_ODP[03]>*** odnosi się do celu; |
| | **RA-01a.01(a)[02]** | polityka oceny ryzyka ***<WYBRANA WARTOŚĆ PARAMETRU RA-01_ODP[03]>*** odnosi się do zakresu; |
| | **RA-01a.01(a)[03]** | polityka oceny ryzyka ***<WYBRANA WARTOŚĆ PARAMETRU RA-01_ODP[03]>*** odnosi się do ról; |
| | **RA-01a.01(a)[04]** | polityka oceny ryzyka ***<WYBRANA WARTOŚĆ PARAMETRU RA-01_ODP[03]>*** odnosi się do obowiązków; |
| | **RA-01a.01(a)[05]** | polityka oceny ryzyka ***<WYBRANA WARTOŚĆ PARAMETRU RA-01_ODP[03]>*** odnosi się do zaangażowania kierownictwa; |
| | **RA-01a.01(a)[06]** | polityka oceny ryzyka ***<WYBRANA WARTOŚĆ PARAMETRU RA-01_ODP[03]>*** odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **RA-01a.01(a)[07]** | polityka oceny ryzyka ***<WYBRANA WARTOŚĆ PARAMETRU RA-01_ODP[03]>*** odnosi się do zgodności; |
| | **RA-01a.01(b)** | polityka oceny ryzyka ***<WYBRANA WARTOŚĆ PARAMETRU RA-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **RA-01b.** | ***<urzędnik RA-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i oceny ryzyka; |
| | **RA-01c.01[01]** | aktualna polityka oceny ryzyka jest przeglądana i aktualizowana z ***<częstotliwością RA-01_ODP[05]>***; |
| | **RA-01c.01[02]** | aktualna polityka oceny ryzyka jest przeglądana i aktualizowana po |

| | | |
|---|---|---|
| **RA-01** | **POLITYKA I PROCEDURY** | |
| | | ***<zdarzeniach RA-01_ODP[06]>***; |
| | **RA-01c.02[01]** | przegląd i aktualizacja procedur oceny ryzyka odbywa się z ***<częstotliwością RA-01_ODP[07]>***; |
| | **RA-01c.02[02]** | aktualne procedury oceny ryzyka są przeglądane i aktualizowane po ***<zdarzeniach RA-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury oceny ryzyka; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **RA-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę ryzyka; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność]. |

| | | |
|---|---|---|
| **RA-02** | **KATEGORYZACJA BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-02a.** | system oraz przetwarzane, przechowywane i przekazywane przez niego informacje są skategoryzowane; |
| | **RA-02b.** | wyniki kategoryzacji bezpieczeństwa, wraz z uzasadnieniem, są udokumentowane w planie bezpieczeństwa systemu; |
| | **RA-02c.** | urzędnik upoważniający lub jego wyznaczony przedstawiciel dokonuje przeglądu i zatwierdza decyzję o nadaniu kategorii bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **RA-02** | **KATEGORYZACJA BEZPIECZEŃSTWA** | |
| | **RA-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; polityka i procedury planowania bezpieczeństwa; procedury dotyczące kategoryzacji bezpieczeństwa informacji i systemów organizacji; dokumentacja dotycząca kategoryzacji bezpieczeństwa; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **RA-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za proces kategoryzacji bezpieczeństwa i ocenę ryzyka; personel organizacyjny odpowiedzialny za bezpieczeństwo i ochronę prywatności]. |
| | **RA-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie kategoryzacji bezpieczeństwa]. |

| | | |
|---|---|---|
| **RA-02(01)** | **KATEGORYZACJA BEZPIECZEŃSTWA \| PRIORYTETYZACJA POZIOMÓW WPŁYWU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-02(01)** | przeprowadza się priorytetyzację poziomu wpływu systemów organizacyjnych, aby uzyskać bardziej szczegółowe informacje w zakresie takich poziomów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-02(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; polityka i procedury planowania bezpieczeństwa i prywatności; procedury dotyczące kategoryzacji bezpieczeństwa informacji i systemów organizacji; dokumentacja dotycząca kategoryzacji bezpieczeństwa; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **RA-02(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za proces kategoryzacji bezpieczeństwa i ocenę ryzyka; personel organizacyjny odpowiedzialny za bezpieczeństwo i ochronę prywatności]. |

| | | |
|---|---|---|
| **RA-02(01)** | **KATEGORYZACJA BEZPIECZEŃSTWA \| PRIORYTETYZACJA POZIOMÓW WPŁYWU** | |
| | **RA-02(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie kategoryzacji bezpieczeństwa]. |

| | | |
|---|---|---|
| **RA-03** | **SZACOWANIE RYZYKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-03_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {plany bezpieczeństwa i ochrony prywatności; raport z oceny ryzyka; <dokument RA-03_ODP[02]>};*** |
| | **RA-03_ODP[02]** | ***określono dokument, w którym mają być udokumentowane wyniki oceny ryzyka (jeśli nie są udokumentowane w planach bezpieczeństwa i ochrony prywatności lub raporcie z oceny ryzyka) (jeśli wybrano);*** |
| | **RA-03_ODP[03]** | ***określono częstotliwość przeglądania wyników oceny ryzyka;*** |
| | **RA-03_ODP[04]** | ***określono personel lub role, wśród których mają być rozpowszechniane wyniki oceny ryzyka;*** |
| | **RA-03_ODP[05]** | ***określono częstotliwość aktualizacji oceny ryzyka;*** |
| | **RA-03a.01** | przeprowadza się ocenę ryzyka w celu określenia zagrożeń dla systemu i jego podatności; |
| | **RA-03a.02** | przeprowadza się ocenę ryzyka w celu określenia prawdopodobieństwa i wielkości szkód wynikających z nieuprawnionego dostępu, wykorzystania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia systemu, informacji, które system przetwarza, przechowuje lub przekazuje, a także wszelkich powiązanych informacji; |
| | **RA-03a.03** | przeprowadza się ocenę ryzyka w celu określenia prawdopodobieństwa wystąpienia i wpływu niekorzystnych skutków dla osób fizycznych, wynikających z przetwarzania danych identyfikacyjnych; |

| | | |
|---|---|---|
| **RA-03** | **SZACOWANIE RYZYKA** | |
| | **RA-03b.** | wyniki oceny ryzyka i decyzje dotyczące zarządzania ryzykiem z perspektywy organizacji, jej misji lub procesu biznesowego są zintegrowane z ocenami ryzyka na poziomie systemu; |
| | **RA-03c.** | wyniki oceny ryzyka są udokumentowane w ***<WYBRANA WARTOŚĆ PARAMETRU RA-03_ODP[01]>***; |
| | **RA-03d.** | wyniki oceny ryzyka podlegają przeglądowi z ***<częstotliwością RA-03_ODP[03]>***; |
| | **RA-03e.** | wyniki oceny ryzyka są rozpowszechniane wśród ***<personelu lub ról RA-03_ODP[04]>***; |
| | **RA-03f.** | ocena ryzyka jest aktualizowana z ***<częstotliwością RA-03_ODP[05]> lub w*** przypadku znaczących zmian w systemie bądź jego środowisku operacyjnym lub w razie wystąpienia innych warunków, które mogą mieć wpływ na stan bezpieczeństwa lub prywatności systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; procedury oceny ryzyka; polityka i procedury planowania bezpieczeństwa i prywatności; procedury dotyczące organizacyjnych ocen ryzyka; ocena ryzyka; wyniki oceny ryzyka; przeglądy oceny ryzyka; aktualizacje oceny ryzyka; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **RA-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę ryzyka; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność]. |
| | **RA-03-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące oceny ryzyka; mechanizmy wspierające lub realizujące, dokumentujące, przeglądające, rozpowszechniające i aktualizujące ocenę ryzyka]. |

| | | |
|---|---|---|
| **RA-03(01)** | **SZACOWANIE RYZYKA \| SZACOWANIE RYZYKA ŁAŃCUCHA DOSTAW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-03(01)_ODP[01]** | ***określono systemy, komponenty systemu i usługi systemowe służące do oceny ryzyka łańcucha dostaw;*** |
| | **RA-03(01)_ODP[02]** | ***określono częstotliwość, z jaką należy aktualizować ocenę ryzyka łańcucha dostaw;*** |
| | **RA-03(01)(a)** | ocenia się ryzyko łańcucha dostaw związane z ***<systemami, komponentami systemu i usługami systemowymi RA-03(01)_ODP[01]>***; |
| | **RA-03(01)(b)** | ocena ryzyka łańcucha dostaw jest aktualizowana z ***<częstotliwością RA-03(01)_ODP[02]>*** , gdy zachodzą istotne zmiany w danym łańcuchu dostaw bądź zmiany w systemie lub jego środowiskach działania, albo gdy występują inne warunki mogące skutkować koniecznością zmiany łańcucha dostaw. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania ryzykiem łańcucha dostaw; spis systemów krytycznych, komponentów systemu i usług systemowych; polityka oceny ryzyka; polityka i procedury planowania bezpieczeństwa; procedury dotyczące organizacyjnych ocen ryzyka łańcucha dostaw; ocena ryzyka; wyniki oceny ryzyka; przeglądy oceny ryzyka; aktualizacje oceny ryzyka; polityka zakupów; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **RA-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę ryzyka; personel organizacyjny odpowiedzialny za bezpieczeństwo; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |

| | | |
|---|---|---|
| **RA-03(01)** | **SZACOWANIE RYZYKA \| SZACOWANIE RYZYKA ŁAŃCUCHA DOSTAW** | |
| | **RA-03(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące oceny ryzyka; mechanizmy wspierające lub przeprowadzające, dokumentujące, przeglądające, rozpowszechniające i aktualizujące ocenę ryzyka łańcucha dostaw]. |

| | | |
|---|---|---|
| **RA-03(02)** | **SZACOWANIE RYZYKA \| WYMIANA INFORMACJI O ZAGROŻENIACH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-03(02)** | Do analizy ryzyka wykorzystywane są informacje ze wszystkich źródeł. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; polityka i procedury planowania bezpieczeństwa; procedury dotyczące organizacyjnych ocen ryzyka; ocena ryzyka;<br>wyniki oceny ryzyka; przeglądy oceny ryzyka; aktualizacje oceny ryzyka; raporty wywiadowcze na temat ryzyka; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę ryzyka; personel organizacyjny odpowiedzialny za bezpieczeństwo]. |
| | **RA-03(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące oceny ryzyka; mechanizmy wspierające lub realizujące, dokumentujące, przeglądające, rozpowszechniające i aktualizujące ocenę ryzyka]. |

| | | |
|---|---|---|
| **RA-03(03)** | **SZACOWANIE RYZYKA \| ŚWIADOMOŚĆ DYNAMIKI ZAGROŻEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-03(03)_ODP** | ***dostępne są środki do bieżącego rozpoznawania aktualnego środowiska cyberzagrożeń;*** |
| | **RA-03(03)** | aktualne środowisko cyberzagrożeń jest rozpoznawane na bieżąco przy użyciu ***<środków RA-03(03)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; polityka i procedury planowania bezpieczeństwa; procedury dotyczące organizacyjnych ocen ryzyka; ocena ryzyka; wyniki oceny ryzyka; przeglądy oceny ryzyka; aktualizacje oceny ryzyka; raporty dotyczące ryzyka; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę ryzyka; personel organizacyjny odpowiedzialny za bezpieczeństwo]. |
| | **RA-03(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące oceny ryzyka; mechanizmy wspierające lub realizujące, dokumentujące, przeglądające, rozpowszechniające i aktualizujące ocenę ryzyka]. |

| | | |
|---|---|---|
| **RA-03(04)** | **SZACOWANIE RYZYKA \| PROGNOZOWANA CYBERANALITYKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-03(04)_ODP[01]** | ***określono zaawansowane środki automatyzacji służące do przewidywania i identyfikacji ryzyka;*** |

| | | |
|---|---|---|
| **RA-03(04)** | **SZACOWANIE RYZYKA \| PROGNOZOWANA CYBERANALITYKA** | |
| | **RA-03(04)_ODP[02]** | ***określono systemy lub komponenty systemu, w których mają być zastosowane zaawansowane rozwiązania w zakresie automatyki i analityki;*** |
| | **RA-03(04)_ODP[03]** | ***określono zaawansowane środki analityki służące do przewidywania i identyfikacji ryzyka;*** |
| | **RA-03(04)[01]** | stosuje się ***<zaawansowane środki automatyzacji RA-03(04)_ODP[01]> do*** przewidywania i identyfikacji ryzyka dla ***<systemu lub komponentów systemu RA-03(04)_ODP[02]>***; |
| | **RA-03(04)[02]** | stosuje się ***<zaawansowane środki analityki RA-03(04)_ODP[03]> do*** przewidywania i identyfikacji ryzyka dla ***<systemu lub komponentów systemu RA-03(04)_ODP[02]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-03(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; polityka i procedury planowania bezpieczeństwa; procedury dotyczące organizacyjnych ocen ryzyka; ocena ryzyka; wyniki oceny ryzyka; przeglądy oceny ryzyka; aktualizacje oceny ryzyka; raporty dotyczące ryzyka; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-03(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę ryzyka; personel organizacyjny odpowiedzialny za bezpieczeństwo]. |
| | **RA-03(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące oceny ryzyka; mechanizmy wspierające lub realizujące, dokumentujące, przeglądające, rozpowszechniające i aktualizujące ocenę ryzyka]. |

| | |
|---|---|
| **RA-04** | **AKTUALIZACJA SZACOWANIA RYZYKA** |
| | [WYCOFANE: Włączone do RA-03]. |

| | | |
|---|---|---|
| **RA-05** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-05_ODP[01]** | ***określono częstotliwość monitorowania systemów i aplikacji hostowanych pod kątem podatności;*** |
| | **RA-05_ODP[02]** | ***określono częstotliwość skanowania systemów i aplikacji hostowanych pod kątem podatności;*** |
| | **RA-05_ODP[03]** | ***określono termin usunięcia wykrytych podatności zgodnie z organizacyjną oceną ryzyka;*** |
| | **RA-05_ODP[04]** | ***określono personel lub role, którym należy udostępnić informacje uzyskane w procesie skanowania pod kątem podatności i oceny zabezpieczeń;*** |
| | **RA-05a.[01]** | systemy i aplikacje hostowane są monitorowane pod kątem podatności z ***<częstotliwością lub losowo zgodnie z procesem określonym przez organizację RA-05_ODP[01]>***, a także w przypadku wykrycia i zgłoszenia nowych podatności potencjalnie dotyczących systemu; |
| | **RA-05a.[02]** | systemy i aplikacje hostowane są skanowane pod kątem podatności z ***<częstotliwością lub losowo zgodnie z procesem określonym przez organizację RA-05_ODP[02]>***, a także w przypadku wykrycia i zgłoszenia nowych podatności potencjalnie dotyczących systemu; |
| | **RA-05b.** | narzędzia i techniki monitorowania podatności są stosowane w celu zapewnienia lepszej interoperacyjności narzędzi; |
| | **RA-05b.01** | narzędzia i techniki monitorowania podatności są wykorzystywane do automatyzacji części procesu zarządzania podatnościami poprzez wykorzystanie standardów wyliczania platform, błędów oprogramowania i nieprawidłowych konfiguracji; |

| | | |
|---|---|---|
| **RA-05** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI** | |
| | **RA-05b.02** | narzędzia i techniki monitorowania podatności są stosowane w celu zapewnienia lepszej interoperacyjności narzędzi i zautomatyzowania części procesu zarządzania podatnościami poprzez wykorzystanie standardów formatowania list kontrolnych i procedur badawczych; |
| | **RA-05b.03** | narzędzia i techniki monitorowania podatności są stosowane w celu zapewnienia lepszej interoperacyjności narzędzi i zautomatyzowania części procesu zarządzania podatnościami poprzez zastosowanie standardów pomiaru wpływu podatności; |
| | **RA-05c.** | raporty ze skanowania podatności oraz wyniki monitorowania podatności są analizowane; |
| | **RA-05d.** | wykryte podatności są usuwane w ***<terminie RA-05_ODP[03]>*** zgodnie z organizacyjną oceną ryzyka; |
| | **RA-05e.** | informacje uzyskane w procesie monitorowania podatności i oceny zabezpieczeń są udostępniane ***<personelowi lub rolom RA-05_ODP[04]>*** w celu wsparcia procesu eliminacji podobnych podatności w innych systemach; |
| | **RA-05f.** | stosuje się narzędzia do monitorowania podatności, które umożliwiają łatwe aktualizowanie zakresu podatności objętych skanowaniem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; procedury dotyczące skanowania podatności; ocena ryzyka; raport z oceny; narzędzia do skanowania podatności i związana z nimi dokumentacja konfiguracyjna; wyniki skanowania podatności; zapisy dotyczące zarządzania poprawkami i podatnościami; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **RA-05** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI** | |
| | **RA-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę ryzyka, ocenę zabezpieczeń i skanowanie podatności; personel organizacyjny odpowiedzialny za analizę procesu skanowania podatności; personel organizacyjny odpowiedzialny za usuwanie podatności; personel organizacyjny odpowiedzialny za bezpieczeństwo; administratorzy systemu/sieci]. |
| | **RA-05-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące skanowania podatności, analizy, usuwania skutków i wymiany informacji; mechanizmy wspierające lub wdrażające skanowanie podatności, analizę, usuwanie skutków i wymianę informacji]. |

| | | |
|---|---|---|
| **RA-05(01)** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI \| AKTUALIZACJA NARZĘDZI** | |
| | [WYCOFANE: Włączone do RA-05]. | |

| | | |
|---|---|---|
| **RA-05(02)** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI \| NADZOROWANIE WYKRYTYCH PODATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-05(02)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{<częstotliwość RA-05(02)_ODP[02]>; przed nowym skanowaniem; po zidentyfikowaniu i zgłoszeniu nowych podatności};*** |
| | **RA-05(02)_ODP[02]** | ***określono częstotliwość aktualizacji skanowanych podatności systemowych (jeśli wybrano);*** |
| | **RA-05(02)** | skanowane podatności systemowe są aktualizowane ***<WYBRANA WARTOŚĆ PARAMETRU RA-05(02)_ODP[01]>***. |

| | | |
|---|---|---|
| **RA-05(02)** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI \| NADZOROWANIE WYKRYTYCH PODATNOŚCI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-05(02)-Badanie** | [WYBÓR SPOŚRÓD: Procedury dotyczące skanowania podatności; raport z oceny; narzędzia do skanowania podatności i związana z nimi dokumentacja konfiguracyjna;<br>wyniki skanowania podatności; zapisy dotyczące zarządzania poprawkami i podatnościami; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za skanowanie podatności; personel organizacyjny odpowiedzialny za analizę podatności; personel organizacyjny odpowiedzialny za bezpieczeństwo; administratorzy systemu/sieci]. |
| | **RA-05(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące skanowania podatności; mechanizmy/narzędzia wspierające lub wdrażające skanowanie podatności]. |

| | | |
|---|---|---|
| **RA-05(03)** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI \| ZAKRES PODATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-05(03)** | określono zakres i głębokość skanowania podatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| RA-05(03) | MONITOROWANIE I SKANOWANIE PODATNOŚCI \| ZAKRES PODATNOŚCI | |
|---|---|---|
| | **RA-05(03)-Badanie** | [WYBÓR SPOŚRÓD: Procedury dotyczące skanowania podatności; raport z oceny; narzędzia do skanowania podatności i związana z nimi dokumentacja konfiguracyjna;<br>wyniki skanowania podatności; zapisy dotyczące zarządzania poprawkami i podatnościami; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(03)-Wywiad** | [WYBÓR SPOŚRÓD: Procedury dotyczące skanowania podatności; raport z oceny; narzędzia do skanowania podatności i związana z nimi dokumentacja konfiguracyjna; wyniki skanowania podatności; zapisy dotyczące zarządzania poprawkami i podatnościami; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące skanowania podatności; mechanizmy/narzędzia wspierające lub wdrażające skanowanie podatności]. |

| RA-05(04) | MONITOROWANIE I SKANOWANIE PODATNOŚCI \| WYKRYWANIE SKANOWANIA | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-05(04)_ODP** | ***określono działania naprawcze, które należy podjąć w przypadku gdy informacje o systemie są możliwe do wykrycia i przejęcia;*** |
| | **RA-05(04)[01]** | informacje o systemie są możliwe do wykrycia; |
| | **RA-05(04)[02]** | podejmowane są ***<działania naprawcze RA-05(04)_ODP>***, jeżeli potwierdzono, że informacje o systemie są możliwe do wykrycia. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| RA-05(04) | MONITOROWANIE I SKANOWANIE PODATNOŚCI \| WYKRYWANIE SKANOWANIA | |
|---|---|---|
| | **RA-05(04)-Badanie** | [WYBÓR SPOŚRÓD: Procedury dotyczące skanowania podatności; raport z oceny; wyniki testów penetracyjnych; wyniki skanowania podatności; raport z oceny ryzyka; zapisy podjętych działań naprawczych; zapisy dotyczące reakcji na incydenty; zapisy z audytów; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za skanowanie podatności lub testy penetracyjne; personel organizacyjny odpowiedzialny za analizę podatności; personel organizacyjny odpowiedzialny za reagowanie na ryzyko; personel organizacyjny odpowiedzialny za zarządzanie i reagowanie na incydenty; personel organizacyjny odpowiedzialny za bezpieczeństwo]. |
| | **RA-05(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące skanowania podatności; procesy organizacyjne dotyczące reagowania na ryzyko; procesy organizacyjne dotyczące zarządzania incydentami i reagowania na nie; mechanizmy/narzędzia wspierające lub wdrażające skanowanie podatności skanowanie podatności;<br>mechanizmy wspierające lub wdrażające procesy reagowania na ryzyko; mechanizmy wspierające lub wdrażające procesy zarządzania incydentami i reagowania na nie]. |

| RA-05(05) | MONITOROWANIE I SKANOWANIE PODATNOŚCI \| DOSTĘP UPRZYWILEJOWANY | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-05(05)_ODP[01]** | ***określono komponenty systemu, do których dostęp jest zarezerwowany dla wybranych czynności w zakresie skanowania podatności;*** |
| | **RA-05(05)_ODP[02]** | ***określono działania związane ze skanowaniem podatności, które wymagają uprzywilejowanego dostępu do komponentów systemu;*** |

| | | |
|---|---|---|
| **RA-05(05)** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI \| DOSTĘP UPRZYWILEJOWANY** | |
| | **RA-05(05)** | stosuje się uprzywilejowany dostęp do ***<komponentów systemu RA-05(05)_ODP[01]> w*** celu realizacji czynności w zakresie ***<skanowania podatności RA-05(05)_ODP[02]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-05(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; procedury dotyczące skanowania podatności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista komponentów systemu przeznaczonych do skanowania podatności; lista uprawnień dostępu personelu; dane uwierzytelniające; zapisy dotyczące uprawnień dostępu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za skanowanie podatności; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za zabezpieczenie dostępu do systemu; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo]. |
| | **RA-05(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące skanowania podatności; procesy organizacyjne dotyczące kontroli dostępu; mechanizmy wspierające lub wdrażające kontrolę dostępu; mechanizmy/narzędzia wspierające lub wdrażające skanowanie podatności]. |

| | | |
|---|---|---|
| **RA-05(06)** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI \| AUTOMATYCZNE ANALIZY TRENDÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-05(06)_ODP** | ***określono automatyczne mechanizmy porównywania wyników wielu skanów wykrywających podatności;*** |
| | **RA-05(06)** | wyniki wielu skanów podatności są porównywane przy użyciu ***<mechanizmów automatycznych RA-05(06)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-05(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; procedury dotyczące skanowania podatności; dokumentacja projektowa systemu; dokumentacja narzędzi i technik skanowania podatności; wyniki skanowania podatności; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(06)-Wywiad** | [WYBÓR SPOŚRÓD: Procedury dotyczące skanowania podatności; raport z oceny; narzędzia do skanowania podatności i związana z nimi dokumentacja konfiguracyjna; wyniki skanowania podatności; zapisy dotyczące zarządzania poprawkami i podatnościami; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące skanowania podatności; automatyczne mechanizmy/narzędzia wspierające lub wdrażające skanowanie podatności; automatyczne mechanizmy wspierające lub wdrażające analizę trendów na podstawie wyników skanowania podatności]. |

| | | |
|---|---|---|
| **RA-05(07)** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI \| AUTOMATYCZNE WYKRYWANIE I POWIADAMIANIE O NIEAUTORYZOWANYCH KOMPONENTACH** | |
| | [WYCOFANE: Włączone do CM-08]. | |

| | | |
|---|---|---|
| **RA-05(08)** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI \| PRZEGLĄD HISTORYCZNYCH LOGÓW AUDYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-05(08)_ODP[01]** | ***określono system, w przypadku którego historyczne dzienniki audytów mają podlegać przeglądowi;*** |
| | **RA-05(08)_ODP[02]** | ***określono okres, w którym podatność systemu mogła być wcześniej wykorzystana;*** |
| | **RA-05(08)** | historyczne dzienniki audytów są przeglądane w celu określenia czy podatność zidentyfikowana w ***<systemie RA-05(08)_ODP[01]>*** została wcześniej wykorzystana w ciągu ***<okresu RA-05(08)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-05(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; procedury dotyczące skanowania podatności; dzienniki audytów; zapisy dotyczące przeglądów dzienników audytów; wyniki skanowania podatności; zapisy dotyczące zarządzania poprawkami i podatnościami; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za skanowanie podatności; personel organizacyjny odpowiedzialny za analizę podatności; personel organizacyjny odpowiedzialny za przeglądanie zapisów z audytu; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo]. |
| | **RA-05(08)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące skanowania podatności; proces organizacyjny dotyczący przeglądu zapisów z audytów i reagowania na nie; mechanizmy/narzędzia wspierające lub wdrażające skanowanie podatności; mechanizmy wspierające lub wdrażające przegląd zapisów z audytu]. |

| | |
|---|---|
| **RA-05(09)** | **MONITOROWANIE I SKANOWANIE \| TESTY PENETRACYJNE I ANALIZY** |
| | [WYCOFANE: Włączone do CA-08]. |

| | | |
|---|---|---|
| **RA-05(10)** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI \| KORELACJA SKANOWANYCH DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-05(10)** | dane wyjściowe z narzędzi do skanowania podatności są korelowane w celu określenia obecności wektorów umożliwiających ataki typu „multi-vulnerability" i „multi-hop". |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-05(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; procedury dotyczące skanowania podatności; ocena ryzyka; dokumentacja narzędzi i technik skanowania podatności; wyniki skanowania podatności; zapisy dotyczące zarządzania podatnościami; zapisy z audytu; dzienniki korelacji zdarzeń i podatności; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(10)-Wywiad** | [WYBÓR SPOŚRÓD: Procedury dotyczące skanowania podatności; raport z oceny; narzędzia do skanowania podatności i związana z nimi dokumentacja konfiguracyjna; wyniki skanowania podatności; zapisy dotyczące zarządzania poprawkami i podatnościami; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(10)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za skanowanie podatności; personel organizacyjny odpowiedzialny za analizę skanowania podatności; personel organizacyjny odpowiedzialny za bezpieczeństwo]. |

| | | |
|---|---|---|
| **RA-05(11)** | **MONITOROWANIE I SKANOWANIE PODATNOŚCI \| PROGRAM UPUBLICZNIANIA PODATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-05(11)** | ustanowiono publiczny kanał sprawozdawczy do przyjmowania zgłoszeń o podatnościach w systemach i komponentach systemów organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-05(11)-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; procedury dotyczące skanowania podatności; ocena ryzyka; dokumentacja narzędzi i technik skanowania podatności; wyniki skanowania podatności; zapisy dotyczące zarządzania podatnościami; zapisy z audytu; ogólnodostępny kanał zgłaszania podatności; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(11)-Wywiad** | [WYBÓR SPOŚRÓD: Procedury dotyczące skanowania podatności; raport z oceny; narzędzia do skanowania podatności i związana z nimi dokumentacja konfiguracyjna; wyniki skanowania podatności; zapisy dotyczące zarządzania poprawkami i podatnościami; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-05(11)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za skanowanie podatności; personel organizacyjny odpowiedzialny za analizę procesu skanowania podatności; personel organizacyjny odpowiedzialny za bezpieczeństwo. |

| | | |
|---|---|---|
| **RA-06** | **TECHNICZNE ZABEZPIECZENIE PRZED PODGLĄDEM I PODSŁUCHEM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-06_ODP[01]** | ***określono miejsca, w których stosuje się techniczne zabezpieczenia przed podglądem i podsłuchem;*** |
| | **RA-06_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{<częstotliwość RA-06_ODP[03]>; w przypadku wystąpienia <zdarzenia lub wartości wskaźnika RA-06_ODP[04]>};*** |
| | **RA-06_ODP[03]** | ***określono częstotliwość, z jaką należy stosować techniczne środki przeciwdziałania podglądom i podsłuchom (jeśli wybrano);*** |
| | **RA-06_ODP[04]** | ***określono zdarzenia skutkujące koniecznością zastosowania technicznych środków przeciwdziałania podglądom i podsłuchom (jeśli wybrano);*** |
| | **RA-06** | w ***<lokalizacjach RA-06_ODP[01]> <WYBRANA WARTOŚĆ PARAMETRU RA-06_ODP[02]>*** stosuje się techniczne środki przeciwdziałania podglądom i podsłuchom. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; procedury dotyczące przeglądów technicznych środków przeciwdziałania podglądom i podsłuchom; zapisy z audytów/rejestry zdarzeń; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za techniczne środki przeciwdziałania podglądom i podsłuchom; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo. |
| | **RA-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące technicznych środków przeciwdziałania podglądom i podsłuchom; mechanizmy/narzędzia wspierające lub wdrażające techniczne środki przeciwdziałania podglądom i podsłuchom]. |

| | | |
|---|---|---|
| **RA-07** | **REAKCJA NA RYZYKO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-07[01]** | reakcja na wyniki ocen bezpieczeństwa przeprowadzana jest zgodnie z tolerancją ryzyka organizacji; |
| | **RA-07[02]** | reakcja na wyniki ocen prywatności przeprowadzana jest zgodnie z tolerancją ryzyka organizacji; |
| | **RA-07[03]** | reakcja na wyniki monitorowania przeprowadzana jest zgodnie z tolerancją ryzyka organizacji; |
| | **RA-07[04]** | reakcja na wyniki audytów przeprowadzana jest zgodnie z tolerancją ryzyka organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; sprawozdania z oceny; zapisy z audytów/rejestry zdarzeń; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **RA-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę i audyt; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo i ochronę prywatności]. |
| | **RA-07-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ocen i audytów; mechanizmy/narzędzia wspierające lub wdrażające oceny i audyty]. |

| | | |
|---|---|---|
| **RA-08** | **OCENY WPŁYWU NA PRYWATNOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-08a.** | przed opracowaniem lub zamówieniem technologii informatycznej, która przetwarza dane identyfikacyjne, w odniesieniu do systemów, programów lub innych działań przeprowadza się oceny wpływu na prywatność; |
| | **RA-08b.[01]** | przed rozpoczęciem zbierania danych identyfikacyjnych, które będą przetwarzane przez technologię informatyczną, w odniesieniu do systemów, programów lub innych działań przeprowadza się oceny wpływu na prywatność; |
| | **RA-08b.[02]** | przed rozpoczęciem zbierania danych identyfikacyjnych, które zawierają informacje umożliwiające fizyczny lub wirtualny (online) kontakt z konkretną osobą, w odniesieniu do systemów, programów lub innych działań przeprowadza się ocenę wpływu na prywatność, pod warunkiem że w tym zakresie dziesięciu lub więcej osobom innym niż organizacje, instytucje lub pracownicy rządu zadano identyczne pytania lub nałożono na takie osoby identyczne wymogi sprawozdawcze. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; sprawozdania z oceny ryzyka w zakresie bezpieczeństwa i prywatności; dokumentacja dotycząca zakupów; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **RA-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę i audyt; administratorzy systemu/sieci; twórcy systemów; kierownicy programów; radca prawny; personel organizacyjny odpowiedzialny za bezpieczeństwo i ochronę prywatności]. |

| | | |
|---|---|---|
| **RA-08** | **OCENY WPŁYWU NA PRYWATNOŚĆ** | |
| | **RA-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ocen i audytów; mechanizmy/narzędzia wspierające lub wdrażające oceny i audyty]. |

| | | |
|---|---|---|
| **RA-09** | **ANALIZA KRYTYCZNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-09_ODP[01]** | ***określono systemy, komponenty systemu lub usługi systemowe, które mają być poddawane analizie krytyczności;*** |
| | **RA-09_ODP[02]** | ***określono punkty decyzyjne w cyklu życia systemu, w których należy przeprowadzić analizę krytyczności;*** |
| | **RA-09** | krytyczne komponenty i funkcje systemu są identyfikowane poprzez wykonanie analizy krytyczności obejmującej ***<systemy, komponenty systemu lub usługi systemowe RA-09_ODP[01]>*** w ***<punktach decyzyjnych w cyklu życia systemu RA-09_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; raporty z oceny; analiza krytyczności/ostateczne określenie krytyczności każdego komponentu/podkomponentu; zapisy z audytu/rejestry zdarzeń; raporty z analizy; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ocenę i audyt; personel organizacyjny odpowiedzialny za analizę krytyczności; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo]. |
| | **RA-09-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ocen i audytów; mechanizmy/narzędzia wspierające lub wdrażające oceny i audyty]. |

| | | |
|---|---|---|
| **RA-10** | **WYSZUKIWANIE ZAGROŻEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **RA-10_ODP** | ***określono częstotliwość, z jaką należy stosować zdolności do wyszukiwania cyberzagrożeń;*** |
| | **RA-10a.01** | ustanowiono i utrzymuje się zdolność do zwalczania cyberzagrożeń w celu wyszukiwania oznak naruszenia bezpieczeństwa w systemach organizacyjnych; |
| | **RA-10a.02** | ustanowiono i utrzymuje się zdolność do zwalczania cyberzagrożeń w celu wykrywania, śledzenia i niszczenia zagrożeń zdolnych do ominięcia istniejących zabezpieczeń; |
| | **RA-10b.** | zdolność do wyszukiwania zagrożeń jest stosowana z ***<częstotliwością RA-10_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **RA-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka oceny ryzyka; sprawozdania z oceny; zapisy z audytów/dzienniki zdarzeń; zdolność do wyszukiwania zagrożeń; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **RA-10-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za wyszukiwanie zagrożeń; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo]. |
| | **RA-10-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ocen i audytów; mechanizmy/narzędzia wspierające lub wdrażające zdolność do wyszukiwania zagrożeń]. |

## 4.17. KATEGORIA SA - NABYWANIE SYSTEMU I USŁUG

| | | |
|---|---|---|
| **SA-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-01_ODP[01]** | ***określono personel lub role, wśród których ma być rozpowszechniana polityka nabywania systemu i usług;*** |
| | **SA-01_ODP[02]** | ***określono personel lub role, wśród których mają być rozpowszechniane procedury nabywania systemu i usług;*** |
| | **SA-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **SA-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami nabywania systemu i usług;*** |
| | **SA-01_ODP[05]** | ***określono częstotliwość, z jaką dokonuje się przeglądu i aktualizacji obowiązującej polityki nabywania systemu i usług;*** |
| | **SA-01_ODP[06]** | ***określono zdarzenia wymagające przeglądu i aktualizacji obecnej polityki nabywania systemu i usług;*** |
| | **SA-01_ODP[07]** | ***określono częstotliwość, z jaką dokonuje się przeglądu i aktualizacji obecnych procedur nabywania systemu i usług;*** |
| | **SA-01_ODP[08]** | ***określono zdarzenia wymagające przeglądu i aktualizacji obecnych procedur nabywania systemu i usług;*** |
| | **SA-01a.[01]** | opracowano i udokumentowano politykę nabywania systemu i usług; |
| | **SA-01a.[02]** | polityka nabywania systemu i usług jest rozpowszechniana wśród ***<personelu lub ról SA-01_ODP[01]>***; |
| | **SA-01a.[03]** | opracowano i udokumentowano procedury nabywania systemu i usług ułatwiające realizację polityki w tym obszarze oraz stosowanie powiązanych zabezpieczeń; |

| SA-01 | POLITYKA I PROCEDURY | |
|---|---|---|
| | **SA-01a.[04]** | procedury nabywania systemu i usług są rozpowszechniane wśród ***<personelu lub ról SA-01_ODP[02]>***; |
| | **SA-01a.01(a)[01]** | polityka nabywania systemu i usług ***<WYBRANA WARTOŚĆ PARAMETRU SA-01_ODP[03]>*** odnosi się do celu; |
| | **SA-01a.01(a)[02]** | polityka nabywania systemu i usług ***<WYBRANA WARTOŚĆ PARAMETRU SA-01_ODP[03]>*** odnosi się do zakresu; |
| | **SA-01a.01(a)[03]** | polityka nabywania systemu i usług ***<WYBRANA WARTOŚĆ PARAMETRU SA-01_ODP[03]>*** odnosi się do ról; |
| | **SA-01a.01(a)[04]** | polityka nabywania systemu i usług ***<WYBRANA WARTOŚĆ PARAMETRU SA-01_ODP[03]>*** odnosi się do obowiązków; |
| | **SA-01a.01(a)[05]** | polityka nabywania systemu i usług ***<WYBRANA WARTOŚĆ PARAMETRU SA-01_ODP[03]>*** odnosi się do zaangażowania kierownictwa; |
| | **SA-01a.01(a)[06]** | polityka nabywania systemu i usług ***<WYBRANA WARTOŚĆ PARAMETRU SA-01_ODP[03]>*** odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **SA-01a.01(a)[07]** | polityka nabywania systemu i usług ***<WYBRANA WARTOŚĆ PARAMETRU SA-01_ODP[03]>*** odnosi się do zgodności; |
| | **SA-01a.01(b)** | polityka nabywania systemu i usług***<WYBRANA WARTOŚĆ PARAMETRU SA-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **SA-01b.** | ***<urzędnik SA-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur nabywania systemu i usług; |

| | | |
|---|---|---|
| **SA-01** | **POLITYKA I PROCEDURY** | |
| | **SA-01c.01[01]** | polityka nabywania systemu i usług jest przeglądana i aktualizowana z ***<częstotliwością SA-01_ODP[05]>***; |
| | **SA-01c.01[02]** | polityka nabywania systemu i usług jest przeglądana i aktualizowana po ***<zdarzeniach SA-01_ODP[06]>***; |
| | **SA-01c.02[01]** | procedury nabywania systemu i usług są przeglądane i aktualizowane z ***<częstotliwością SA-01_ODP[07]>***; |
| | **SA-01c.02[02]** | procedury nabywania systemu i usług są przeglądane i aktualizowane po ***<zdarzeniach SA-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; polityka zarządzania ryzykiem łańcucha dostaw; procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |

| | | |
|---|---|---|
| **SA-02** | **PRZYDZIAŁ ZASOBÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-02a.[01]** | wymogi dotyczące wysokiego poziomu bezpieczeństwa informacji dla systemu lub usługi systemowej są określane podczas planowania misji i procesów biznesowych; |

| | | |
|---|---|---|
| **SA-02** | **PRZYDZIAŁ ZASOBÓW** | |
| | **SA-02a.[02]** | wymogi dotyczące wysokiego poziomu prywatności informacji dla systemu lub usługi systemowej są określane podczas planowania misji i procesów biznesowych; |
| | **SA-02b.[01]** | zasoby wymagane do ochrony systemu lub usługi systemowej są określane i dokumentowane w ramach procesu planowania kapitału organizacyjnego i zabezpieczenia inwestycji; |
| | **SA-02b.[02]** | zasoby wymagane do ochrony systemu lub usługi systemowej są przydzielane w ramach procesu planowania kapitału organizacyjnego i zabezpieczenia inwestycji; |
| | **SA-02c.[01]** | w dokumentacji organizacji dotyczącej programowania i budżetowania ustanowiono odrębną pozycję dotyczącą bezpieczeństwa informacji; |
| | **SA-02c.[02]** | w dokumentacji organizacji dotyczącej programowania i budżetowania ustanowiono odrębną pozycję dotyczącą ochrony prywatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; strategia i plany nabywania systemu i usług; procedury dotyczące przydzielania zasobów zgodnie z wymogami bezpieczeństwa informacji i prywatności; procedury dotyczące planowania kapitałowego i zabezpieczenia inwestycji; dokumentacja dotycząca programowania i budżetowania w organizacji; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-02** | **PRZYDZIAŁ ZASOBÓW** | |
| | **SA-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za planowanie kapitałowe, zabezpieczanie inwestycji, programowanie i budżetowanie w organizacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące określania wymagań w zakresie bezpieczeństwa i prywatności informacji; procesy organizacyjne dotyczące planowania kapitałowego, programowania i budżetowania; mechanizmy wspierające lub wdrażające planowanie kapitałowe, programowanie i budżetowanie w organizacji]. |

| | | |
|---|---|---|
| **SA-03** | **CYKL ŻYCIA SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-03_ODP** | ***określono cykl życia systemu;*** |
| | **SA-03a.[01]** | system jest nabywany, rozwijany i zarządzany z wykorzystaniem ***<cyklu życia systemu SA-03_ODP>***, który uwzględnia kwestie bezpieczeństwa informacji; |
| | **SA-03a.[02]** | system jest nabywany, rozwijany i zarządzany z wykorzystaniem ***<cyklu życia systemu SA-03_ODP>***, który uwzględnia kwestie ochrony prywatności; |
| | **SA-03b.[01]** | role i obowiązki w zakresie bezpieczeństwa informacji są definiowane i dokumentowane w całym cyklu życia systemu; |
| | **SA-03b.[02]** | role i obowiązki w zakresie ochrony prywatności są definiowane i dokumentowane w całym cyklu życia systemu; |

| | | |
|---|---|---|
| **SA-03** | **CYKL ŻYCIA SYSTEMU** | |
| | **SA-03c.[01]** | określono osoby odpowiedzialne za bezpieczeństwo informacji i pełniące rolę w tym zakresie; |
| | **SA-03c.[02]** | określono osoby odpowiedzialne za ochronę prywatności i pełniące rolę w tym zakresie; |
| | **SA-03d.[01]** | organizacyjne procesy zarządzania ryzykiem w zakresie bezpieczeństwa informacji są zintegrowane z działaniami związanymi z cyklem życia systemu; |
| | **SA-03d.[02]** | organizacyjne procesy zarządzania ryzykiem w zakresie ochrony prywatności są zintegrowane z działaniami związanymi z cyklem życia systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące integracji procesów bezpieczeństwa informacji, ochrony prywatności i zarządzania ryzykiem łańcucha dostaw z procesem dotyczącym cyklu życia systemu; dokumentacja cyklu życia systemu; organizacyjna strategia zarządzania ryzykiem; dokumentacja strategii zarządzania ryzykiem w zakresie bezpieczeństwa informacji i ochrony prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; plan programu ochrony prywatności; dokumentacja architektury organizacyjnej; dokumentacja programu szkoleniowego w zakresie bezpieczeństwa i ochrony prywatności opartego na rolach; dokumentacja mapowania danych; inne istotne dokumenty lub zapisy]. |
| | **SA-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za cykl życia systemu; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |

| | | |
|---|---|---|
| **SA-03** | **CYKL ŻYCIA SYSTEMU** | |
| | **SA-03-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania i dokumentowania cyklu życia systemu; procesy organizacyjne dotyczące identyfikacji ról i obowiązków w cyklu życia systemu;<br>procedury dotyczące integracji procesów bezpieczeństwa informacji, ochrony prywatności i zarządzania ryzykiem łańcucha dostaw z procesem dotyczącym cyklu życia systemu; mechanizmy wspierające lub wdrażające procesy dotyczące cyklu życia systemu]. |

| | | |
|---|---|---|
| **SA-03(01)** | **CYKL ŻYCIA SYSTEMU \| ZARZĄDZANIE ŚRODOWISKIEM PRZEDPRODUKCYJNYM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-03(01)** | środowiska przedprodukcyjne systemu są chronione proporcjonalnie do ryzyka występującego w całym cyklu życia systemu, komponentu systemu lub usługi systemowej. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące integracji procesów zarządzania ryzykiem w zakresie bezpieczeństwa i łańcucha dostaw z procesem cyklu życia systemu; dokumentacja cyklu życia systemu; procedury dotyczące planowania ochrony programu; wyniki analizy krytyczności; strategia/dokumentacja programu zarządzania ryzykiem w zakresie bezpieczeństwa i łańcucha dostaw; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i rozwój w zakresie cyklu życia systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| SA-03(01) | CYKL ŻYCIA SYSTEMU \| ZARZĄDZANIE ŚRODOWISKIEM PRZEDPRODUKCYJNYM | |
|---|---|---|
| | **SA-03(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania i dokumentowania cyklu życia systemu; procesy organizacyjne dotyczące identyfikowania ról i obowiązków w cyklu życia systemu; proces organizacyjny dotyczący integrowania procesu zarządzania ryzykiem bezpieczeństwa z cyklem życia systemu; mechanizmy wspierające lub wdrażające cykl życia systemu]. |

| SA-03(02) | CYKL ŻYCIA SYSTEMU \| KORZYSTANIE Z DANYCH BIEŻĄCYCH LUB OPERACYJNYCH | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-03(02)a.[01]** | wykorzystanie danych bieżących w środowiskach przedprodukcyjnych w odniesieniu do systemu, komponentu systemu lub usługi systemowej jest zatwierdzane; |
| | **SA-03(02)a.[02]** | wykorzystanie danych bieżących w środowiskach przedprodukcyjnych w odniesieniu do systemu, komponentu systemu lub usługi systemowej jest dokumentowane; |
| | **SA-03(02)a.[03]** | wykorzystanie danych bieżących w środowiskach przedprodukcyjnych w odniesieniu do systemu, komponentu systemu lub usługi systemowej jest kontrolowane; |
| | **SA-03(02)b.** | środowiska przedprodukcyjne systemu, komponentu systemu lub usługi systemowej są zabezpieczone na tym samym poziomie wpływu lub klasyfikacji co wszelkie dane bieżące używane w środowiskach przedprodukcyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SA-03(02) | CYKL ŻYCIA SYSTEMU \| KORZYSTANIE Z DANYCH BIEŻĄCYCH LUB OPERACYJNYCH | |
|---|---|---|
| | **SA-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące integracji procesów bezpieczeństwa i ochrony prywatności z procesem cyklu życia systemu; dokumentacja cyklu życia systemu; dokumentacja oceny ryzyka w zakresie bezpieczeństwa; ocena wpływu na prywatność; dokumentacja oceny ryzyka w zakresie ochrony prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja dotycząca mapowania danych; polityka przetwarzania danych identyfikacyjnych; procedury dotyczące uprawnień do przeprowadzania testów z wykorzystaniem danych identyfikacyjnych; procedury dotyczące minimalizacji informacji danych identyfikacyjnych wykorzystywanych w testach, szkoleniach i badaniach; inne istotne dokumenty lub zapisy]. |
| | **SA-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za rozwój w zakresie cyklu życia systemu]. |
| | **SA-03(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne wykorzystanie danych bieżących w środowiskach przedprodukcyjnych; mechanizmy ochrony danych bieżących w środowiskach przedprodukcyjnych]. |

| SA-03(03) | CYKL ŻYCIA SYSTEMU \| ODŚWIEŻANIE TECHNOLOGII | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-03(03)[01]** | zaplanowano harmonogram odświeżania technologii systemu w całym cyklu życia; |
| | **SA-03(03)[02]** | harmonogram odświeżania technologii systemu w całym cyklu życia jest wdrażany. |

| | | |
|---|---|---|
| **SA-03(03)** | **CYKL ŻYCIA SYSTEMU \| ODŚWIEŻANIE TECHNOLOGII** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące planowania i wdrażania odświeżania technologii; dokumentacja cyklu życia systemu; harmonogram odświeżania technologii; dokumentacja dotycząca oceny ryzyka w zakresie bezpieczeństwa; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka w zakresie prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za rozwój w zakresie cyklu życia systemu]. |
| | **SA-03(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania i dokumentowania cyklu życia systemu; procesy organizacyjne dotyczące identyfikacji ról i obowiązków w cyklu życia systemu; procedury dotyczące integracji procesów bezpieczeństwa informacji i ochrony prywatności z procesem dotyczącym cyklu życia systemu; mechanizmy wspierające lub wdrażające procesy dotyczące cyklu życia systemu]. |

| | | |
|---|---|---|
| **SA-04** | **PROCES NABYCIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {standardowy język umowy; <język umowy SA-04_ODP[02]>};*** |
| | **SA-04_ODP[02]** | ***określono język umowy (jeśli wybrano);*** |

| SA-04 | PROCES NABYCIA | |
|---|---|---|
| | **SA-04a.[01]** | wymagania, opisy i kryteria dotyczące funkcji bezpieczeństwa są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04a.[02]** | wymagania, opisy i kryteria dotyczące funkcji ochrony prywatności są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04b.** | wymagania, opisy i kryteria dotyczące siły mechanizmów bezpieczeństwa są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04c.[01]** | wymagania, opisy i kryteria dotyczące pewności w zakresie bezpieczeństwa są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04c.[02]** | wymagania, opisy i kryteria dotyczące pewności w zakresie ochrony prywatności są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04d.[01]** | zabezpieczenia niezbędne do spełnienia wymagań, opisów i kryteriów w zakresie bezpieczeństwa są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |

| SA-04 | PROCES NABYCIA | |
|---|---|---|
| | **SA-04d.[02]** | zabezpieczenia niezbędne do spełnienia wymogów, opisów i kryteriów w zakresie prywatności są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04e.[01]** | wymagania, opisy i kryteria dotyczące dokumentacji zabezpieczeń są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04e.[02]** | wymagania, opisy i kryteria dotyczące dokumentacji w zakresie ochrony prywatności są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04f.[01]** | wymagania w zakresie zabezpieczania dokumentacji bezpieczeństwa, opisów i kryteriów są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04f.[02]** | wymagania w zakresie zabezpieczania dokumentacji dotyczącej ochrony prywatności, opisów i kryteriów są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04g.** | opis środowiska rozwoju i eksploatacji systemu oraz wymagania i kryteria są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |

| | | |
|---|---|---|
| **SA-04** | **PROCES NABYCIA** | |
| | **SA-04h.[01]** | podział rozliczalności lub określenie stron odpowiedzialnych za bezpieczeństwo informacji, a także opisy i kryteria, są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04h.[02]** | podział rozliczalności lub określenie stron odpowiedzialnych za ochronę prywatności, a także opisy i kryteria, są włączone do umowy bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>***; |
| | **SA-04h.[03]** | podział rozliczalności lub określenie stron odpowiedzialnych za zarządzanie ryzykiem łańcucha dostaw, a także opisy i kryteria, są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej; |
| | **SA-04i.** | wymagania i opisy kryteriów akceptacji są włączone bezpośrednio lub przez odniesienie przy użyciu ***<WYBRANA WARTOŚĆ PARAMETRU SA-04_ODP[01]>*** do umowy nabycia systemu, komponentu systemu lub usługi systemowej. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące integracji procesów bezpieczeństwa informacji, ochrony prywatności i zarządzania ryzykiem łańcucha dostaw z procesem dotyczącym nabywania; plan zarządzania konfiguracją; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja projektowa systemu; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-04** | **PROCES NABYCIA** | |
| | **SA-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-04-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące określania wymagań w zakresie funkcji, siły zabezpieczeń oraz zapewnienia odpowiedniego poziomu bezpieczeństwa i ochrony prywatności dla systemu; procesy organizacyjne dotyczące opracowywania umów nabycia; mechanizmy wspierające lub realizujące nabywanie oraz uwzględnianie w umowach wymagań dotyczących bezpieczeństwa i ochrony prywatności]. |

| | | |
|---|---|---|
| **SA-04(01)** | **PROCES NABYCIA \| WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04(01)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się dostarczenia opisu właściwości funkcjonalnych zabezpieczeń, które mają być zastosowane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące integracji wymogów, opisów i kryteriów w zakresie bezpieczeństwa i ochrony prywatności z procesem nabywania; dokumenty przetargowe; dokumentacja dotycząca nabywania; umowy nabycia systemu, komponentu systemu lub usług systemowych; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-04(01)** | **PROCES NABYCIA \| WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ** | |
| | **SA-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |
| | **SA-04(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące określania wymagań funkcjonalnych w zakresie bezpieczeństwa systemu; procesy organizacyjne dotyczące opracowywania umów nabycia; mechanizmy wspierające lub wdrażające nabywanie oraz uwzględnianie w umowach wymagań dotyczących bezpieczeństwa i ochrony prywatności]. |

| | | |
|---|---|---|
| **SA-04(02)** | **PROCES NABYCIA \| PROJEKTOWANIE/IMPLEMENTACJA ZABEZPIECZEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04(02)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {istotne dla bezpieczeństwa zewnętrzne interfejsy systemu; projekt wysokopoziomowy; projekt niskopoziomowy; kod źródłowy lub schematy sprzętu <informacje dotyczące projektu i wdrożenia SA-04(02)_ODP[02]>};*** |
| | **SA-04(02)_ODP[02]** | ***określono informacje dotyczące projektu i wdrożenia (jeśli wybrano);*** |
| | **SA-04(02)_ODP[03]** | ***określono poziom szczegółowości;*** |

| | | |
|---|---|---|
| **SA-04(02)** | **PROCES NABYCIA \| PROJEKTOWANIE/IMPLEMENTACJA ZABEZPIECZEŃ** | |
| | **SA-04(02)** | twórca systemu, komponentu systemu lub usługi systemowej jest zobowiązany do dostarczenia informacji dotyczących projektu i wdrożenia zabezpieczeń, które obejmują zastosowanie ***<WYBRANA WARTOŚĆ PARAMETRU SA-04(02)_ODP[01]>*** przy ***<poziomie szczegółowości SA-04(02)_ODP[03]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-04(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące integracji wymogów, opisów i kryteriów dotyczących bezpieczeństwa z procesem nabywania; dokumenty przetargowe; dokumentacja dotycząca nabywania; umowy nabycia systemu, komponentów systemu lub usług systemowych; informacje dotyczące projektowania i wdrażania zabezpieczeń stosowanych w systemie, komponencie systemu lub usłudze systemowej; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-04(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za określenie wymagań bezpieczeństwa systemu; programiści systemu lub dostawcy usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-04(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące określania poziomu szczegółowości projektu systemu i zabezpieczeń; procesy organizacyjne dotyczące sporządzania umów nabycia; mechanizmy wspierające lub wdrażające opracowywanie szczegółów dotyczących projektu systemu]. |

| SA-04(03) | PROCES NABYCIA \| METODY, TECHNIKI I PRAKTYKI ROZWOJU | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04(03)_ODP[01]** | ***określono metody inżynierii systemów;*** |
| | **SA-04(03)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{<metody inżynierii bezpieczeństwa systemów SA-04(03)_ODP[03]>; <metody inżynierii ochrony prywatności SA-04(03)_ODP[04]>};*** |
| | **SA-04(03)_ODP[03]** | ***określono metody inżynierii bezpieczeństwa systemu (jeśli wybrano);*** |
| | **SA-04(03)_ODP[04]** | ***określono metody inżynierii prywatności (jeśli wybrano);*** |
| | **SA-04(03)_ODP[05]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{<metody tworzenia oprogramowania SA-04(03)_ODP[06]>; <metody testowania, oceny, weryfikacji i walidacji SA-04(03)_ODP[07]>;***<br>***<procesy kontroli jakości SA-04(03)_ODP[08]>};*** |
| | **SA-04(03)_ODP[06]** | ***określono metody tworzenia oprogramowania (jeśli wybrano);*** |
| | **SA-04(03)_ODP[07]** | ***określono metody testowania, oceny, weryfikacji i walidacji (jeśli wybrano);*** |
| | **SA-04(03)_ODP[08]** | ***określono procesy kontroli jakości (jeśli wybrano);*** |

| | | |
|---|---|---|
| **SA-04(03)** | **PROCES NABYCIA \| METODY, TECHNIKI I PRAKTYKI ROZWOJU** | |
| | **SA-04(03)(a)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykazania stosowania procesu cyklu życia systemu, który obejmuje<br>***<metody inżynierii systemów SA-04(03)_ODP[01]>***; |
| | **SA-04(03)(b)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykazania stosowania procesu cyklu życia systemu, który obejmuje<br>***<WYBRANA WARTOŚĆ PARAMETRU SA-04(03)_ODP[02]>***; |
| | **SA-04(03)(c)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykazania stosowania procesu cyklu życia systemu, który obejmuje<br>***<WYBRANA WARTOŚĆ PARAMETRU SA-04(03)_ODP[05]>*.** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SA-04(03) | PROCES NABYCIA \| METODY, TECHNIKI I PRAKTYKI ROZWOJU | |
|---|---|---|
| | **SA-04(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące integracji wymogów, opisów i kryteriów dotyczących bezpieczeństwa i ochrony prywatności z procesem nabywania; dokumenty przetargowe; dokumentacja dotycząca nabywania; umowy nabycia systemu, komponentu systemu lub usługi systemowej; wykaz metod inżynierii bezpieczeństwa i ochrony prywatności systemów, które należy włączyć do cyklu życia opracowywanego systemu; wykaz technik tworzenia oprogramowania, które należy włączyć do cyklu życia opracowywanego systemu; wykaz technik testowania, oceny lub walidacji, które należy włączyć do cyklu życia opracowywanego systemu; wykaz technik tworzenia oprogramowania, które należy włączyć do cyklu życia opracowywanego systemu. cyklu życia systemu; wykaz metod tworzenia oprogramowania, które mają być włączone do cyklu życia systemu opracowanego przez twórcę;<br><br>wykaz technik testowania, oceny lub walidacji, które mają być włączone do cyklu życia systemu opracowanego przez twórcę; wykaz procesów kontroli jakości, które mają być włączone do cyklu życia systemu opracowanego przez twórcę; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-04(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za cykl życia systemu; programiści systemu lub dostawcy usług]. |
| | **SA-04(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące metod, technik i procesów tworzenia oprogramowania]. |

| SA-04(04) | PROCES NABYCIA \| PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW |
|---|---|
| | [WYCOFANE: Włączone do CM-08(09)]. |

| SA-04(05) | PROCES NABYCIA \| KONFIGURACJI SYSTEMÓW, KOMPONENTÓW I USŁUG | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04(05)_ODP** | ***określono konfiguracje bezpieczeństwa dla systemu, komponentu lub usługi;*** |
| | **SA-04(05)(a)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się dostarczenia systemu, komponentu lub usługi z zaimplementowanymi ***<konfiguracjami zabezpieczeń SA-04(05)_ODP>;*** |
| | **SA-04(05)(b)** | konfiguracje te są używane jako domyślne przy każdej kolejnej ponownej instalacji lub aktualizacji systemu, komponentu lub usługi. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-04(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące integracji wymogów, opisów i kryteriów dotyczących bezpieczeństwa z procesem nabywania; dokumenty przetargowe; dokumentacja dotycząca nabywania; umowy nabycia systemu, komponentu systemu lub usługi systemowej; konfiguracje bezpieczeństwa, które mają być wdrożone przez twórcę systemu, komponentu systemu lub usługi systemowej; umowy o poziomie usług; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-04(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za określenie wymagań bezpieczeństwa systemu; programiści systemu lub dostawcy usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-04(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy stosowane do weryfikacji, że konfiguracja systemu, komponentu lub usługi została dostarczona zgodnie ze specyfikacją]. |

| | | |
|---|---|---|
| **SA-04(06)** | **PROCES NABYCIA \| KORZYSTANIE Z PRODUKTÓW ZAPEWNIAJĄCYCH BEZPIECZEŃSTWO INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04(06)(a)** | jeżeli sieci organizacji wykorzystywane do przesyłania informacji są opatrzone niższym poziomem klauzuli tajności niż informacje przesyłane, do ochrony informacji niejawnych stosuje się wyłącznie ogólnodostępne rządowe lub komercyjne produkty informatyczne zatwierdzone przez krajową władzę bezpieczeństwa; |
| | **SA-04(06)(b)** | produkty te zostały ocenione lub zatwierdzone przez krajową władzę bezpieczeństwa zgodnie z zatwierdzonymi przez nią procedurami. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-04(06)-Badanie** | [WYBÓR SPOŚRÓD: Plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemu i usług; procedury dotyczące integracji wymogów, opisów i kryteriów dotyczących bezpieczeństwa z procesem nabywania; dokumenty przetargowe; dokumentacja dotycząca nabywania; umowy nabycia systemu, komponentu systemu lub usługi systemowej; konfiguracje bezpieczeństwa, które mają być wdrożone przez twórcę systemu, komponentu systemu lub usługi systemowej; umowy o poziomie usług;<br>wykaz wdrożonych produktów/rozwiązań informatycznych; wykaz produktów zatwierdzonych przez krajową władzę bezpieczeństwa; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-04(06)** | **PROCES NABYCIA \| KORZYSTANIE Z PRODUKTÓW ZAPEWNIAJĄCYCH BEZPIECZEŃSTWO INFORMACJI** | |
| | **SA-04(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa systemu; personel organizacyjny odpowiedzialny za zapewnienie, że produkty zapewniające bezpieczeństwo informacji są zatwierdzone przez krajową władzę bezpieczeństwa NSA i są oceniane zgodnie z jej procedurami; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-04(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne mające na celu wybór i stosowanie ocenionych lub zatwierdzonych produktów i usług ochrony informacji, stanowiących zatwierdzone przez krajową władzę bezpieczeństwa rozwiązanie do ochrony informacji niejawnych]. |

| | | |
|---|---|---|
| **SA-04(07)** | **PROCES NABYCIA \| ZATWIERDZONE PROFILE OCHRONY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04(07)(a)** | korzystanie z komercyjnych oraz zatwierdzonych produktów do ochrony bezpieczeństwa informacji jest ograniczone do tych produktów, które zostały pozytywnie ocenione pod kątem profilu ochronnego zatwierdzonego w ramach Krajowego Partnerstwa na rzecz Zapewnienia Bezpieczeństwa Informacji (NIAP) dla danego rodzaju technologii, jeżeli taki profil istnieje; |

| | | |
|---|---|---|
| **SA-04(07)** | **PROCES NABYCIA \| ZATWIERDZONE PROFILE OCHRONY** | |
| | **SA-04(07)(b)** | jeżeli dla danego rodzaju technologii nie istnieje profil ochronny zatwierdzony przez NIAP, a komercyjny produkt informatyczny opiera się na funkcjach kryptograficznych służących egzekwowaniu polityki bezpieczeństwa, wymaga się, aby moduł kryptograficzny posiadał świadectwo FIPS (federalne standardy przetwarzania informacji) lub był zatwierdzony przez krajową władzę bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-04(07)-Badanie** | [WYBÓR SPOŚRÓD: Plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemu i usług; procedury dotyczące integracji wymogów, opisów i kryteriów bezpieczeństwa z procesem nabywania; dokumenty przetargowe; dokumentacja dotycząca nabywania; umowy nabycia systemu, komponentu systemu lub usługi systemowej; wykaz wdrożonych produktów/rozwiązań informatycznych; profile ochronne zatwierdzone przez NIAP; informacje dotyczące wystawiania świadectwa FIPS dla funkcji kryptograficznych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-04(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za określanie wymogów bezpieczeństwa dla systemu; personel organizacyjny odpowiedzialny za zapewnienie, że produkty zapewniające bezpieczeństwo informacji zostały ocenione pod kątem profilu ochronnego zatwierdzonego przez NIAP lub za zapewnienie, że produkty wykorzystujące funkcje kryptograficzne posiadają świadectwo FIPS; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-04(07)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne mające na celu wybór i stosowanie produktów/usług ocenianych pod kątem profilu ochronnego zatwierdzonego przez NIAP lub produktów posiadających świadectwo FIPS]. |

| | | |
|---|---|---|
| **SA-04(08)** | **PROCES NABYCIA \| PLAN CIĄGŁEGO MONITOROWANIA ZABEZPIECZEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04(08)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się opracowania planu ciągłego monitorowania skuteczności zabezpieczeń, który jest zgodny z organizacyjnym programem ciągłego monitorowania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-04(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące planów ciągłego monitorowania stosowanych przez programistów; procedury dotyczące integracji wymogów, opisów i kryteriów bezpieczeństwa z procesem nabywania; plany stałego monitorowania stosowane przez programistów; plany oceny bezpieczeństwa; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja nabycia; dokumentacja przetargowa; umowy o poziomie usług; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-04(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za określanie wymagań bezpieczeństwa dla systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-04(08)-Test** | [WYBÓR SPOŚRÓD: Procesy dostawcy w zakresie ciągłego monitorowania; mechanizmy wspierające lub wdrażające ciągłe monitorowanie stosowane przez programistę]. |

| | | |
|---|---|---|
| **SA-04(09)** | **PROCES NABYCIA \| FUNKCJE, PORTY, PROTOKOŁY / USŁUGI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04(09)[01]** | twórca systemu, komponentu systemu lub usługi systemowej jest zobowiązany do określenia funkcji przeznaczonych do użytku przez organizację; |
| | **SA-04(09)[02]** | twórca systemu, komponentu systemu lub usługi systemowej jest zobowiązany do określenia portów przeznaczonych do użytku przez organizację; |
| | **SA-04(09)[03]** | twórca systemu, komponentu systemu lub usługi systemowej jest zobowiązany do określenia protokołów przeznaczonych do użytku przez organizację; |
| | **SA-04(09)[04]** | twórca systemu, komponentu systemu lub usługi systemowej jest zobowiązany do określenia usług przeznaczonych do użytku przez organizację; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-04(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące włączania wymogów, opisów i kryteriów bezpieczeństwa do procesu nabywania; dokumentacja projektowa systemu; dokumentacja systemu, w tym funkcje, porty, protokoły i usługi przeznaczone do użytku przez organizację; umowy nabycia systemów lub usług; dokumentacja dotycząca nabywania; dokumentacja przetargowa; umowy o poziomie usług; wymogi, opisy i kryteria bezpieczeństwa organizacyjnego dla programistów systemów, komponentów systemu i usług systemowych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| SA-04(09) | PROCES NABYCIA \| FUNKCJE, PORTY, PROTOKOŁY / USŁUGI | |
|---|---|---|
| | **SA-04(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za określenie wymagań bezpieczeństwa dla systemu; administratorzy systemu/sieci; personel organizacyjny obsługujący, eksploatujący lub utrzymujący system; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| SA-04(10) | PROCES NABYCIA \| WYKORZYSTANIE ZATWIERDZONYCH PRODUKTÓW | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04(10)** | stosowane są wyłącznie produkty informatyczne znajdujące się na liście produktów zatwierdzonych w ramach standardu FIPS 201 na potrzeby funkcji weryfikacji tożsamości wdrożonej w systemach organizacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-04(10)-Badanie** | [WYBÓR SPOŚRÓD: Plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemu i usług; procedury dotyczące integracji wymogów, opisów i kryteriów bezpieczeństwa z procesem nabycia; dokumentacja przetargowa; dokumentacja nabycia; umowy nabycia systemu, komponentu systemu lub usługi systemowej; umowy o poziomie usług; wykaz produktów zatwierdzonych w ramach FIPS 201; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-04(10)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za określanie wymagań dotyczących bezpieczeństwa systemu; personel organizacyjny odpowiedzialny za zapewnienie, że wdrażane są wyłącznie produkty zatwierdzone w ramach FIPS 201; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SA-04(10)** | **PROCES NABYCIA \| WYKORZYSTANIE ZATWIERDZONYCH PRODUKTÓW** | |
| | **SA-04(10)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wyboru i stosowania produktów zatwierdzonych w ramach FIPS 201]. |

| | | |
|---|---|---|
| **SA-04(11)** | **PROCES NABYCIA \| SYSTEM DOKUMENTOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04(11)_ODP** | ***określono wymogi ustawy o ochronie danych dotyczące funkcjonowania systemu rejestrów;*** |
| | **SA-04(11)** | ***<wymogi ustawy o ochronie danych SA-04(11)_ODP>*** zawarto w umowie o świadczenie usług dotyczących obsługi systemu rejestrów w imieniu organizacji w celu realizacji jej misji lub funkcji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-04(11)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące włączenia wymogów ustawy o ochronie danych do systemów rejestrów obsługiwanych przez organizacje zewnętrzne; dokumentacja przetargowa; dokumentacja nabycia; umowy nabycia systemu, komponentu systemu lub usługi systemowej; umowy o poziomie usług;<br>plan bezpieczeństwa systemu; plan ochrony prywatności; polityka przetwarzania informacji umożliwiających identyfikację osób; plan programu ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla prywatności; inne właściwe dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-04(11)** | **PROCES NABYCIA \| SYSTEM DOKUMENTOWANIA** | |
| | **SA-04(11)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SA-04(11)-Test** | [WYBÓR SPOŚRÓD: Procesy zarządzania umową w celu sprawdzenia czy zdefiniowano wymogi ustawy o ochronie danych w odniesieniu do działania systemu rejestrów; procesy sprzedawcy w celu wykazania włączenia wymogów ustawy o ochronie danych do procesu eksploatacji systemu rejestrów]. |

| | | |
|---|---|---|
| **SA-04(12)** | **PROCES NABYCIA \| WŁASNOŚĆ DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-04(12)_ODP** | ***określono ramy czasowe na usunięcie danych z systemu wykonawcy i ich zwrot do organizacji;*** |
| | **SA-04(12)(a)** | wymagania dotyczące własności danych organizacyjnych są zawarte w umowie nabycia; |
| | **SA-04(12)(b)** | wymagane jest usunięcie wszystkich danych z systemu wykonawcy i zwrócenie ich do organizacji w ***<terminie SA-04(12)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-04(12)** | **PROCES NABYCIA \| WŁASNOŚĆ DANYCH** | |
| | **SA-04(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące integracji wymogów, opisów i kryteriów bezpieczeństwa i prywatności informacji z procesem nabywania; procedury dotyczące dysponowania danymi identyfikacyjnymi; dokumentacja przetargowa; dokumentacja dotycząca nabywania; umowy nabycia systemu lub usługi systemowej; polityka przetwarzania danych identyfikacyjnych; umowy o poziomie usług; umowy o udostępnianiu informacji; protokoły ustaleń; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka w zakresie ochrony prywatności; inne właściwe dokumenty lub zapisy]. |
| | **SA-04(12)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za zarządzanie danymi i wymagania dotyczące ich przetwarzania; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SA-04(12)-Test** | [WYBÓR SPOŚRÓD: Procesy zarządzania umowami w celu weryfikacji, czy dane są usuwane zgodnie z wymogami; procesy dostawców dotyczące usuwania danych w wymaganych terminach; mechanizmy weryfikujące usunięcie i zwrot danych]. |

| | | |
|---|---|---|
| **SA-05** | **DOKUMENTACJA SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-05_ODP[01]** | ***określono działania, które należy podjąć, jeżeli dokumentacja systemu, komponentu systemu lub usługi systemowej jest niedostępna lub nie istnieje;*** |
| | **SA-05_ODP[02]** | ***określono personel lub role, do których ma trafić dokumentacja systemu;*** |

| SA-05 | DOKUMENTACJA SYSTEMU | |
|---|---|---|
| | **SA-05a.01[01]** | uzyskano lub opracowano dokumentację administratora dla systemu, komponentu systemu lub usługi systemowej, opisującą bezpieczną konfigurację systemu, komponentu bądź usługi; |
| | **SA-05a.01[02]** | uzyskano lub opracowano dokumentację administratora dla systemu, komponentu systemu lub usługi systemowej, opisującą bezpieczną instalację systemu, komponentu lub usługi; |
| | **SA-05a.01[03]** | uzyskano lub opracowano dokumentację administratora dla systemu, komponentu systemu lub usługi systemowej, która opisuje bezpieczną eksploatację systemu, komponentu lub usługi; |
| | **SA-05a.02[01]** | uzyskano lub opracowano dokumentację administratora dla systemu, komponentu systemu lub usługi systemowej, opisującą skuteczne wykorzystanie funkcji i mechanizmów bezpieczeństwa; |
| | **SA-05a.02[02]** | uzyskano lub opracowano dokumentację administratora dla systemu, komponentu systemu lub usługi systemowej, opisującą skuteczne utrzymanie funkcji i mechanizmów bezpieczeństwa; |
| | **SA-05a.02[03]** | uzyskano lub opracowano dokumentację administratora dla systemu, komponentu systemu lub usługi systemowej, opisującą skuteczne wykorzystanie funkcji i mechanizmów prywatności; |
| | **SA-05a.02[04]** | uzyskano lub opracowano dokumentację administratora dla systemu, komponentu systemu lub usługi systemowej, opisującą skuteczne utrzymanie funkcji i mechanizmów prywatności; |
| | **SA-05a.03[01]** | uzyskano lub opracowano dokumentację administratora dla systemu, komponentu systemu lub usługi systemowej, opisującą znane podatności w zakresie konfiguracji funkcji administracyjnych lub uprzywilejowanych; |

| SA-05 | DOKUMENTACJA SYSTEMU | |
|---|---|---|
| | **SA-05a.03[02]** | uzyskano lub opracowano dokumentację administratora dla systemu, komponentu systemu lub usługi systemowej, opisującą znane podatności w zakresie wykorzystywania funkcji administracyjnych lub uprzywilejowanych; |
| | **SA-05b.01[01]** | uzyskano lub opracowano dokumentację użytkownika dla systemu, komponentu systemu lub usługi systemowej, opisującą dostępne dla użytkownika funkcje i mechanizmy bezpieczeństwa; |
| | **SA-05b.01[02]** | uzyskano lub opracowano dokumentację użytkownika dla systemu, komponentu systemu lub usługi systemowej, opisującą skuteczne korzystanie z funkcji i mechanizmów bezpieczeństwa (dostępnych dla użytkownika); |
| | **SA-05b.01[03]** | uzyskano lub opracowano dokumentację użytkownika dla systemu, komponentu systemu lub usługi systemowej, opisującą funkcje i mechanizmy ochrony prywatności dostępne dla użytkownika; |
| | **SA-05b.01[04]** | uzyskano lub opracowano dokumentację użytkownika dla systemu, komponentu systemu lub usługi systemowej, opisującą skuteczne korzystanie z funkcji i mechanizmów ochrony prywatności (dostępnych dla użytkownika); |
| | **SA-05b.02[01]** | uzyskano lub opracowano dokumentację użytkownika dla systemu, komponentu systemu lub usługi systemowej, opisującą metody interakcji z użytkownikiem, które umożliwiają osobom fizycznym korzystanie z systemu, komponentu lub usługi w bardziej bezpieczny sposób; |
| | **SA-05b.02[02]** | uzyskano lub opracowano dokumentację użytkownika dla systemu, komponentu systemu lub usługi systemowej, opisującą metody interakcji z użytkownikiem, które umożliwiają osobom fizycznym korzystanie z systemu, komponentu lub usługi w celu ochrony prywatności; |

| | | |
|---|---|---|
| **SA-05** | **DOKUMENTACJA SYSTEMU** | |
| | **SA-05b.03[01]** | uzyskano lub opracowano dokumentację użytkownika dla systemu, komponentu systemu lub usługi systemowej, która opisuje obowiązki użytkownika w zakresie dbałości o bezpieczeństwo systemu, komponentu lub usługi; |
| | **SA-05b.03[02]** | uzyskano lub opracowano dokumentację użytkownika dla systemu, komponentu systemu lub usługi systemowej, która opisuje obowiązki użytkownika w zakresie ochrony prywatności; |
| | **SA-05c.[01]** | udokumentowano próby uzyskania dokumentacji dla systemu, komponentu systemu lub usługi systemowej w przypadku gdy jest ona niedostępna lub nie istnieje; |
| | **SA-05c.[02]** | po próbach uzyskania dokumentacji dla systemu, komponentu systemu lub usługi systemowej w przypadku gdy jest ona niedostępna lub nie istnieje,<br>podejmowane są ***<działania SA-05_ODP[01]>***. |
| | **SA-05d.** | dokumentacja jest przekazywana ***<personelowi lub rolom SA-05_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące dokumentacji systemu; dokumentacja systemu, w tym podręczniki administratora i użytkownika; dokumentacja projektowa systemu; zapisy dokumentujące próby uzyskania niedostępnej lub nieistniejącej dokumentacji systemu; wykaz działań podejmowanych w odpowiedzi na udokumentowane, nieudane próby uzyskania dokumentacji systemu, komponentu systemu lub usługi systemowej; dokumentacja strategii zarządzania ryzykiem; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| SA-05 | DOKUMENTACJA SYSTEMU | |
|---|---|---|
| | **SA-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu; personel organizacyjny odpowiedzialny za obsługę, eksploatację lub utrzymanie systemu; programiści systemu]. |
| | **SA-05-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie pozyskiwania, ochrony i dystrybucji dokumentacji administratora i użytkownika systemu]. |

| SA-05(01) | DOKUMENTACJA SYSTEMU \| WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ |
|---|---|
| | [WYCOFANE: Włączone do SA-04(01)]. |

| SA-05(02) | DOKUMENTACJA SYSTEMU \| BEZPIECZEŃSTWO INTERFEJSÓW SYSTEMU ZEWNĘTRZNEGO |
|---|---|
| | [WYCOFANE: Włączone do SA-04(02)]. |

| SA-05(03) | DOKUMENTACJA SYSTEMU \| PROJEKTOWANIE WYSOKOPOZIOMOWE |
|---|---|
| | [WYCOFANE: Włączone do SA-04(02)]. |

| SA-05(04) | DOKUMENTACJA SYSTEMU \| PROJEKTOWANIE NISKOPOZIOMOWE |
|---|---|
| | [WYCOFANE: Włączone do SA-04(02)]. |

| SA-05(05) | DOKUMENTACJA SYSTEMU \| KOD ŹRÓDŁOWY |
|---|---|
| | [WYCOFANE: Włączone do SA-04(02)]. |

| SA-06 | OGRANICZENIA W UŻYCIU OPROGRAMOWANIA |
|---|---|
| | [WYCOFANE: Włączone do CM-10, SI-07]. |

| SA-07 | OPROGRAMOWANIE ZAINSTALOWANE PRZEZ UŻYTKOWNIKA |
|---|---|
| | [WYCOFANE: Włączone do CM-11, SI-07]. |

| SA-08 | ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08_ODP[01]** | ***określono zasady inżynierii bezpieczeństwa dla systemów;*** |
| | **SA-08_ODP[02]** | ***określono zasady inżynierii prywatności dla systemów;*** |
| | **SA-08[01]** | ***<zasady inżynierii bezpieczeństwa dla systemów SA-08_ODP[01]>*** są stosowane w specyfikacji systemu i jego komponentów; |
| | **SA-08[02]** | ***<zasady inżynierii bezpieczeństwa dla systemów SA-08_ODP[01]>*** są stosowane przy projektowaniu systemu i jego komponentów; |
| | **SA-08[03]** | ***<zasady inżynierii bezpieczeństwa dla systemów SA-08_ODP[01]>*** są stosowane przy tworzeniu systemu i jego komponentów; |
| | **SA-08[04]** | ***<zasady inżynierii bezpieczeństwa dla systemów SA-08_ODP[01]>*** są stosowane przy wdrażaniu systemu i jego komponentów; |

| | | |
|---|---|---|
| **SA-08** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **SA-08[05]** | ***<zasady inżynierii bezpieczeństwa dla systemów SA-08_ODP[01]>*** są stosowane przy modyfikacji systemu i jego komponentów; |
| | **SA-08[06]** | ***<zasady inżynierii prywatności SA-08_ODP[02]>*** są stosowane w specyfikacji systemu i jego komponentów; |
| | **SA-08[07]** | ***<zasady inżynierii prywatności SA-08_ODP[02]>*** są stosowane przy projektowaniu systemu i jego komponentów; |
| | **SA-08[08]** | ***<zasady inżynierii prywatności SA-08_ODP[02]>*** są stosowane przy tworzeniu systemu i jego komponentów; |
| | **SA-08[09]** | ***<zasady inżynierii prywatności SA-08_ODP[02]>*** są stosowane przy wdrażaniu systemu i jego komponentów; |
| | **SA-08[10]** | ***<zasady inżynierii prywatności SA-08_ODP[02]>*** są stosowane przy modyfikacji systemu i jego komponentów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury oceny i autoryzacji; procedury dotyczące zasad inżynierii bezpieczeństwa i prywatności stosowanych przy tworzeniu specyfikacji, projektowaniu, opracowywaniu, wdrażaniu i modyfikowaniu systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu]. |

| | | |
|---|---|---|
| **SA-08** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **SA-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasad inżynierii bezpieczeństwa i prywatności przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasad inżynierii bezpieczeństwa i prywatności przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(01)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| PRZEJRZYSTE ABSTRAKCJE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(01)** | wdrożono zasadę projektowania bezpieczeństwa opartą na zasadzie przejrzystych abstrakcji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zasady projektowania zabezpieczeń w oparciu o przejrzyste abstrakcje przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SA-08(01)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| PRZEJRZYSTE ABSTRAKCJE** | |
| | **SA-08(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zasady projektowania zabezpieczeń w oparciu o przejrzyste abstrakcje przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o przejrzyste abstrakcje przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(02)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| MINIMALIZACJA MECHANIZMÓW WSPÓLNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(02)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o minimalizację wspólnych mechanizmów bezpieczeństwa;*** |
| | **SA-08(02)** | ***<systemy lub komponenty systemu SA-08(02)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o minimalizację wspólnych mechanizmów bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o minimalizację wspólnych mechanizmów bezpieczeństwa przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-08(02)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| MINIMALIZACJA MECHANIZMÓW WSPÓLNYCH** | |
| | **SA-08(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o minimalizację wspólnych mechanizmów bezpieczeństwa przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu;<br>mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o minimalizację wspólnych mechanizmów bezpieczeństwa przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(03)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| MODUŁOWOŚĆ I WARSTWOWOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(03)_ODP[01]** | ***określono systemy lub komponenty systemu, które wdrażają zasadę modułowego projektowania zabezpieczeń;*** |
| | **SA-08(03)_ODP[02]** | ***określono systemy lub komponenty systemu, które wdrażają zasadę warstwowego projektowania zabezpieczeń;*** |
| | **SA-08(03)[01]** | ***<systemy lub komponenty systemu SA-08(03)_ODP[01]>*** wdrażają zasadę modułowego projektowania zabezpieczeń; |

| | | |
|---|---|---|
| **SA-08(03)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| MODUŁOWOŚĆ I WARSTWOWOŚĆ** | |
| | **SA-08(03)[02]** | ***<systemy lub komponenty systemu SA-08(03)_ODP[02]>*** wdrażają zasadę warstwowego projektowania zabezpieczeń; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasad modułowego i warstwowego projektowania zabezpieczeń przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasad modułowego i warstwowego projektowania zabezpieczeń przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu;<br>mechanizmy wspierające stosowanie stosowania zasad modułowego i warstwowego projektowania zabezpieczeń przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające lub wdrażające granicę izolacji]. |

| | | |
|---|---|---|
| **SA-08(04)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| UPORZĄDKOWANIE ZALEŻNOŚCI POMIĘDZY SEGMENTAMI SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(04)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o częściowo uporządkowane zależności;*** |
| | **SA-08(04)** | ***<systemy lub komponenty systemu SA-08(04)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o częściowo uporządkowane zależności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zasady projektowania zabezpieczeń w oparciu o częściowo uporządkowane zależności przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SA-08(04)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| UPORZĄDKOWANIE ZALEŻNOŚCI POMIĘDZY SEGMENTAMI SYSTEMU** | |
| | **SA-08(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o częściowo uporządkowane zależności przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o częściowo uporządkowane zależności przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(05)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \|DOSTĘP Z EFEKTYWNĄ MEDIACJĄ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(05)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o skuteczny dostęp za pośrednictwem mediacji;*** |
| | **SA-08(05)** | ***<systemy lub komponenty systemu SA-08(05)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o skuteczny dostęp za pośrednictwem mediacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-08(05)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \|DOSTĘP Z EFEKTYWNĄ MEDIACJĄ** | |
| | **SA-08(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zasady projektowania zabezpieczeń w oparciu o skuteczny dostęp za pośrednictwem mediacji przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie/umowy; personel organizacyjny odpowiedzialny za określanie wymagań dotyczących bezpieczeństwa i prywatności systemu;<br>personel organizacyjny odpowiedzialny za specyfikację, projektowanie, rozwój, implementację i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o skuteczny dostęp za pośrednictwem mediacji przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o skuteczny dostęp za pośrednictwem mediacji przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(06)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| MINIMALIZACJA WSPÓŁUŻYTKOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(06)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o minimalizację współużytkowania;*** |
| | **SA-08(06)** | ***<systemy lub komponenty systemu SA-08(06)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o minimalizację współużytkowania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zasady projektowania zabezpieczeń w oparciu o minimalizację współużytkowania przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SA-08(06)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| MINIMALIZACJA WSPÓŁUŻYTKOWANIA** | |
| | **SA-08(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o minimalizację współużytkowania przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające projektowanie zabezpieczeń w oparciu o minimalizację współużytkowania przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(07)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \|ZMNIEJSZONA ZŁOŻONOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(07)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń opartą na zmniejszonej złożoności;*** |
| | **SA-08(07)** | ***<systemy lub komponenty systemu SA-08(07)_ODP>*** wdrażają zasadę projektowania zabezpieczeń opartą na zmniejszonej złożoności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zasady projektowania zabezpieczeń opartej na zmniejszonej złożoności przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-08(07)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \|ZMNIEJSZONA ZŁOŻONOŚĆ** | |
| | **SA-08(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(07)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń opartej na zmniejszonej złożoności przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń opartej na zmniejszonej złożoności przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(08)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZNA EWOLUCJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(08)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczną ewolucję;*** |
| | **SA-08(08)** | ***<systemy lub komponenty systemu SA-08(08)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczną ewolucję. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-08(08)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZNA EWOLUCJA** | |
| | **SA-08(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zasady projektowania zabezpieczeń w oparciu o bezpieczną ewolucję przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(08)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o bezpieczną ewolucję przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o bezpieczną ewolucję przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(09)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZAUFANE KOMPONENTY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(09)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o zaufane komponenty;*** |

| | | |
|---|---|---|
| **SA-08(09)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZAUFANE KOMPONENTY** | |
| | **SA-08(09)** | ***<systemy lub komponenty systemu SA-08(09)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o zaufane komponenty. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(09)-Badanie** | [WYBÓR SPOŚRÓD: Plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemu i usług; procedury dotyczące zasady projektowania zabezpieczeń w oparciu o zaufane komponenty przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa, zarządzania ryzykiem łańcucha dostaw oraz prywatności systemu; architektura bezpieczeństwa i prywatności systemu; procedury określania wiarygodności komponentów; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za specyfikację, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-08(09)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o zaufane komponenty przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o zaufane komponenty przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(10)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZAUFANIE HIERARCHICZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(10)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o hierarchiczne zaufanie;*** |
| | **SA-08(10)** | ***<systemy lub komponenty systemu SA-08(10)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o hierarchiczne zaufanie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o hierarchiczne zaufanie przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(10)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(10)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o hierarchiczne zaufanie przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o hierarchiczne zaufanie przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(11)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \|ODWROTNY PRÓG MODYFIKACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(11)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o odwrotny próg modyfikacji;*** |
| | **SA-08(11)** | ***<systemy lub komponenty systemu SA-08(11)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o odwrotny próg modyfikacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(11)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o odwrócony próg modyfikacji przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(11)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SA-08(11)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \|ODWROTNY PRÓG MODYFIKACJI** | |
| | **SA-08(11)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o odwrócony próg modyfikacji przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o odwrócony próg modyfikacji przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(12)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| OCHRONA HIERARCHICZNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(12)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o ochronę hierarchiczną;*** |
| | **SA-08(12)** | ***<systemy lub komponenty systemu SA-08(12)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o ochronę hierarchiczną. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zasady projektowania zabezpieczeń w oparciu o ochronę hierarchiczną przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-08(12)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| OCHRONA HIERARCHICZNA** | |
| | **SA-08(12)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(12)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o ochronę hierarchiczną przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o ochronę hierarchiczną przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(13)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| MINIMALIZACJA ELEMENTÓW BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(13)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o minimalizację elementów bezpieczeństwa;*** |
| | **SA-08(13)** | ***<systemy lub komponenty systemu SA-08(13)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o minimalizację elementów bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-08(13)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| MINIMALIZACJA ELEMENTÓW BEZPIECZEŃSTWA** | |
| | **SA-08(13)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o minimalizację elementów bezpieczeństwa przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(13)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(13)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o minimalizację elementów bezpieczeństwa przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o minimalizację elementów bezpieczeństwa przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(14)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZASADA WIEDZY KONIECZNEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(14)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o najmniejsze uprzywilejowanie;*** |

| | | |
|---|---|---|
| **SA-08(14)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZASADA WIEDZY KONIECZNEJ** | |
| | **SA-08(14)** | ***<systemy lub komponenty systemu SA-08(14)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o najmniejsze uprzywilejowanie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(14)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o najmniejsze uprzywilejowanie przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(14)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(14)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o najmniejsze uprzywilejowanie przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o najmniejsze uprzywilejowanie<br>przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(15)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \|PREDYKAT ZEZWOLEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(15)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o predykat zezwoleń;*** |
| | **SA-08(15)** | ***<systemy lub komponenty systemu SA-08(15)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o predykat zezwoleń. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(15)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o predykat zezwoleń przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(15)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SA-08(15)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \|PREDYKAT ZEZWOLEŃ** | |
| | **SA-08(15)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o predykat zezwoleń przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o predykat zezwoleń przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu]. |

| | | |
|---|---|---|
| **SA-08(16)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| SAMOISTNA WIARYGODNOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(16)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o samoistną wiarygodność;*** |
| | **SA-08(16)** | ***<systemy lub komponenty systemu SA-08(16)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o samoistną wiarygodność. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(16)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o samoistną wiarygodność przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-08(16)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| SAMOISTNA WIARYGODNOŚĆ** | |
| | **SA-08(16)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(16)-Test** | [WYBÓR SPOŚRÓD: Procesy dotyczące organizacyjne stosowania zasady projektowania zabezpieczeń w oparciu o samoistną wiarygodność przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o samoistną wiarygodność przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(17)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZNY SKŁAD ROZPROSZONY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(17)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczny skład rozproszony;*** |
| | **SA-08(17)** | ***<systemy lub komponenty systemu SA-08(17)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczny skład rozproszony. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-08(17)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZNY SKŁAD ROZPROSZONY** | |
| | **SA-08(17)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zasady projektowania zabezpieczeń w oparciu o bezpieczny skład rozproszony przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(17)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(17)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o bezpieczny skład rozproszony przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o bezpieczny skład rozproszony przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(18)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZAUFANE KANAŁY KOMUNIKACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(18)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o zaufane kanały komunikacji;*** |

| | | |
|---|---|---|
| **SA-08(18)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZAUFANE KANAŁY KOMUNIKACJI** | |
| | **SA-08(18)** | ***<systemy lub komponenty systemu SA-08(18)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o zaufane kanały komunikacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(18)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o zaufane kanały komunikacji przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(18)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(18)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o zaufane kanały komunikacji przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o zaufane kanały komunikacji przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(19)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| CIĄGŁA OCHRONA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(19)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o ciągłą ochronę;*** |
| | **SA-08(19)** | ***<systemy lub komponenty systemu SA-08(19)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o ciągłą ochronę. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(19)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka kontroli dostępu; polityka ochrony systemu i komunikacji; procedury dotyczące ochrony granic; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o ciągłą ochronę przy tworzeniu specyfikacji, projektowaniu, opracowywaniu, wdrażaniu i modyfikacji systemu;<br>ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(19)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określanie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za specyfikację, projektowanie, rozwój, wdrażanie i modyfikację systemu;<br>personel organizacyjny odpowiedzialny za egzekwowanie uprawnień dostępu; administratorzy systemu/sieci; programiści systemu; personel organizacyjny odpowiedzialny za ochronę informacji; personel organizacyjny odpowiedzialny za ochronę granic]. |

| | | |
|---|---|---|
| **SA-08(19)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| CIĄGŁA OCHRONA** | |
| | **SA-08(19)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o ciągłą ochronę przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu;<br>mechanizmy wdrażające funkcje egzekwowania uprawnień dostępu;<br>mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o ciągłą ochronę przy tworzeniu specyfikacji, projektowaniu, opracowywaniu, wdrażaniu i modyfikowaniu systemu; mechanizmy wspierające lub wdrażające zasadę bezpiecznej awarii]. |

| | | |
|---|---|---|
| **SA-08(20)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZNE ZARZĄDZANIE METADANYMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(20)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczne zarządzanie metadanymi;*** |
| | **SA-08(20)** | ***<systemy lub komponenty systemu SA-08(20)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczne zarządzanie metadanymi. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-08(20)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZNE ZARZĄDZANIE METADANYMI** | |
| | **SA-08(20)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zasady projektowania zabezpieczeń w oparciu o bezpieczne zarządzanie metadanymi przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(20)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(20)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o bezpieczne zarządzanie metadanymi przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu;<br>mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o bezpieczne zarządzanie metadanymi przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(21)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| SAMOANALIZY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(21)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o samoanalizę;*** |
| | **SA-08(21)** | ***<systemy lub komponenty systemu SA-08(21)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o samoanalizę. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(21)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o samoanalizę przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(21)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(21)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o samoanalizę przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu;<br>mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o samoanalizę przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(22)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI I OCHRONY PRYWATNOŚCI \| ROZLICZALNOŚĆ I IDENTYFIKOWALNOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(22)_ODP[01]** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń, w oparciu o rozliczalność;*** |
| | **SA-08(22)_ODP[02]** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń, w oparciu o identyfikowalność;*** |
| | **SA-08(22)[01]** | ***<systemy lub komponenty systemu SA-08(22)_ODP[01]>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o rozliczalność; |
| | **SA-08(22)[02]** | ***<systemy lub komponenty systemu SA-08(22)_ODP[02]>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o identyfikowalność. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(22)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka audytu i rozliczalności; polityka kontroli dostępu; procedury dotyczące zasady wiedzy koniecznej; procedury dotyczące zdarzeń podlegających audytowi; polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o rozliczalność i identyfikowalność przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikowaniu systemu; dokumentacja projektowa systemu; zapisy z audytu systemu; zdarzenia systemowe podlegające audytowi; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-08(22)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI I OCHRONY PRYWATNOŚCI \| ROZLICZALNOŚĆ I IDENTYFIKOWALNOŚĆ** | |
| | **SA-08(22)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za audyt i rozliczalność; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(22)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o rozliczalność i identyfikowalność przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o rozliczalność i identyfikowalność przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wdrażające audyt systemu informatycznego; mechanizmy wdrażające funkcje dotyczące zasady wiedzy koniecznej]. |

| | | |
|---|---|---|
| **SA-08(23)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZABEZPIECZENIA DOMYŚLNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(23)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń, w oparciu o zabezpieczenia domyślne;*** |
| | **SA-08(23)** | ***<systemy lub komponenty systemu SA-08(23)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o zabezpieczenia domyślne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-08(23)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZABEZPIECZENIA DOMYŚLNE** | |
| | **SA-08(23)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka zarządzania konfiguracją; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o zabezpieczenia domyślne przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; procedury dotyczące konfiguracji bazowej systemu; plan zarządzania konfiguracją; architektura i dokumentacja konfiguracyjna systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; procedury dotyczące dokumentacji systemu; dokumentacja systemowa; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(23)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(23)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o zabezpieczenia domyślne przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o zabezpieczenia domyślne przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; procesy organizacyjne dotyczące zarządzania konfiguracjami bazowymi; mechanizmy wspierające kontrolę konfiguracji bazowej]. |

| | | |
|---|---|---|
| **SA-08(24)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZNA AWARIA I ODZYSKIWANIE DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(24)_ODP[01]** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczną awarię;*** |
| | **SA-08(24)_ODP[02]** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczne odzyskiwanie danych;*** |
| | **SA-08(24)[01]** | ***<systemy lub komponenty systemu SA-08(24)_ODP[01]>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczną awarię; |
| | **SA-08(24)[02]** | ***<systemy lub komponenty systemu SA-08(24)_ODP[02]>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczne odzyskiwanie danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(24)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka ochrony systemu i komunikacji; polityka planowania awaryjnego; procedury dotyczące odzyskiwania i odtwarzania systemu informacyjnego; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o bezpieczną awarię i odzyskiwanie danych przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; plan awaryjny; procedury dotyczące tworzenia kopii zapasowych systemu; dokumentacja testowa planu awaryjnego; wyniki testów planu awaryjnego; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-08(24)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZNA AWARIA I ODZYSKIWANIE DANYCH** | |
| | **SA-08(24)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; personel organizacyjny odpowiedzialny za testowanie planów awaryjnych;<br>personel organizacyjny odpowiedzialny za odzyskiwanie i odtwarzanie systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za tworzenie kopii zapasowych systemów informatycznych]. |
| | **SA-08(24)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o bezpieczną awarię i odzyskiwanie przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o bezpieczną awarię i odzyskiwanie przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające lub wdrażające stosowanie zasady bezpiecznej awarii; procesy organizacyjne dotyczące testowania planu awaryjnego; mechanizmy wspierające testowanie planu awaryjnego; mechanizmy wspierające odzyskiwanie i odtwarzanie systemu; procesy organizacyjne dotyczące tworzenia kopii zapasowych systemu; mechanizmy wspierające lub wdrażające tworzenie kopii zapasowych systemu]. |

| | | |
|---|---|---|
| **SA-08(25)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZEŃSTWO EKONOMICZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(25)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczeństwo ekonomiczne;*** |
| | **SA-08(25)** | ***<systemy lub komponenty systemu SA-08(25)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczeństwo ekonomiczne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(25)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zasady projektowania zabezpieczeń w oparciu o bezpieczeństwo ekonomiczne przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; analiza kosztów i korzyści; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(25)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SA-08(25)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZEŃSTWO EKONOMICZNE** | |
| | **SA-08(25)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o bezpieczeństwo ekonomiczne przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o bezpieczeństwo ekonomiczne przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(26)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| PEWNOŚĆ DZIAŁANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(26)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o pewność działania;*** |
| | **SA-08(26)** | ***<systemy lub komponenty systemu SA-08(26)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o pewność działania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(26)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o pewność działania przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; analiza dotycząca kompromisu między wydajnością a bezpieczeństwem; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-08(26)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| PEWNOŚĆ DZIAŁANIA** | |
| | **SA-08(26)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(26)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o pewność działania przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o pewność działania przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu]. |

| | | |
|---|---|---|
| **SA-08(27)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZEŃSTWO UWZGLĘDNIAJĄCE CZYNNIK LUDZKI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(27)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o czynnik ludzki;*** |
| | **SA-08(27)** | ***<systemy lub komponenty systemu SA-08(27)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o czynnik ludzki. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-08(27)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZEŃSTWO UWZGLĘDNIAJĄCE CZYNNIK LUDZKI** | |
| | **SA-08(27)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o czynnik ludzki przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu;<br>dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; analiza użyteczności; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(27)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za zabezpieczenia projektowane w oparciu o czynnik ludzki;<br>personel organizacyjny odpowiedzialny za specyfikację, projektowanie, rozwój, implementację i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(27)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o czynnik ludzki przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o czynnik ludzki przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu; mechanizmy egzekwujące stosowanie polityki bezpieczeństwa]. |

| | | |
|---|---|---|
| **SA-08(28)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| AKCEPTOWALNY POZIOM BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(28)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń, w oparciu o akceptowalny poziom bezpieczeństwa;*** |
| | **SA-08(28)** | ***<systemy lub komponenty systemu SA-08(28)_ODP>*** wdrażają zasadę projektowania zabezpieczeń, w oparciu o akceptowalny poziom bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(28)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o akceptowalny poziom bezpieczeństwa przy tworzeniu specyfikacji, projektowaniu, rozwoju i modyfikacji systemu; dokumentacja projektowa systemu;<br>wymogi i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; polityka przetwarzania danych identyfikacyjnych; powiadomienia o ochronie prywatności przekazywane użytkownikom; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka w zakresie ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-08(28)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu]. |

| | | |
|---|---|---|
| **SA-08(28)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| AKCEPTOWALNY POZIOM BEZPIECZEŃSTWA** | |
| | **SA-08(28)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o akceptowalny poziom bezpieczeństwa przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie z zasady projektowania zabezpieczeń w oparciu o akceptowalny poziom bezpieczeństwa przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu;<br>mechanizmy egzekwujące stosowanie polityki bezpieczeństwa]. |

| | | |
|---|---|---|
| **SA-08(29)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| POWTARZALNE I UDOKUMENTOWANE PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(29)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o powtarzalne i udokumentowane procedury;*** |
| | **SA-08(29)** | ***<systemy lub komponenty systemu SA-08(29)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o powtarzalne i udokumentowane procedury. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-08(29)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| POWTARZALNE I UDOKUMENTOWANE PROCEDURY** | |
| | **SA-08(29)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o powtarzalne i udokumentowane procedury przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(29)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(29)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o powtarzalne i udokumentowane procedury przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o powtarzalne i udokumentowane procedury przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy stosowanie egzekwujące polityki bezpieczeństwa]. |

| | | |
|---|---|---|
| **SA-08(30)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| RYGOR PROCEDURALNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(30)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o rygor proceduralny;*** |
| | **SA-08(30)** | ***<systemy lub komponenty systemu SA-08(30)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o rygor proceduralny. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(30)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o rygor proceduralny przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(30)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SA-08(30)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| RYGOR PROCEDURALNY** | |
| | **SA-08(30)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o rygor proceduralny przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o rygor proceduralny przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy egzekwujące stosowanie polityki bezpieczeństwa]. |

| | | |
|---|---|---|
| **SA-08(31)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZNA MODYFIKACJA SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(31)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczną modyfikację systemu;*** |
| | **SA-08(31)** | ***<systemy lub komponenty systemu SA-08(31)_ODP>*** wdrażają zasadę projektowania zabezpieczeń w oparciu o bezpieczną modyfikację systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-08(31)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| BEZPIECZNA MODYFIKACJA SYSTEMU** | |
| | **SA-08(31)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka i procedury zarządzania konfiguracją; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o bezpieczną modyfikację systemu przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dotycząca zabezpieczania zmian konfiguracji; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(31)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SA-08(31)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o bezpieczną modyfikację systemu przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o bezpieczną modyfikację systemu przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy egzekwujące stosowanie polityki bezpieczeństwa; procesy organizacyjne w zakresie zarządzania konfiguracją zmian; mechanizmy wspierające kontrolę konfiguracji]. |

| | | |
|---|---|---|
| **SA-08(32)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| NIEZBĘDNA DOKUMENTACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(32)_ODP** | ***określono systemy lub komponenty systemu, które wdrażają zasadę projektowania zabezpieczeń, w oparciu o niezbędną dokumentację;*** |
| | **SA-08(32)** | ***<systemy lub komponenty systemu SA-08(32)_ODP>*** wdrażają zasadę projektowania zabezpieczeń, w oparciu o niezbędną dokumentację. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-08(32)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o niezbędną dokumentację przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu;<br>dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dotycząca zabezpieczania zmian konfiguracji; wymagania i specyfikacje dotyczące bezpieczeństwa i prywatności systemu; dokumentacja dotycząca bezpieczeństwa i prywatności systemu; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-08(32)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie wymagań dotyczących bezpieczeństwa i prywatności systemu; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SA-08(32)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| NIEZBĘDNA DOKUMENTACJA** | |
| | **SA-08(32)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady projektowania zabezpieczeń w oparciu o niezbędną dokumentację przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu;<br>mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o niezbędną dokumentację przy tworzeniu specyfikacji, projektowaniu, rozwoju, implementacji i modyfikacji systemu; mechanizmy egzekwujące stosowanie polityki bezpieczeństwa; procesy organizacyjne dotyczące zarządzania konfiguracją zmian; mechanizmy wspierające kontrolę konfiguracji]. |

| | | |
|---|---|---|
| **SA-08(33)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZASADA MINIMALIZACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-08(33)_ODP** | ***określono procesy, które wdrażają zasadę ochrony prywatności w oparciu o minimalizację;*** |
| | **SA-08(33)** | zasada ochrony prywatności w oparciu o minimalizację jest wdrażana za pomocą ***<procesów SA-08(33)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-08(33)** | **ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| ZASADA MINIMALIZACJI** | |
| | **SA-08(33)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; polityka przetwarzania danych identyfikacyjnych; procedury dotyczące minimalizacji stosowania danych identyfikacyjnych w projekcie systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>dokumentacja dotycząca zabezpieczania zmian konfiguracji; wymogi i specyfikacje dotyczące bezpieczeństwa i prywatności informacji w systemie; architektura bezpieczeństwa i prywatności systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka w zakresie ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-08(33)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za tworzenie specyfikacji, projektowanie, rozwój, wdrażanie i modyfikację systemu; programiści systemu]. |
| | **SA-08(33)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania zasady ochrony prywatności w oparciu o minimalizację przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy wspierające stosowanie zasady projektowania zabezpieczeń w oparciu o niezbędną dokumentację przy tworzeniu specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu; mechanizmy egzekwujące stosowanie polityki bezpieczeństwa i prywatności; procesy organizacyjne w zakresie zarządzania konfiguracją zmian; mechanizmy wspierające kontrolę konfiguracji]. |

| | | |
|---|---|---|
| **SA-09** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-09_ODP[01]** | ***określono zabezpieczenia, które mają być stosowane przez dostawców zewnętrznych usług systemowych;*** |
| | **SA-09_ODP[02]** | ***określono procesy, metody i techniki stosowane do monitorowania stosowania zabezpieczeń przez zewnętrznych dostawców usług;*** |
| | **SA-09a.[01]** | dostawcy zewnętrznych usług systemowych spełniają organizacyjne wymogi w zakresie bezpieczeństwa; |
| | **SA-09a.[02]** | dostawcy zewnętrznych usług systemowych spełniają organizacyjne wymogi w zakresie ochrony prywatności; |
| | **SA-09a.[03]** | dostawcy zewnętrznych usług systemowych stosują ***<zabezpieczenia SA-09_ODP[01]>***; |
| | **SA-09b.[01]** | określono i udokumentowano kwestie dotyczące nadzoru organizacyjnego w odniesieniu do zewnętrznych usług systemowych; |
| | **SA-09b.[02]** | określono i udokumentowano role i obowiązki użytkowników w odniesieniu do zewnętrznych usług systemowych; |
| | **SA-09c.** | stosuje się ***<procesy, metody i techniki SA-09_ODP[02]>*** do bieżącego monitorowania zgodności zabezpieczeń wykorzystywanych przez zewnętrznych dostawców usług. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-09** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE** | |
| | **SA-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące metod i technik monitorowania zgodności zabezpieczeń wykorzystywanych przez dostawców zewnętrznych usług systemowych; dokumentacja dotycząca nabywania; umowy; umowy o poziomie usług; umowy międzyorganizacyjne; umowy licencyjne; wykaz wymogów organizacyjnych dotyczących bezpieczeństwa i prywatności usług świadczonych przez zewnętrznych usługodawców; wyniki lub sprawozdania z oceny zabezpieczeń przeprowadzonej przez dostawców zewnętrznych usług systemowych; plan bezpieczeństwa systemu; plan ochrony prywatności; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; zewnętrzni dostawcy usług systemowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-09-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące bieżącego monitorowania zgodności zabezpieczeń i środków ochrony prywatności wykorzystywanych przez zewnętrznych dostawców usług; mechanizmy bieżącego monitorowania zgodności zabezpieczeń i środków ochrony prywatności wykorzystywanych przez zewnętrznych dostawców usług]. |

| | | |
|---|---|---|
| **SA-09(01)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| OCENA RYZYKA/ZATWIERDZENIA ORGANIZACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-09(01)_ODP** | ***określono personel lub role, które zatwierdzają nabycie lub zlecenie wykonania dedykowanych usług w zakresie bezpieczeństwa informacji;*** |

| | | |
|---|---|---|
| **SA-09(01)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| OCENA RYZYKA/ZATWIERDZENIA ORGANIZACYJNE** | |
| | **SA-09(01)(a)** | określono personel lub role, które zatwierdzają nabycie lub zlecenie wykonania dedykowanych usług w zakresie bezpieczeństwa informacji; |
| | **SA-09(01)(b)** | ***<personel lub role SA-09(01)_ODP>*** zatwierdzają nabycie lub zlecenie wykonania dedykowanych usług w zakresie bezpieczeństwa informacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-09(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka i procedury zarządzania ryzykiem łańcucha dostaw; procedury dotyczące zewnętrznych usług systemowych; dokumentacja dotycząca nabycia; umowy nabycia systemu, komponentu systemu lub usługi systemowej; sprawozdania z oceny ryzyka; dokumentacja dotycząca zatwierdzenia nabycia lub zlecenia wykonania dedykowanych usług w zakresie bezpieczeństwa; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-09(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo systemu; dostawcy zewnętrznych usług systemowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-09(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przeprowadzania oceny ryzyka przed nabyciem lub zleceniem wykonania dedykowanych usług w zakresie bezpieczeństwa informacji; procesy organizacyjne dotyczące zatwierdzania zlecenia wykonania dedykowanych usług w zakresie bezpieczeństwa informacji; mechanizmy wspierające lub wdrażające ocenę ryzyka; mechanizmy wspierające lub wdrażające procesy zatwierdzania]. |

| | | |
|---|---|---|
| **SA-09(02)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| IDENTYFIKACJA FUNKCJI, PORTÓW, PROTOKOŁÓW I USŁUG** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-09(02)_ODP** | ***określono zewnętrzne usługi systemowe, które wymagają zidentyfikowania funkcji, portów, protokołów i innych usług;*** |
| | **SA-09(02)** | dostawcy ***<zewnętrznych usług systemowych SA-09(02)_ODP>*** są zobowiązani do zidentyfikowania funkcji, portów, protokołów i innych usług wymaganych do korzystania z takich usług. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-09(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka i procedury zarządzania ryzykiem łańcucha dostaw; procedury dotyczące zewnętrznych usług systemowych; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja nabycia; dokumentacja przetargowa; umowy o poziomie usług; organizacyjne wymogi w zakresie bezpieczeństwa organizacyjnego i specyfikacje bezpieczeństwa dla zewnętrznych dostawców usług; wykaz wymaganych funkcji, portów, protokołów i innych usług; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-09(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; dostawcy zewnętrznych usług systemowych]. |

| | | |
|---|---|---|
| **SA-09(03)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| TWORZENIE/UTRZYMANIE RELACJI ZAUFANIA Z DOSTAWCAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-09(03)_ODP[01]** | ***określono wymagania, właściwości, czynniki lub warunki w zakresie bezpieczeństwa określające dopuszczalne relacje zaufania, na podstawie których utrzymywana jest relacja zaufania;*** |
| | **SA-09(03)_ODP[02]** | ***określono wymagania, właściwości, czynniki lub warunki w zakresie prywatności określające dopuszczalne relacje zaufania, na podstawie których utrzymywana jest relacja zaufania;*** |
| | **SA-09(03)[01]** | ustanowiono i udokumentowano relacje zaufania z zewnętrznymi dostawcami usług, oparte na ***<wymaganiach, właściwościach, czynnikach lub warunkach w zakresie bezpieczeństwa SA-09(03)_ODP[01]>***; |
| | **SA-09(03)[02]** | utrzymywane są relacje zaufania z zewnętrznymi dostawcami usług, oparte na ***<wymaganiach, właściwościach, czynnikach lub warunkach w zakresie bezpieczeństwa SA-09(03)_ODP[01]>***; |
| | **SA-09(03)[03]** | ustanowiono i udokumentowano relacje zaufania z zewnętrznymi dostawcami usług, oparte na ***<wymaganiach, właściwościach, czynnikach lub warunkach w zakresie prywatności SA-09(03)_ODP[02]>***; |
| | **SA-09(03)[04]** | utrzymywane są relacje zaufania z zewnętrznymi dostawcami usług, oparte na ***<wymaganiach, właściwościach, czynnikach lub warunkach w zakresie prywatności SA-09(03)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-09(03)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| TWORZENIE/UTRZYMANIE RELACJI ZAUFANIA Z DOSTAWCAMI** | |
| | **SA-09(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja nabycia; dokumentacja zamówienia; umowy o poziomie usług; protokół ustaleń; protokół uzgodnień; wykaz wymogów, właściwości, czynników lub warunków dotyczących usług świadczonych przez dostawców zewnętrznych; dokumentacja dotycząca relacji zaufania z zewnętrznymi dostawcami usług; plan bezpieczeństwa systemu; plan ochrony prywatności; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-09(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; zewnętrzni dostawcy usług systemowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; zewnętrzni dostawcy usług systemowych; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |

| | | |
|---|---|---|
| **SA-09(04)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| ZGODNOŚĆ INTERESÓW KONSUMENTÓW I DOSTAWCÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-09(04)_ODP[01]** | ***określono zewnętrznych dostawców usług;*** |
| | **SA-09(04)_ODP[02]** | ***określono działania, które należy podjąć w celu weryfikacji, czy interesy zewnętrznych dostawców usług są zgodne z interesami organizacji i odzwierciedlają je;*** |

| | | |
|---|---|---|
| **SA-09(04)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| ZGODNOŚĆ INTERESÓW KONSUMENTÓW I DOSTAWCÓW** | |
| | **SA-09(04)** | podejmowane są ***<działania SA-09(04)_ODP[02]> w*** celu sprawdzenia czy interesy ***<zewnętrznych dostawców usług SA-09(04)_ODP[01]>*** są zgodne z interesami organizacji i odzwierciedlają je. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-09(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zewnętrznych usług systemowych; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; organizacyjne wymagania/zabezpieczenia w zakresie zewnętrznych dostawców usług; polityka bezpieczeństwa personelu w zakresie zewnętrznych dostawców usług; oceny przeprowadzane w odniesieniu do zewnętrznych dostawców usług; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-09(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; zewnętrzni dostawcy usług systemowych; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-09(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące określania i stosowania zabezpieczeń w celu zapewnienia zgodności interesów organizacji oraz zewnętrznych dostawców usług; mechanizmy wspierające lub wdrażające zabezpieczenia w celu zapewnienia zgodności interesów organizacji oraz zewnętrznych dostawców usług]. |

| | | |
|---|---|---|
| **SA-09(05)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| OBSZAR PROCESOWANIA, PRZECHOWYWANIA I OBSŁUGI TECHNICZNEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-09(05)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {przetwarzanie informacji; informacje lub dane; usługi systemowe};*** |
| | **SA-09(05)_ODP[02]** | ***określono lokalizacje, gdzie <WYBRANA WARTOŚĆ PARAMETRU SA-09(05)_ODP[01]> podlega ograniczeniom;*** |
| | **SA-09(05)_ODP[03]** | ***określono wymagania lub warunki w zakresie ograniczania lokalizacji <WYBRANA WARTOŚĆ PARAMETRU SA-09(05)_ODP[01]>;*** |
| | **SA-09(05)** | na podstawie ***<wymagań SA-09(05)_ODP[03]> <WYBRANA WARTOŚĆ PARAMETRU SA-09(05)_ODP[01]>*** jest ograniczona do ***<lokalizacji SA-09(05)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-09(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zewnętrznych usług systemowych; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; ograniczenia w zakresie lokalizacji przetwarzania informacji; informacji/danych lub usług systemowych; przetwarzanie informacji, informacji/danych lub usługi systemowe, które mają być utrzymywane w lokalizacjach objętych ograniczeniami; organizacyjne wymagania lub warunki w zakresie bezpieczeństwa obowiązujące dostawców zewnętrznych; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-09(05)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| OBSZAR PROCESOWANIA, PRZECHOWYWANIA I OBSŁUGI TECHNICZNEJ** | |
| | **SA-09(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; zewnętrzni dostawcy usług systemowych; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-09(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie określania wymagań dotyczących ograniczeń co do lokalizacji przetwarzania informacji, informacji/danych lub usług informacyjnych; procesy organizacyjne w zakresie zapewnienia, że lokalizacja jest objęta ograniczeniami zgodnie z ustanowionymi wymaganiami lub warunkami]. |

| | | |
|---|---|---|
| **SA-09(06)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| NADZOROWANIE ZARZĄDZANIA KLUCZAMI KRYPTOGRAFICZNYMI PRZEZ ORGANIZACJĘ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-09(06)** | utrzymywana jest wyłączna kontrola nad kluczami kryptograficznymi zabezpieczającymi zaszyfrowane materiały przechowywane lub przesyłane przez system zewnętrzny. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-09(06)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| NADZOROWANIE ZARZĄDZANIA KLUCZAMI KRYPTOGRAFICZNYMI PRZEZ ORGANIZACJĘ** | |
| | **SA-09(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zewnętrznych usług systemowych; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; procedury dotyczące zarządzania kluczami kryptograficznymi kontrolowanymi przez organizację; organizacyjne wymagania lub warunki w zakresie bezpieczeństwa obowiązujące dostawców zewnętrznych; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-09(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie kluczami kryptograficznymi; zewnętrzni dostawcy usług systemowych; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-09(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zarządzania kluczami kryptograficznymi; mechanizmy wspomagania i wdrażania procesu zarządzania kluczami kryptograficznymi kontrolowanymi przez organizację]. |

| | | |
|---|---|---|
| **SA-09(07)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| ORGANIZACYJNIE KONTROLOWANE ZABEZPIECZENIA INTEGRALNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-09(07)** | zapewniono możliwość weryfikacji integralności informacji przechowywanej w systemie zewnętrznym. |

| | | |
|---|---|---|
| **SA-09(07)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| ORGANIZACYJNIE KONTROLOWANE ZABEZPIECZENIA INTEGRALNOŚCI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-09(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zewnętrznych usług systemowych; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja przetargowa; dokumentacja nabycia;<br>umowy o poziomie usług; procedury dotyczące kontrolowanej przez organizację weryfikacji integralności; informacji/danych lub usług systemowych; wymagania lub warunki w zakresie bezpieczeństwa obowiązujące dostawców zewnętrznych; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-09(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za weryfikację integralności; zewnętrzni dostawcy usług systemowych; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-09(07)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące weryfikacji integralności; mechanizmy wspierania i wdrażania weryfikacji integralności informacji w systemach zewnętrznych]. |

| | |
|---|---|
| **SA-09(08)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| LOKALIZACJA PRZETWARZANIA I PRZECHOWYWANIA - JURYSDYKCJA KRAJOWA** |
| | **CEL OCENY:**<br>*Ustalenie, czy:* |

| | | |
|---|---|---|
| **SA-09(08)** | **ZEWNĘTRZNE USŁUGI SYSTEMOWE \| LOKALIZACJA PRZETWARZANIA I PRZECHOWYWANIA - JURYSDYKCJA KRAJOWA** | |
| | **SA-09(08)** | geograficzna lokalizacja przetwarzania informacji i przechowywania danych jest ograniczona do obiektów znajdujących się w granicach jurysdykcji prawnej Państwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-09(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące zewnętrznych usług systemowych; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; procedury dotyczące ograniczania lokalizacji przetwarzania i przechowywania danych do tych znajdujących się w jurysdykcji Państwa; informacje/dane lub usługi systemowe;<br><br>organizacyjne wymagania lub warunki w zakresie bezpieczeństwa obowiązujące dostawców zewnętrznych; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-09(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw; zewnętrzni dostawcy usług systemowych]. |
| | **SA-09(08)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne ograniczające przetwarzanie i przechowywanie danych przez zewnętrznych dostawców usług systemowych do granic jurysdykcji prawnej Państwa]. |

| | | |
|---|---|---|
| **SA-10** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-10_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {projektowanie, opracowanie, wdrożenie, obsługa, utylizacja};*** |
| | **SA-10_ODP[02]** | ***określono elementy konfiguracji w ramach zarządzania konfiguracją;*** |
| | **SA-10_ODP[03]** | ***określono personel, któremu zgłaszane są luki w zabezpieczeniach systemu, komponentu lub usługi oraz sposoby ich usuwania;*** |
| | **SA-10a.** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby zarządzał konfiguracją podczas eksploatacji takiego systemu, komponentu lub usługi<br>***<WYBRANA WARTOŚĆ PARAMETRU SA-10_ODP[01]>***; |
| | **SA-10b.[01]** | twórca systemu, komponentu systemu lub usługi systemowej jest zobowiązany do udokumentowania integralności zmian w***<elementach konfiguracji SA-10_ODP[02]>***; |
| | **SA-10b.[02]** | twórca systemu, komponentu systemu lub usługi systemowej jest zobowiązany do zarządzania integralnością zmian w***<elementach konfiguracji SA-10_ODP[02]>***; |
| | **SA-10b.[03]** | twórca systemu, komponentu systemu lub usługi systemowej jest zobowiązany do kontrolowania integralności zmian w***<elementach konfiguracji SA-10_ODP[02]>***; |
| | **SA-10c.** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wdrażania w systemie, komponencie lub usłudze wyłącznie zmian zatwierdzonych przez organizację; |
| | **SA-10d.[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się dokumentowania zatwierdzonych zmian wdrożonych w takim systemie, komponencie lub usłudze; |

| | | |
|---|---|---|
| **SA-10** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA** | |
| | **SA-10d.[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się dokumentowania potencjalnego wpływu zatwierdzonych zmian na bezpieczeństwo; |
| | **SA-10d.[03]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się dokumentowania potencjalnego wpływu zatwierdzonych zmian na prywatność; |
| | **SA-10e.[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się śledzenia usterek w takim systemie, komponencie lub usłudze; |
| | **SA-10e.[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się śledzenia procesu usuwania usterek w takim systemie, komponencie lub usłudze; |
| | **SA-10e.[03]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się zgłaszania poczynionych ustaleń ***<personelowi SA-10_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemów i usług; procedury dotyczące zarządzania konfiguracją przez programistę systemu; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plan dotyczący zarządzania konfiguracją systemu przez programistę; dokumentacja dotycząca luk w zabezpieczeniach i ich usuwania; dokumentacja dotycząca zatwierdzania zmian w systemie; dokumentacja dotycząca zabezpieczania zmian konfiguracji; dokumentacja dotycząca zarządzania konfiguracją; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-10** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA** | |
| | **SA-10-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; programiści systemu]. |
| | **SA-10-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania procesu zarządzania konfiguracją przez programistę; mechanizmy wspierające lub wdrażające monitorowanie procesu zarządzania konfiguracją przez programistę]. |

| | | |
|---|---|---|
| **SA-10(01)** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA \| WERYFIKACJA INTEGRALNOŚCI PROGRAMÓW I OPROGRAMOWANIA UKŁADOWEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-10(01)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby umożliwiał weryfikację integralności komponentów aplikacji i oprogramowania układowego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-10(01)** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA \| WERYFIKACJA INTEGRALNOŚCI PROGRAMÓW I OPROGRAMOWANIA UKŁADOWEGO** | |
| | **SA-10(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemów i usług; procedury dotyczące zarządzania konfiguracją przez programistę systemu; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plan dotyczący zarządzania konfiguracją systemu przez programistę; zapisy dotyczące weryfikacji integralności oprogramowania i oprogramowania układowego; zapisy dotyczące autoryzacji zmian w systemie; dokumentacja dotycząca zabezpieczania zmian konfiguracji; zapisy dotyczące zarządzania konfiguracją; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-10(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją;<br>programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-10(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania procesu zarządzania konfiguracją przez programistę; mechanizmy wspierające lub wdrażające monitorowanie procesu zarządzania konfiguracją przez programistę]. |

| | | |
|---|---|---|
| **SA-10(02)** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA \| ALTERNATYWNE PROCESY ZARZĄDZANIA KONFIGURACJĄ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-10(02)** | zapewniono alternatywny proces zarządzania konfiguracją z wykorzystaniem personelu organizacyjnego w przypadku braku dedykowanego zespołu programistów zarządzających konfiguracją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-10(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; polityka zarządzania konfiguracją; plan zarządzania konfiguracją; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plan dotyczący zarządzania konfiguracją systemu przez programistę; analizy wpływu na bezpieczeństwo; analizy wpływu na prywatność; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-10(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; programiści systemu]. |
| | **SA-10(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania procesu zarządzania konfiguracją przez programistę; mechanizmy wspierające lub wdrażające monitorowanie procesu zarządzania konfiguracją przez programistę]. |

| | | |
|---|---|---|
| **SA-10(03)** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA \| WERYFIKACJA INTEGRALNOŚCI SPRZĘTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-10(03)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się umożliwienia weryfikacji integralności komponentów sprzętowych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-10(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zarządzania konfiguracją programiści systemu; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plan zarządzania konfiguracją programiści systemu; zapisy dotyczące weryfikacji integralności sprzętu; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-10(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją;<br>programiści systemu; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-10(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania procesu zarządzania konfiguracją przez programistę; mechanizmy wspierające lub wdrażające monitorowanie procesu zarządzania konfiguracją przez programistę]. |

| | | |
|---|---|---|
| **SA-10(04)** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA \| ZAUFANA GENERACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-10(04)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się stosowania narzędzi do porównywania nowo wygenerowanych wersji opisów sprzętu istotnych z punktu widzenia bezpieczeństwa z poprzednimi wersjami; |
| | **SA-10(04)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się stosowania narzędzi do porównywania nowo wygenerowanych wersji kodu źródłowego z poprzednimi wersjami; |
| | **SA-10(04)[03]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się stosowania narzędzi do porównywania nowo wygenerowanych wersji kodu obiektowego z poprzednimi wersjami. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-10(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zarządzania konfiguracją systemu przez programistę; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plan zarządzania konfiguracją systemu przez programistę; dokumentacja kontroli zmian; dokumentacja zarządzania konfiguracją; dokumentacja audytu kontroli konfiguracji; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-10(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania procesu zarządzania konfiguracją przez programistę; mechanizmy wspierające lub wdrażające monitorowanie procesu zarządzania konfiguracją przez programistę]. |

| | | |
|---|---|---|
| **SA-10(05)** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA \| INTEGRALNOŚĆ MAPOWANIA KONTROLI WERSJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-10(05)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się zachowania integralności mapowania pomiędzy danymi kompilacji głównej opisującymi aktualną wersję istotnego dla bezpieczeństwa sprzętu komputerowego, oprogramowania i oprogramowania układowego oraz przechowywaną na terenie obiektu główną kopią danych dla aktualnej wersji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-10(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zarządzania konfiguracją systemu przez programistę; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plan zarządzania konfiguracją systemu przez programistę; dokumentacja dotycząca zabezpieczania zmian konfiguracji; zapisy dotyczące zarządzania konfiguracją; zapisy dotyczące kontroli zmian/aktualizacji wersji; zapisy dotyczące weryfikacji integralności między kopiami głównymi istotnego z punktu widzenia bezpieczeństwa sprzętu, oprogramowania i oprogramowania układowego (w tym projektów i kodu źródłowego); plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-10(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; programiści systemu]. |

| | | |
|---|---|---|
| **SA-10(05)** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA \| INTEGRALNOŚĆ MAPOWANIA KONTROLI WERSJI** | |
| | **SA-10(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania procesu zarządzania konfiguracją przez programistę; mechanizmy wspierające lub wdrażające monitorowanie procesu zarządzania konfiguracją przez programistę]. |

| | | |
|---|---|---|
| **SA-10(06)** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA \| ZAUFANA DYSTRYBUCJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-10(06)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się realizacji procedur zapewniających, że istotne z punktu widzenia bezpieczeństwa aktualizacje sprzętu, oprogramowania i oprogramowania układowego są rozpowszechniane w strukturach organizacji w identycznej formie jak w ich wzorcach. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-10(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemów i usług; procedury dotyczące zarządzania konfiguracją systemu przez programistę; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plan zarządzania konfiguracją systemu przez programistę; dokumentacja dotycząca zabezpieczania zmian konfiguracji; zapisy dotyczące zarządzania konfiguracją; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-10(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; programiści systemu]. |

| | | |
|---|---|---|
| **SA-10(06)** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA \| ZAUFANA DYSTRYBUCJA** | |
| | **SA-10(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania procesu zarządzania konfiguracją przez programistę; mechanizmy wspierające lub wdrażające monitorowanie procesu zarządzania konfiguracją przez programistę]. |

| | | |
|---|---|---|
| **SA-10(07)** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA \| PERSONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-10(07)_ODP[01]** | ***określono przedstawicieli ds. bezpieczeństwa, którzy mają być włączeni w proces zarządzania i zabezpieczania zmiany konfiguracji;*** |
| | **SA-10(07)_ODP[02]** | ***określono przedstawicieli ds. prywatności, którzy mają być włączeni w proces zarządzania i zabezpieczania zmiany konfiguracji;*** |
| | **SA-10(07)_ODP[03]** | ***określono procesy zarządzania zmianami i zabezpieczania konfiguracji, w które muszą być zaangażowani przedstawiciele ds. bezpieczeństwa;*** |
| | **SA-10(07)_ODP[04]** | ***określono procesy zarządzania zmianami i zabezpieczania konfiguracji, w które muszą być zaangażowani przedstawiciele ds. prywatności;*** |
| | **SA-10(07)[01]** | ***<urzędnicy ds. bezpieczeństwa SA-10(07)_ODP[01]>*** muszą być zaangażowani w<br>***<procesy zarządzania zmianami i zabezpieczania konfiguracji SA-10(07)_ODP[03]>***; |
| | **SA-10(07)[02]** | ***<urzędnicy ds. prywatności SA-10(07)_ODP[02]>*** muszą być zaangażowani w<br>***<procesy zarządzania zmianami i zabezpieczania konfiguracji SA-10(07)_ODP[04]>***. |

| | | |
|---|---|---|
| **SA-10(07)** | **ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA \| PERSONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-10(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; polityka zarządzania konfiguracją; plan zarządzania konfiguracją; dokumentacja przetargowa wymagająca przedstawicieli ds. bezpieczeństwa i prywatności; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plan zarządzania konfiguracją systemu przez programistę; dokumentacja dotycząca zabezpieczania zmian konfiguracji; zapisy dotyczące zarządzania konfiguracją; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-10(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; programiści systemu]. |

| | | |
|---|---|---|
| **SA-11** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-11_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {jednostkowe; integracyjne; systemowe; regresyjne}*** |
| | **SA-11_ODP[02]** | ***określono częstotliwość przeprowadzania testowania/oceny <WYBRANA WARTOŚĆ PARAMETRU SA-11_ODP[01]>;*** |
| | **SA-11_ODP[03]** | ***określono głębokość i zakres testowania/oceny <WYBRANA WARTOŚĆ PARAMETRU SA-11_ODP[01]>;*** |

| SA-11 | TESTOWANIE I OCENA PRZEZ DEWELOPERA | |
|---|---|---|
| | **SA-11a.[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby na wszystkich etapach cyklu życia po zaprojektowaniu systemu opracowywał plan dla bieżących ocen bezpieczeństwa; |
| | **SA-11a.[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby na wszystkich etapach cyklu życia po zaprojektowaniu systemu wdrażał plan dla bieżących ocen bezpieczeństwa; |
| | **SA-11a.[03]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby na wszystkich etapach cyklu życia po zaprojektowaniu systemu opracowywał plan dla bieżących ocen prywatności; |
| | **SA-11a.[04]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby na wszystkich etapach cyklu życia po zaprojektowaniu systemu wdrażał plan dla bieżących ocen prywatności; |
| | **SA-11b.** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby na wszystkich etapach cyklu życia po zaprojektowaniu systemu wykonywał testy/oceny<br>***<WYBRANA WARTOŚĆ PARAMETRU SA-11_ODP[01]>***<br>z ***<częstotliwością przeprowadzania SA-11_ODP[02]>***<br>**oraz** z zastosowaniem ***<głębokości i zakresu SA-11_ODP[03]>*****;** |
| | **SA-11c.[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby na wszystkich etapach cyklu życia po zaprojektowaniu systemu przedkładał dowody na zrealizowanie planu oceny; |
| | **SA-11c.[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby na wszystkich etapach cyklu życia po zaprojektowaniu systemu przedkładał wyniki testów i oceny; |
| | **SA-11d.** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby na wszystkich etapach cyklu życia po zaprojektowaniu systemu stosował możliwy do zweryfikowania proces usuwania luk w zabezpieczeniach; |

| | | |
|---|---|---|
| **SA-11** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA** | |
| | **SA-11e.** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby na wszystkich etapach cyklu życia po zaprojektowaniu systemu usuwał luki w zabezpieczeniach zidentyfikowane podczas testów i oceny; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-11-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące testów bezpieczeństwa i prywatności przeprowadzanych przez programistów systemu; procedury dotyczące usuwania luk w zabezpieczeniach; dokumentacja przetargowa; dokumentacja dotycząca nabycia; umowy o poziomie usług; umowy dotyczące nabycia systemu, komponentu systemu lub usługi systemowej; architektura bezpieczeństwa i prywatności; dokumentacja projektowa systemu; plany oceny bezpieczeństwa i prywatności systemu przez programistów; wyniki ocen bezpieczeństwa i prywatności systemu, komponentu systemu lub usługi systemowej przez programistów; dokumentacja dotycząca śledzenia luk w zakresie bezpieczeństwa i prywatności oraz środków zaradczych; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka w zakresie ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-11-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za proces testowania bezpieczeństwa i prywatności przez programistów; programiści systemu]. |

| | | |
|---|---|---|
| **SA-11** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA** | |
| | **SA-11-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania testów i ocen bezpieczeństwa przeprowadzanych przez programistów; mechanizmy wspierające lub wdrażające monitorowanie testów i ocen bezpieczeństwa oraz prywatności przeprowadzanych przez programistów]. |

| | | |
|---|---|---|
| **SA-11(01)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| STATYCZNA ANALIZA KODU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-11(01)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się stosowania narzędzi do analizy statycznej kodu w celu identyfikacji wspólnych luk w zabezpieczeniach; |
| | **SA-11(01)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się zastosowania narzędzi do statycznej analizy kodu w celu udokumentowania wyników analizy. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SA-11(01) | TESTOWANIE I OCENA PRZEZ DEWELOPERA \| STATYCZNA ANALIZA KODU | |
|---|---|---|
| | **SA-11(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące testowania bezpieczeństwa systemu przez programistów; procedury dotyczące usuwania luk w zabezpieczeniach; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; architektura bezpieczeństwa i prywatności; dokumentacja projektowa systemu; plany oceny bezpieczeństwa i prywatności przez programistów systemu; wyniki oceny bezpieczeństwa i prywatności systemu przez programistów; dokumentacja dotycząca śledzenia luk w zabezpieczeniach i ich usuwania; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-11(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za testowanie bezpieczeństwa i prywatności systemu przez programistów; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; programiści systemu]. |
| | **SA-11(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania testów i ocen bezpieczeństwa przeprowadzanych przez programistów; mechanizmy wspierające lub wdrażające monitorowanie testów i ocen bezpieczeństwa przeprowadzanych przez programistów; narzędzia do statycznej analizy kodu]. |

| | | |
|---|---|---|
| **SA-11(02)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| MODELOWANIE ZAGROŻEŃ I ANALIZA PODATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-11(02)_ODP[01]** | ***określono informacje dotyczące wpływu, środowiska działania, znanych lub zakładanych zagrożeń oraz dopuszczalnych poziomów ryzyka, które mają być wykorzystane jako informacje kontekstowe do modelowania zagrożeń i analiz podatności;*** |
| | **SA-11(02)_ODP[02]** | ***określono narzędzia i metody, które mają być stosowane do modelowania zagrożeń i analiz podatności;*** |
| | **SA-11(02)_ODP[03]** | ***określono zakres i głębokość wymaganego modelowania zagrożeń;*** |
| | **SA-11(02)_ODP[04]** | ***określono zakres i głębokość wymaganych analiz podatności;*** |
| | **SA-11(02)_ODP[05]** | ***określono dowody spełniające wyznaczone kryteria akceptacji na potrzeby modelowania zagrożeń;*** |
| | **SA-11(02)_ODP[06]** | ***Określono dowody spełniające wyznaczone kryteria akceptacji na potrzeby analiz podatności;*** |
| | **SA-11(02)(a)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia modelowania zagrożeń podczas opracowywania systemu, komponentu lub usługi, która wykorzystuje ***<informacje SA-11(02)_ODP[01]>***; |
| | **SA-11(02)(a)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia analiz podatności podczas opracowywania systemu, komponentu lub usługi, która wykorzystuje ***<informacje SA-11(02)_ODP[01]>***; |

| | | |
|---|---|---|
| **SA-11(02)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| MODELOWANIE ZAGROŻEŃ I ANALIZA PODATNOŚCI** | |
| | **SA-11(02)(a)[03]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia modelowania zagrożeń podczas kolejnych testów i ocen systemu, komponentu lub usługi, która wykorzystuje ***<informacje SA-11(02)_ODP[01]>***; |
| | **SA-11(02)(a)[04]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia analizy podatności podczas kolejnych testów i ocen systemu, komponentu lub usługi, która wykorzystuje ***<informacje SA-11(02)_ODP[01]>***; |
| | **SA-11(02)(b)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia modelowania zagrożeń podczas opracowywania systemu, komponentu lub usługi, która wykorzystuje ***<narzędzia i metody SA-11(02)_ODP[02]>***; |
| | **SA-11(02)(b)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia modelowania zagrożeń podczas kolejnych testów i ocen systemu, komponentu lub usługi, która wykorzystuje ***<narzędzia i metody SA-11(02)_ODP[02]>***; |
| | **SA-11(02)(b)[03]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia analiz podatności podczas opracowywania systemu, komponentu lub usługi, która wykorzystuje ***<narzędzia i metody SA-11(02)_ODP[02]>;*** |
| | **SA-11(02)(b)[04]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia analiz podatności podczas kolejnych testów i ocen systemu, komponentu lub usługi, która wykorzystuje ***<narzędzia i metody SA-11(02)_ODP[02]>***; |
| | **SA-11(02)(c)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia modelowania zagrożeń z zastosowaniem ***<zakresu i głębokości SA-11(02)_ODP[03]>*** podczas opracowywania systemu, komponentu lub usługi; |

| | | |
|---|---|---|
| **SA-11(02)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| MODELOWANIE ZAGROŻEŃ I ANALIZA PODATNOŚCI** | |
| | **SA-11(02)(c)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia analiz podatności z zastosowaniem***<zakresu i głębokości SA-11(02)_ODP[04]>*** podczas kolejnych testów i ocen systemu, komponentu lub usługi; |
| | **SA-11(02)(d)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia modelowania zagrożeń podczas opracowywania systemu, komponentu lub usługi, w wyniku którego powstają dowody spełniające ***<kryteria akceptacji SA-11(02)_ODP[05]>***; |
| | **SA-11(02)(d)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia modelowania zagrożeń podczas kolejnych testów i ocen systemu, komponentu lub usługi, w wyniku którego powstają dowody spełniające ***<kryteria akceptacji SA-11(02)_ODP[05]>***; |
| | **SA-11(02)(d)[03]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia analiz podatności podczas opracowywania systemu, komponentu lub usługi, w wyniku których powstają dowody spełniające ***<SA-11(02)_ODP[06] kryteria akceptacji***>; |
| | **SA-11(02)(d)[04]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia analiz podatności podczas kolejnych testów i ocen systemu, komponentu lub usługi, w wyniku których powstają dowody spełniające ***<SA-11(02)_ODP[06] kryteria akceptacji***>. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-11(02)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| MODELOWANIE ZAGROŻEŃ I ANALIZA PODATNOŚCI** | |
| | **SA-11(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemów i usług; procedury dotyczące testowania bezpieczeństwa systemu przez programistów; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plany testowania bezpieczeństwa systemu przez programistów; zapisy wyników testowania bezpieczeństwa systemu, komponentu systemu lub usługi systemowej przez programistów; wyniki skanowania podatności; raporty z oceny ryzyka systemu; raporty z analizy zagrożeń i podatności; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-11(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za testowanie bezpieczeństwa systemu przez programistów; programiści systemów; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem w łańcuchu dostaw]. |
| | **SA-11(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania testów i ocen bezpieczeństwa przeprowadzanych przez programistów; mechanizmy wspierające lub wdrażające monitorowanie testów i oceny przeprowadzanych przez programistów]. |

| | | |
|---|---|---|
| **SA-11(03)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| NIEZALEŻNA WERYFIKACJA PLANÓW OCENY/EWIDENCJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-11(03)_ODP** | ***określono kryteria niezależności, które musi spełniać niezależny organ;*** |

| | | |
|---|---|---|
| **SA-11(03)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| NIEZALEŻNA WERYFIKACJA PLANÓW OCENY/EWIDENCJA** | |
| | **SA-11(03)(a)[01]** | od niezależnego organu wymaga się spełnienia ***<kryteriów niezależności SA-11(03)_ODP>*** w celu weryfikacji poprawności wdrażania planu oceny bezpieczeństwa przez twórcę systemu oraz dowodów uzyskanych podczas testów i ocen; |
| | **SA-11(03)(a)[02]** | od niezależnego organu wymaga się spełnienia ***<kryteriów niezależności SA-11(03)_ODP>*** w celu weryfikacji poprawności wdrażania planu ochrony prywatności przez twórcę systemu oraz dowodów uzyskanych podczas testów i ocen; |
| | **SA-11(03)(b)** | niezależnemu organowi zapewniono informacje wystarczające do zakończenia procesu weryfikacji lub przyznano mu uprawnienia do uzyskania takich informacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-11(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące testowania bezpieczeństwa systemu przez programistów; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; sprawozdania z niezależnej weryfikacji i walidacji; plany oceny bezpieczeństwa i prywatności; wyniki oceny bezpieczeństwa i prywatności systemu, komponentu systemu lub usługi systemowej; plan bezpieczeństwa systemu; plan ochrony prywatności; plan programu ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-11(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za testowanie bezpieczeństwa systemu przez programistów; programiści systemu; niezależny organ weryfikacyjny]. |

| | | |
|---|---|---|
| **SA-11(03)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| NIEZALEŻNA WERYFIKACJA PLANÓW OCENY/EWIDENCJA** | |
| | **SA-11(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania testów i ocen bezpieczeństwa przeprowadzanych przez programistów; mechanizmy wspierające lub wdrażające monitorowanie testów i oceny przeprowadzanych przez programistów]. |

| | | |
|---|---|---|
| **SA-11(04)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| MANUALNY PRZEGLĄD KODU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-11(04)_ODP[01]** | ***określono kod wymagający ręcznego przeglądu;*** |
| | **SA-11(04)_ODP[02]** | ***określono procesy, procedury lub techniki stosowane do ręcznego przeglądu kodu;*** |
| | **SA-11(04)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia ręcznego przeglądu ***<konkretnego kodu SA-11(04)_ODP[01]>*** z wykorzystaniem<br>***<procesów, procedur lub technik SA-11(04)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-11(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące testowania bezpieczeństwa systemu przez programistów; procesy, procedury lub techniki przeprowadzania ręcznych przeglądów kodu; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej;<br>plany testowania bezpieczeństwa systemu i oceny przez programistów; lista kodów wymagających ręcznych przeglądów; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| SA-11(04) | TESTOWANIE I OCENA PRZEZ DEWELOPERA \| MANUALNY PRZEGLĄD KODU | |
|---|---|---|
| | **SA-11(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za testowanie bezpieczeństwa systemu przez programistów; programiści systemu; niezależny organ weryfikacyjny]. |
| | **SA-11(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania testów i ocen bezpieczeństwa przeprowadzanych przez programistów; mechanizmy wspierające lub wdrażające monitorowanie testów i oceny bezpieczeństwa przeprowadzane przez programistów]. |

| SA-11(05) | TESTOWANIE I OCENA PRZEZ DEWELOPERA \| TESTOWANIE PENETRACYJNE | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-11(05)_ODP[01]** | ***określono zakres testów penetracyjnych;*** |
| | **SA-11(05)_ODP[02]** | ***określono głębokość testów penetracyjnych;*** |
| | **SA-11(05)_ODP[03]** | ***określono ograniczenia dla testów penetracyjnych;*** |
| | **SA-11(05)(a)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzania testów penetracyjnych o następującym poziomie rygoru:***<zakres SA-11(05)_ODP[01]>***; |
| | **SA-11(05)(a)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzania testów penetracyjnych o następującym poziomie rygoru:***<głębokość SA-11(05)_ODP[02]>***; |

| | | |
|---|---|---|
| **SA-11(05)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| TESTOWANIE PENETRACYJNE** | |
| | **SA-11(05)(b)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzania testów penetracyjnych o następującym poziomie rygoru:***<ograniczenia SA-11(05)_ODP[03]>*.** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-11(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące testowania bezpieczeństwa systemu przez programistów; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plany testów penetracyjnych i ocen przeprowadzanych przez programistów; wyniki testów penetracyjnych i ocen przeprowadzanych przez programistów; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka przetwarzania danych identyfikacyjnych; inne istotne dokumenty lub zapisy]. |
| | **SA-11(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za testowanie bezpieczeństwa systemu przez programistów; programiści systemu; niezależny organ weryfikacyjny]. |
| | **SA-11(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania ocen bezpieczeństwa i prywatności przeprowadzanych przez programistów; mechanizmy wspierające lub wdrażające monitorowanie ocen bezpieczeństwa i prywatności przeprowadzanych przez programistów]. |

| | | |
|---|---|---|
| **SA-11(06)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| PRZEGLĄD PŁASZCZYZNY ATAKU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-11(06)** | twórca systemu, komponentu systemu lub usługi systemowej jest zobowiązany do wykonania przeglądów płaszczyzny ataku. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-11(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące testowania bezpieczeństwa systemu przez programistów; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plany testów i oceny bezpieczeństwa przeprowadzane przez programistów; wyniki testów i ocen bezpieczeństwa przeprowadzanych przez programistów; zapisy przeglądów płaszczyzn ataku; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-11(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za testowanie bezpieczeństwa przez programistów; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; programiści systemu]. |
| | **SA-11(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania testów i ocen bezpieczeństwa przeprowadzanych przez programistów; mechanizmy wspierające lub wdrażające monitorowanie testów i oceny przeprowadzanych przez programistów]. |

| | | |
|---|---|---|
| **SA-11(07)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| WERYFIKACJA ZAKRESU TESTU/OCENA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-11(07)_ODP[01]** | ***określono zakres badania i oceny wymaganych zabezpieczeń;*** |
| | **SA-11(07)_ODP[02]** | ***określono głębokość badania i oceny wymaganych zabezpieczeń;*** |
| | **SA-11(07)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się sprawdzenia czy zakres badań i oceny obejmuje wszystkie wymagane zabezpieczenia na następującym poziomie rygoru: ***<zakres SA-11(07)_ODP[01]>***; |
| | **SA-11(07)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się sprawdzenia czy zakres badań i oceny obejmuje wszystkie wymagane zabezpieczenia na następującym poziomie rygoru: ***<głębokość SA-11(07)_ODP[02]>*.** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-11(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące testowania bezpieczeństwa systemu przez programistów; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plany testów i ocen bezpieczeństwa przeprowadzanych przez programistów; wyniki testów i ocen bezpieczeństwa przeprowadzanych przez programistów; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-11(07)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| WERYFIKACJA ZAKRESU TESTU/OCENA** | |
| | **SA-11(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za testowanie bezpieczeństwa systemu przez programistów; programiści systemu; niezależny organ weryfikacyjny]. |
| | **SA-11(07)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania testów i ocen bezpieczeństwa przeprowadzanych przez programistów; mechanizmy wspierające lub wdrażające monitorowanie testów i oceny przeprowadzanych przez programistów]. |

| | | |
|---|---|---|
| **SA-11(08)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| DYNAMICZNA ANALIZA KODU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-11(08)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się stosowania narzędzi do dynamicznej analizy kodu w celu identyfikacji typowych luk w zabezpieczeniach; |
| | **SA-11(08)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się udokumentowania wyników analizy. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-11(08)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| DYNAMICZNA ANALIZA KODU** | |
| | **SA-11(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące testowania bezpieczeństwa systemu przez programistów; procedury dotyczące usuwania luk w zabezpieczeniach; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plany testów i oceny bezpieczeństwa przeprowadzane przez programistów; wyniki testów i ocen bezpieczeństwa; raporty dotyczące śledzenia i usuwania luk w zabezpieczeniach; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-11(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za testowanie bezpieczeństwa przez programistów; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; programiści systemu]. |
| | **SA-11(08)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania testów i ocen bezpieczeństwa przeprowadzanych przez programistów; mechanizmy wspierające lub wdrażające monitorowanie testów i oceny przeprowadzanych przez programistów]. |

| | | |
|---|---|---|
| **SA-11(09)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| INTERAKTYWNE TESTOWANIE BEZPIECZEŃSTWA APLIKACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-11(09)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się stosowania interaktywnych narzędzi do testowania bezpieczeństwa aplikacji w celu identyfikacji luk w zabezpieczeniach; |

| | | |
|---|---|---|
| **SA-11(09)** | **TESTOWANIE I OCENA PRZEZ DEWELOPERA \| INTERAKTYWNE TESTOWANIE BEZPIECZEŃSTWA APLIKACJI** | |
| | **SA-11(09)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się dokumentowania wyników procesu wykrywania luk w zabezpieczeniach. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-11(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemów i usług; procedury dotyczące testowania bezpieczeństwa systemu przez programistów; procedury dotyczące testowania bezpieczeństwa aplikacji interaktywnych; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plany testów i ocen bezpieczeństwa przeprowadzanych przez programistów; wyniki testów i ocen bezpieczeństwa; raporty dotyczące śledzenia i usuwania luk w zabezpieczeniach; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-11(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za testowanie bezpieczeństwa przez programistów; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją; programiści systemu]. |
| | **SA-11(09)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące interaktywnego badania bezpieczeństwa aplikacji; mechanizmy wspierające lub wdrażające interaktywne badanie bezpieczeństwa aplikacji]. |

| | |
|---|---|
| **SA-12** | **BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW** |
| | [WYCOFANE: Włączone do kategorii SR]. |

| SA-12(01) | BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| STRATEGIE ZAKUPÓW, NARZĘDZIA, METODY |
|---|---|
| | [WYCOFANE: Włączone do SR-05]. |

| SA-12(02) | BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| PRZEGLĄD DOSTAWCÓW |
|---|---|
| | [WYCOFANE: Włączone do SR-06]. |

| SA-12(03) | BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| ZAUFANA WYSYŁKA I MAGAZYNOWANIE |
|---|---|
| | [WYCOFANE: Włączone do SR-03]. |

| SA-12(04) | BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| DYWERSYFIKACJA DOSTAWCÓW |
|---|---|
| | [WYCOFANE: Włączone do SR-03(01)]. |

| SA-12(05) | BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| OGRANICZENIE SZKODY |
|---|---|
| | [WYCOFANE: Włączone do SR-03(02)]. |

| SA-12(06) | BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| MINIMALIZACJA CZASU ZAMÓWIENIA |
|---|---|
| | [WYCOFANE: Włączone do SR-05(01)]. |

| | |
|---|---|
| **SA-12(07)** | **BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| OCENY PRZED WYBOREM/ODBIOREM/AKTUALIZACJĄ** |
| | [WYCOFANE: Włączone do SR-05(02)]. |

| | |
|---|---|
| **SA-12(08)** | **BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| POZYSKIWANIE INFORMACJI Z WSZYSTKICH DOSTĘPNYCH ŹRÓDEŁ** |
| | [WYCOFANE: Włączone do RA-03(02)]. |

| | |
|---|---|
| **SA-12(09)** | **BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| BEZPIECZEŃSTWO OPERACYJNE** |
| | [WYCOFANE: Włączone do SR-07]. |

| | |
|---|---|
| **SA-12(10)** | **BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| OCENA ORYGINALNOŚCI I NIEZMIENNOŚCI** |
| | [WYCOFANE: Włączone do SR-04(03)]. |

| | |
|---|---|
| **SA-12(11)** | **BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| TESTOWANIE PENETRACYJNE/ANALIZA ELEMENTÓW, PROCESÓW I WYKONAWCÓW** |
| | [WYCOFANE: Włączone do SR-06(01)]. |

| | |
|---|---|
| **SA-12(12)** | **BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| UMOWY MIĘDZYORGANIZACYJNE** |
| | [WYCOFANE: Włączone do SR-08]. |

| | |
|---|---|
| **SA-12(13)** | **BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| KOMPONENTY KRYTYCZNE SYSTEMU INFORMATYCZNEGO** |
| | [Wycofane: Włączone do MA-06, RA-09]. |

| | |
|---|---|
| **SA-12(14)** | **BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| IDENTYFIKACJA I ŚLEDZENIE** |
| | [WYCOFANE: Włączone do SR-04(01), SR-04(02)]. |

| | |
|---|---|
| **SA-12(15)** | **BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW \| MECHANIZMY ELIMINOWANIA SŁABYCH STRON LUB WAD** |
| | [WYCOFANE: Włączone do SR-03]. |

| | |
|---|---|
| **SA-13** | **WIARYGODNOŚĆ** |
| | [WYCOFANE: Włączone do SA-08]. |

| | |
|---|---|
| **SA-14** | **ANALIZA KRYTYCZNOŚCI** |
| | [WYCOFANE: Włączone do RA-09]. |

| | |
|---|---|
| **SA-14(01)** | **ANALIZA KRYTYCZNOŚCI \| KRYTYCZNE KOMPONENTY POZBAWIONE ALTERNATYWNEGO ŹRÓDŁA ZAOPATRZENIA** |
| | [WYCOFANE: Włączone do SA-20]. |

| | | |
|---|---|---|
| **SA-15** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-15_ODP[01]** | ***określono częstotliwość, z jaką należy dokonywać przeglądu procesu rozwoju, standardów, narzędzi, opcji narzędziowych i konfiguracji narzędzi;*** |
| | **SA-15_ODP[02]** | ***określono wymagania dotyczące bezpieczeństwa, które mają być spełnione przez proces, standardy, narzędzia, opcje narzędziowe i konfiguracje narzędzi;*** |
| | **SA-15_ODP[03]** | ***określono wymagania dotyczące prywatności, które mają być spełnione przez proces, standardy, narzędzia, opcje narzędziowe i konfiguracje narzędzi;*** |
| | **SA-15a.01[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przestrzegania udokumentowanego procesu rozwoju, który wyraźnie uwzględnia wymagania dotyczące bezpieczeństwa; |
| | **SA-15a.01[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przestrzegania udokumentowanego procesu rozwoju, który wyraźnie uwzględnia wymagania dotyczące prywatności; |
| | **SA-15a.02[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykorzystania udokumentowanego procesu rozwoju, określającego standardy stosowane w tymże procesie; |
| | **SA-15a.02[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykorzystania udokumentowanego procesu rozwoju, określającego narzędzia stosowane w tymże procesie; |
| | **SA-15a.03[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykorzystania udokumentowanego procesu rozwoju, określającego konkretne narzędzie używane w tymże procesie; |

| | | |
|---|---|---|
| **SA-15** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA** | |
| | **SA-15a.03[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykorzystania udokumentowanego procesu rozwoju, w ramach którego rejestruje się konkretne konfiguracje narzędzia używanego w tymże procesie; |
| | **SA-15a.04** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykorzystania udokumentowanego procesu rozwoju, który rejestruje zmiany oraz zapewnia zarządzanie nimi i ich integralność w procesie rozwoju lub narzędziach użytych w ramach tegoż procesu; |
| | **SA-15b.[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykorzystania udokumentowanego procesu rozwoju, w którym proces rozwoju, standardy, narzędzia, opcje narzędziowe i konfiguracje narzędzi są poddawane przeglądowi z ***<częstotliwością SA-15_ODP[01]>*** w celu ustalenia, czy wybrany i zastosowany proces, standardy, narzędzia, opcje narzędziowe i konfiguracje narzędzi spełniają ***<wymagania dotyczące bezpieczeństwa SA-15_ODP[02]>***; |
| | **SA-15b.[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykorzystania udokumentowanego procesu rozwoju, w którym proces rozwoju, standardy, narzędzia, opcje narzędziowe i konfiguracje narzędzi są poddawane przeglądowi z ***<częstotliwością SA-15_ODP[01]>*** w celu ustalenia, czy wspomniany proces, standardy, narzędzia, opcje narzędziowe i konfiguracje narzędzi spełniają ***<wymagania dotyczące prywatności SA-15_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-15** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA** | |
| | **SA-15-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące procesu rozwoju, standardów i narzędzi; procedury dotyczące integracji wymagań w zakresie bezpieczeństwa i prywatności podczas procesu rozwoju; dokumentacja przetargowa; dokumentacja nabycia; dokumentacja inwentaryzacji komponentów krytycznych; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja programisty systemu zawierająca wykaz opcji/konfiguracji narzędzi; polityka zarządzania konfiguracją; dokumentacja zarządzania konfiguracją; dokumentacja przeglądów procesu rozwoju z wykorzystaniem modeli dojrzałości; dokumentacja dotycząca zabezpieczania zmian konfiguracji; dokumentacja dotycząca zabezpieczania konfiguracji; udokumentowane przeglądy procesu rozwoju, standardów, narzędzi oraz opcji/konfiguracji narzędzi; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-15-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |

| | | |
|---|---|---|
| **SA-15(01)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| METRYKI JAKOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-15(01)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{<częstotliwość SA-15(01)_ODP[02]>; <przegląd programu SA-15(01)_ODP[03]>; po dostarczeniu};*** |

| | | |
|---|---|---|
| **SA-15(01)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| METRYKI JAKOŚCI** | |
| | **SA-15(01)_ODP[02]** | ***określono częstotliwość dostarczania dowodów na spełnienie kryteriów jakości (jeśli wybrano);*** |
| | **SA-15(01)_ODP[03]** | ***określono kamienie milowe dla przeglądu programu (jeśli wybrano);*** |
| | **SA-15(01)(a)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się dokumentowania kryteriów jakości na początku procesu rozwoju; |
| | **SA-15(01)(b)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się dokumentowania dowodów na spełnienie kryteriów jakości ***<WYBRANA WARTOŚĆ PARAMETRU SA-15(01)_ODP[01]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-15(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, standardów i narzędzi; procedury dotyczące integracji wymogów bezpieczeństwa z procesem nabywania; dokumentacja przetargowa; dokumentacja dotycząca nabywania; umowy o poziomie usług;<br>umowy nabycia systemu, komponentu systemu lub usługi systemowej; wykaz kryteriów jakości; dokumentacja potwierdzająca spełnienie kryteriów jakości; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-15(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |

| | | |
|---|---|---|
| **SA-15(02)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| NARZĘDZIA DO MONITOROWANIA BEZPIECZEŃSTWA I PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-15(02)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wyboru i stosowania narzędzi do monitorowania bezpieczeństwa w procesie rozwoju; |
| | **SA-15(02)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wyboru i stosowania narzędzi do monitorowania ochrony prywatności w procesie rozwoju. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-15(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące procesu rozwoju, standardów i narzędzi; procedury dotyczące integracji wymogów w zakresie bezpieczeństwa i prywatności z procesem nabywania; dokumentacja przetargowa; dokumentacja dotycząca nabywania; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja wyboru narzędzi śledzenia bezpieczeństwa i prywatności; dowody na stosowanie narzędzi monitorowania bezpieczeństwa i ochrony prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-15(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za prywatność]. |

| | | |
|---|---|---|
| **SA-15(03)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| ANALIZA KRYTYCZNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-15(03)_ODP[01]** | ***określono punkty decyzyjne w cyklu życia systemu;*** |
| | **SA-15(03)_ODP[02]** | ***określono zakres analizy krytyczności;*** |
| | **SA-15(03)_ODP[03]** | ***określono głębokość analizy krytyczności;*** |
| | **SA-15(03)(a)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzania analiz krytyczności w ***<punktach decyzyjnych SA-15(03)_ODP[01]> w*** cyklu życia systemu; |
| | **SA-15(03)(b)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzania analiz krytyczności o następującym poziomie rygoru:***<zakres SA-15(03)_ODP[02]>***; |
| | **SA-15(03)(b)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzania analiz krytyczności o następującym poziomie rygoru:***<głębokość SA-15(03)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-15(03)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| ANALIZA KRYTYCZNOŚCI** | |
| | **SA-15(03)-Badanie** | [WYBÓR SPOŚRÓD: Plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemu i usług; procedury dotyczące procesu, standardów i narzędzi rozwoju; procedury dotyczące wymogów dla analizy krytyczności systemu, komponentu systemu lub usługi systemowej; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja analizy krytyczności; dokumentacja analizy wpływu na działalność; dokumentacja cyklu życia oprogramowania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-15(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za przeprowadzenie analizy krytyczności; programista systemu; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SA-15(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przeprowadzania analizy krytyczności; mechanizmy wspierające lub wdrażające analizę krytyczności]. |

| | |
|---|---|
| **SA-15(04)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| MODELOWANIE ZAGROŻEŃ/ANALIZA PODATNOŚCI** |
| | [WYCOFANE: Włączone do SA-11(02)]. |

| | | |
|---|---|---|
| **SA-15(05)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| OGRANICZANIE PŁASZCZYZNY ATAKU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-15(05)_ODP** | ***określono wartości progowe, do których mają być zredukowane płaszczyzny ataku;*** |
| | **SA-15(05)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się zredukowania płaszczyzn ataku aż do osiągnięcia ***<wartości progowych SA-15(05)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-15(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące procesu rozwoju, standardów i narzędzi; procedury dotyczące redukcji płaszczyzn ataku; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu lub usługi systemowej; dokumentacja projektowa systemu; diagram sieci; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja ustanawiająca/wzmacniająca określone przez organizację wartości progowe, do których ma być zmniejszona płaszczyzna ataku; lista zastrzeżonych portów, protokołów, funkcji i usług; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-15(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za wartości progowe, do których ma być zredukowana płaszczyzna ataku; programista systemu]. |
| | **SA-15(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne definiujące wartości progowe, do których ma być zredukowana płaszczyzna ataku]. |

| | | |
|---|---|---|
| **SA-15(06)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| CIĄGŁE DOSKONALENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-15(06)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wdrożenia jasno sprecyzowanego mechanizmu ciągłego doskonalenia procesu rozwoju. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-15(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące procesu rozwoju, standardów i narzędzi; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; cele jakościowe i kryteria służące poprawie procesu rozwoju systemu; oceny bezpieczeństwa; przeglądy procesu rozwoju systemu pod kątem kontroli jakości; plany działania i kamienie milowe służące poprawie procesu rozwoju systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-15(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu]. |

| | | |
|---|---|---|
| **SA-15(07)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| AUTOMATYCZNA ANALIZA PODATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-15(07)_ODP[01]** | ***określono częstotliwość, z jaką należy przeprowadzać analizę podatności;*** |
| | **SA-15(07)_ODP[02]** | ***określono narzędzia służące do przeprowadzania automatycznej analizy podatności;*** |
| | **SA-15(07)_ODP[03]** | ***określono personel lub role, wśród których mają być rozpowszechniane dane wyjściowe z narzędzi oraz wyniki analizy;*** |
| | **SA-15(07)(a)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzania automatycznej analizy podatności z ***<częstotliwością SA-15(07)_ODP[01]>*** przy użyciu ***<narzędzi SA-15(07)_ODP[02]>***; |
| | **SA-15(07)(b)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się określania potencjału wykorzystania zidentyfikowanych podatności z ***<częstotliwością SA-15(07)_ODP[01]>***; |
| | **SA-15(07)(c)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się określenia potencjalnych środków łagodzenia ryzyka związanego z wykrytymi podatnościami z ***<częstotliwością SA-15(07)_ODP[01]>***; |
| | **SA-15(07)(d)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się dostarczania danych wyjściowych z narzędzi i wyników analizy z ***<częstotliwością SA-15(07)_ODP[01]> do <personelu lub ról SA-15(07)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-15(07)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| AUTOMATYCZNA ANALIZA PODATNOŚCI** | |
| | **SA-15(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące procesu rozwoju, standardów i narzędzi; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; narzędzia do analizy podatności i związana z nimi dokumentacja; raporty z oceny ryzyka; wyniki analizy podatności; raporty dotyczące minimalizacji podatności; dokumentacja dotycząca strategii ograniczania ryzyka; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-15(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny przeprowadzający automatyczną analizę podatności systemu]. |
| | **SA-15(07)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące analizy podatności systemów, komponentów systemu lub usług systemowych w fazie rozwoju; mechanizmy wspierające lub wdrażające analizę podatności systemów, komponentów systemu lub usług systemowych w fazie rozwoju]. |

| | | |
|---|---|---|
| **SA-15(08)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| PONOWNIE UŻYCIE INFORMACJI O ZAGROŻENIACH I PODATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-15(08)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby w bieżącym procesie rozwoju wykorzystywał modelowanie zagrożeń z podobnych systemów, komponentów lub usług; |

| | | |
|---|---|---|
| **SA-15(08)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| PONOWNIE UŻYCIE INFORMACJI O ZAGROŻENIACH I PODATNOŚCI** | |
| | **SA-15(08)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, aby w bieżącym procesie rozwoju wykorzystywał analizy podatności z podobnych systemów, komponentów lub usług. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-15(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemów i usług; plan zarządzania ryzykiem łańcucha dostaw; procedury dotyczące procesu rozwoju, standardów i narzędzi; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; modelowanie zagrożeń i analizy podatności z podobnych systemów,<br>komponentów systemu komponentów systemu lub usług systemowych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-15(08)-Wywiad** | [WYBÓR SPOŚRÓD: personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |

| | | |
|---|---|---|
| **SA-15(09)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| KREATYWNE WYKORZYSTANIE DANYCH** | |
| | [WYCOFANE: Włączone do SA-03(02)]. | |

| | | |
|---|---|---|
| **SA-15(10)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| PLAN REAGOWANIA NA INCYDENTY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-15(10)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się dostarczenia planu reagowania na incydenty; |
| | **SA-15(10)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wdrożenia planu reagowania na incydenty; |
| | **SA-15(10)[03]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przetestowania planu reagowania na incydenty; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-15(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące reagowania na incydenty, standardy i narzędzia; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentów systemu lub usług; dokumentacja przetargowa; umowy o poziomie usług; plan reagowania na incydenty przez programistę; plan bezpieczeństwa systemu; plan ochrony prywatności; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-15(10)-Wywiad** | [WYBÓR SPOŚRÓD: personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |

| | | |
|---|---|---|
| **SA-15(11)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| ARCHIWIZACJA SYSTEMU LUB KOMPONENTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-15(11)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się dokonania archiwizacji wydanego/dostarczonego systemu lub komponentu wraz z odpowiednimi dowodami wskazującymi na przeprowadzenie końcowego przeglądu bezpieczeństwa i ochrony prywatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-15(11)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące procesu rozwoju, standardów i narzędzi; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu lub komponentu systemu; dowody na przeprowadzenie archiwizacji systemu lub komponentu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-15(11)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za prywatność]. |

| | | |
|---|---|---|
| **SA-15(12)** | **PROCES ROZWOJU, STANDARDY I NARZĘDZIA \| MINIMALIZACJA INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSOBY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-15(12)** | twórca systemu lub komponentu systemu jest zobowiązany do minimalizacji wykorzystania danych identyfikacyjnych w środowiskach rozwojowych i testowych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-15(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące procesu rozwoju; procedury dotyczące minimalizacji używania danych identyfikacyjnych podczas testów, szkoleń i badań; polityka przetwarzania danych identyfikacyjnych; procedury dotyczące uprawnień do przeprowadzania testów z wykorzystaniem danych identyfikacyjnych; standardy i narzędzia; dokumentacja przetargowa; umowy o poziomie usług;<br>umowy dotyczące nabycia systemu lub usług; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-15(12)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programista systemu]. |
| | **SA-15(12)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne minimalizacji stosowania danych identyfikacyjnych w środowiskach rozwojowych i testowych; mechanizmy ułatwiające minimalizację stosowania danych identyfikacyjnych w środowiskach rozwojowych i testowych]. |

| | | |
|---|---|---|
| **SA-16** | **SZKOLENIA PROWADZONE PRZEZ DEWELOPERA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-16_ODP** | ***określono wymagane szkolenie w zakresie prawidłowego użytkowania i obsługi wdrażanych funkcji bezpieczeństwa i prywatności, zabezpieczeń lub mechanizmów dostarczonych przez twórcę systemu, komponentu systemu lub usługi systemowej;*** |
| | **SA-16** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przeprowadzenia ***<szkolenia SA-16_ODP>*** w zakresie prawidłowego wykorzystania i działania wdrażanych funkcji, zabezpieczeń lub mechanizmów bezpieczeństwa i prywatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-16-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące szkoleń zapewnianych przez dewelopera; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; organizacyjna polityka szkoleń w zakresie bezpieczeństwa i ochrony prywatności; materiały szkoleniowe zapewniane przez programistę; dokumentacja szkoleniowa; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-16-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programista systemu; zewnętrzni lub wewnętrzni programiści odpowiedzialni za szkolenie w zakresie systemu, komponentu systemu lub usługi systemu informatycznego]. |

| | | |
|---|---|---|
| **SA-17** | **ARCHITEKTURA ORAZ PROJEKT BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI DEWELOPERA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-17(a)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się sporządzenia specyfikacji projektu i architektury bezpieczeństwa, które są zgodne z architekturą bezpieczeństwa organizacji, stanowiącą integralną część jej architektury korporacyjnej; |
| | **SA-17(a)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się sporządzenia specyfikacji projektu i architektury prywatności, które są zgodne z architekturą prywatności organizacji, stanowiącą integralną część jej architektury korporacyjnej; |
| | **SA-17(b)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się sporządzenia specyfikacji projektu i architektury bezpieczeństwa, które dokładnie i wyczerpująco opisują wymagane funkcje bezpieczeństwa oraz podział zabezpieczeń pomiędzy komponentami fizycznymi i logicznymi; |
| | **SA-17(b)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się sporządzenia specyfikacji projektu i architektury bezpieczeństwa, które dokładnie i wyczerpująco opisują wymagane funkcje prywatności oraz podział zabezpieczeń pomiędzy komponentami fizycznymi i logicznymi; |
| | **SA-17(c)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się sporządzenia specyfikacji projektu i architektury bezpieczeństwa, które wyrażają, w jaki sposób<br>poszczególne funkcje, mechanizmy i usługi bezpieczeństwa współdziałają ze sobą w celu zapewnienia wymaganych zdolności w zakresie bezpieczeństwa oraz jednolitego podejścia do ochrony; |

| | | |
|---|---|---|
| **SA-17** | **ARCHITEKTURA ORAZ PROJEKT BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI DEWELOPERA** | |
| | **SA-17(c)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się sporządzenia specyfikacji projektu i architektury bezpieczeństwa, które wyrażają, w jaki sposób poszczególne funkcje, mechanizmy i usługi bezpieczeństwa współdziałają ze sobą w celu zapewnienia wymaganych zdolności w zakresie ochrony prywatności oraz jednolitego podejścia do ochrony. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-17-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; polityka w zakresie architektury korporacyjnej; dokumentacja architektury korporacyjnej; procedury dotyczące architektury bezpieczeństwa i ochrony prywatności oraz specyfikacje projektowe systemu przygotowane przez programistę; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu informatycznego i związana z nimi dokumentacja; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-17-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programista systemu]. |

| | | |
|---|---|---|
| **SA-17(01)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| FORMALNY MODEL POLITYKI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-17(01)_ODP[01]** | ***określono organizacyjną politykę bezpieczeństwa, która ma być egzekwowana;*** |
| | **SA-17(01)_ODP[02]** | ***określono organizacyjną politykę ochrony prywatności, która ma być egzekwowana;*** |
| | **SA-17(01)(a)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, jako integralną część procesu rozwoju, wytworzenia formalnego modelu polityki opisującego ***<organizacyjną politykę bezpieczeństwa SA-17(01)_ODP[01]>***, która ma być egzekwowana; |
| | **SA-17(01)(a)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, jako integralną część procesu rozwoju, wytworzenia formalnego modelu polityki opisującego ***<organizacyjną politykę ochrony prywatności SA-17(01)_ODP[02]>***, która ma być egzekwowana; |
| | **SA-17(01)(b)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykazania, że formalny model polityki jest wewnętrznie spójny i wystarczający do egzekwowania określonych elementów polityki bezpieczeństwa po jego wdrożeniu. |
| | **SA-17(01)(b)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykazania, że formalny model polityki jest wewnętrznie spójny i wystarczający do egzekwowania określonych elementów polityki ochrony prywatności po jego wdrożeniu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-17(01)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| FORMALNY MODEL POLITYKI** | |
| | **SA-17(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury nabywania systemu i usług; polityka w zakresie architektury korporacyjnej; dokumentacja architektury korporacyjnej; procedury dotyczące architektury bezpieczeństwa i ochrony prywatności oraz specyfikacje projektowe systemu przygotowane przez programistę; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-17(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programista systemu]. |

| | | |
|---|---|---|
| **SA-17(02)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| BAZOWE ELEMENTY BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-17(02)(a)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się zdefiniowania sprzętu istotnego dla bezpieczeństwa; |
| | **SA-17(02)(a)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się zdefiniowania oprogramowania istotnego dla bezpieczeństwa; |

| | | |
|---|---|---|
| **SA-17(02)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| BAZOWE ELEMENTY BEZPIECZEŃSTWA** | |
| | **SA-17(02)(a)[03]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się zdefiniowania oprogramowania układowego istotnego dla bezpieczeństwa; |
| | **SA-17(02)(b)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przedstawienia uzasadnienia, że sprzęt, aplikacje i oprogramowanie układowe mające znaczenie dla bezpieczeństwa zdefiniowano w sposób wyczerpujący. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-17(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka w zakresie nabywania systemu i usług; polityka w zakresie architektury korporacyjnej; formalny model polityki; procedury dotyczące specyfikacji projektowych i architektury bezpieczeństwa systemu; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; formalna dokumentacja specyfikacji najwyższego poziomu; dokumentacja projektowa i dotycząca architektury bezpieczeństwa systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja opisująca istotny z punktu widzenia bezpieczeństwa sprzęt, oprogramowanie i oprogramowanie układowe, nieuwzględnione w formalnej dokumentacji specyfikacji najwyższego poziomu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-17(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za architekturę i projektowanie bezpieczeństwa informacji]. |

| | | |
|---|---|---|
| **SA-17(03)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| FORMALNA SPECYFIKACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-17(03)(a)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, jako integralną część procesu rozwoju, wytworzenia formalnej specyfikacji najwyższego poziomu, która określa interfejsy sprzętu, aplikacji i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa powiązane merytorycznie z wyjątkami; |
| | **SA-17(03)(a)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, jako integralną część procesu rozwoju, wytworzenia formalnej specyfikacji najwyższego poziomu, która określa interfejsy sprzętu, aplikacji i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa powiązane merytorycznie z komunikatami o błędach; |
| | **SA-17(03)(a)[03]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, jako integralną część procesu rozwoju, wytworzenia formalnej specyfikacji najwyższego poziomu, która określa interfejsy sprzętu, aplikacji i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa powiązane merytorycznie ze skutkami; |
| | **SA-17(03)(b)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się przedstawienia dowodów na to, że formalna specyfikacja najwyższego poziomu jest zgodna z formalnym modelem polityki w zakresie, w jakim jest to wykonalne, włącznie z dodatkową, nieformalną prezentacją, o ile będzie ona wymagana; |
| | **SA-17(03)(c)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykazania w drodze nieformalnej prezentacji, że formalna specyfikacja najwyższego poziomu w pełni obejmuje interfejsy sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa; |

| | | |
|---|---|---|
| **SA-17(03)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| FORMALNA SPECYFIKACJA** | |
| | **SA-17(03)(d)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykazania, że formalna specyfikacja najwyższego poziomu stanowi dokładny opis wdrażanego sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa; |
| | **SA-17(03)(e)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się opisania istotnych dla bezpieczeństwa mechanizmów związanych ze sprzętem, oprogramowaniem i oprogramowaniem układowym, które nie są uwzględnione w formalnej specyfikacji najwyższego poziomu, ale ściśle dotyczą sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-17(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka w zakresie architektury korporacyjnej; formalny model polityki; procedury dotyczące architektury bezpieczeństwa i specyfikacji projektowej systemu przygotowanych przez programistę; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług;<br><br>umowy nabycia systemu, komponentu systemu lub usługi systemowej; formalna dokumentacja specyfikacji najwyższego poziomu; dokumentacja architektury bezpieczeństwa i projektu systemu; dokumentacja projektu systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br><br>dokumentacja opisująca istotny z punktu widzenia bezpieczeństwa sprzęt, oprogramowanie i oprogramowanie układowe, nieuwzględnione w formalnej dokumentacji specyfikacji najwyższego poziomu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-17(03)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| FORMALNA SPECYFIKACJA** | |
| | **SA-17(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za architekturę i projektowanie bezpieczeństwa informacji]. |

| | | |
|---|---|---|
| **SA-17(04)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| NIEFORMALNE SPECYFIKACJE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-17(04)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {nieformalna prezentacja, przekonujący argument z zastosowaniem metod formalnych, jeśli jest to możliwe};*** |
| | **SA-17(04)(a)[01]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, jako integralną część procesu rozwoju, wytworzenia nieformalnej, opisowej specyfikacji najwyższego poziomu, która określa interfejsy sprzętu, aplikacji i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa powiązane merytorycznie z wyjątkami; |
| | **SA-17(04)(a)[02]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, jako integralną część procesu rozwoju, wytworzenia nieformalnej, opisowej specyfikacji najwyższego poziomu, która określa interfejsy sprzętu, aplikacji i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa powiązane merytorycznie z komunikatami o błędach; |

| | | |
|---|---|---|
| **SA-17(04)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| NIEFORMALNE SPECYFIKACJE** | |
| | **SA-17(04)(a)[03]** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się, jako integralną część procesu rozwoju, wytworzenia nieformalnej, opisowej specyfikacji najwyższego poziomu, która określa interfejsy sprzętu, aplikacji i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa powiązane merytorycznie ze skutkami; |
| | **SA-17(04)(b)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykazania poprzez ***<WYBRANA WARTOŚĆ PARAMETRU SA-17(04)_ODP>***, że opisowa specyfikacja najwyższego poziomu jest zgodna z formalnym modelem polityki; |
| | **SA-17(04)(c)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykazania w drodze nieformalnej prezentacji, że opisowa specyfikacja najwyższego poziomu w pełni obejmuje interfejsy sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa; |
| | **SA-17(04)(d)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wykazania, że opisowa specyfikacja najwyższego poziomu stanowi dokładny opis interfejsów sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa; |
| | **SA-17(04)(e)** | od twórcy systemu, komponentu systemowego lub usługi systemowej wymaga się opisania istotnych dla bezpieczeństwa mechanizmów związanych ze sprzętem, oprogramowaniem i oprogramowaniem układowym, które nie są uwzględnione w opisowej specyfikacji najwyższego poziomu, ale ściśle dotyczą sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-17(04)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| NIEFORMALNE SPECYFIKACJE** | |
| | **SA-17(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka w zakresie architektury korporacyjnej; formalny model polityki; procedury dotyczące architektury bezpieczeństwa i specyfikacji projektowych systemu; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; nieformalna, opisowa dokumentacja specyfikacji najwyższego poziomu; dokumentacja architektury bezpieczeństwa systemu i projektu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br><br>dokumentacja opisująca sprzęt, oprogramowanie i oprogramowanie układowe istotne z punktu widzenia bezpieczeństwa, nieuwzględnione w nieformalnej, opisowej dokumentacji specyfikacji najwyższego poziomu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-17(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za architekturę i projektowanie bezpieczeństwa informacji]. |

| | | |
|---|---|---|
| **SA-17(05)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| PROJEKT PROSTY KONCEPCYJNIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-17(05)(a)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się projektowania i strukturyzowania sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa w celu wykorzystania kompletnego, prostego koncepcyjnie mechanizmu ochrony z precyzyjnie zdefiniowaną semantyką; |
| | **SA-17(05)(b)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się wewnętrznego ustrukturyzowania sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa, ze szczególnym uwzględnieniem tego mechanizmu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-17(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka w zakresie architektury korporacyjnej; procedury dotyczące architektury bezpieczeństwa oraz specyfikacje projektowe systemu przygotowane przez programistę; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługa systemowa; dokumentacja projektowa systemu; dokumentacja architektury bezpieczeństwa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja programisty opisująca projekt i strukturę sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SA-17(05)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| PROJEKT PROSTY KONCEPCYJNIE** | |
| | **SA-17(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za architekturę i projektowanie bezpieczeństwa informacji]. |

| | | |
|---|---|---|
| **SA-17(06)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| STRUKTURA DO TESTOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-17(06)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się stworzenia sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa w celu ułatwienia testowania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SA-17(06)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| STRUKTURA DO TESTOWANIA** | |
| | **SA-17(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka w zakresie architektury korporacyjnej; procedury dotyczące architektury bezpieczeństwa oraz specyfikacje projektowe systemu przygotowane przez programistę; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja projektowa systemu; dokumentacja architektury bezpieczeństwa systemu; dokumentacja architektury prywatności; ustawienia konfiguracyjne systemu oraz związana z nimi dokumentacja; dokumentacja programisty opisująca projekt i strukturę sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa w celu ułatwienia testowania; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-17(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usługi; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programista systemu; personel organizacyjny odpowiedzialny za architekturę i projektowanie w zakresie bezpieczeństwa i prywatności informacji]. |

| | | |
|---|---|---|
| **SA-17(07)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| STRUKTURA NAJNIŻSZYCH UPRAWNIEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-17(07)** | od twórcy systemu, komponentu systemu lub usługi systemowej wymaga się tworzenia sprzętu, oprogramowania i oprogramowania układowego istotnego z punktu widzenia bezpieczeństwa w celu ułatwienia kontroli dostępu z zastosowaniem zasady wiedzy koniecznej. |

| | | |
|---|---|---|
| **SA-17(07)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| STRUKTURA NAJNIŻSZYCH UPRAWNIEŃ** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-17(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka w zakresie architektury korporacyjnej ; procedury dotyczące architektury bezpieczeństwa oraz specyfikacje projektowe systemu przygotowane przez programistę; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja projektowa systemu; dokumentacja architektury bezpieczeństwa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br><br>dokumentacja programisty opisująca projekt i strukturę istotnych z punktu widzenia bezpieczeństwa komponentów sprzętu, oprogramowania i oprogramowania układowego w celu ułatwienia kontroli dostępu z zastosowaniem zasady wiedzy koniecznej; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-17(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usługi; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za architekturę i projektowanie bezpieczeństwa informacji]. |

| | | |
|---|---|---|
| **SA-17(08)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| ARANŻACJA (ORKIESTRACJA)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-17(08)_ODP[01]** | ***określono krytyczne systemy lub komponenty systemu;*** |

| | | |
|---|---|---|
| **SA-17(08)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| ARANŻACJA (ORKIESTRACJA)** | |
| | **SA-17(08)_ODP[02]** | ***określono zdolności, które mają być zapewniane przez systemy lub ich komponenty;*** |
| | **SA-17(08)** | zaprojektowano ***<krytyczne systemy SA-17(08)_ODP[01]>*** oparte na skoordynowanym zachowaniu w celu wdrożenia ***<zdolności SA-17(08)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-17(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka w zakresie architektury korporacyjnej; procedury dotyczące architektury bezpieczeństwa i ochrony prywatności oraz specyfikacje projektowe systemu przygotowane przez programistę; architektura korporacyjna; architektura bezpieczeństwa; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>dokumentacja programisty opisująca orkiestrację projektu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SA-17(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabycie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programista systemu; personel organizacyjny odpowiedzialny za architekturę bezpieczeństwa informacji]. |

| | | |
|---|---|---|
| **SA-17(09)** | **ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA \| ROZPROSZENIE PROJEKTOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-17(09)_ODP** | ***określono krytyczne systemy lub komponenty systemu, które mają być zrealizowane w oparciu o różne projekty;*** |
| | **SA-17(09)** | ***<krytyczne systemy SA-17(09)_ODP>*** opracowano w oparciu o różne projekty w celu spełnienia wspólnego zestawu wymagań lub zapewnienia równoważnej funkcjonalności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-17(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; polityka w zakresie architektury korporacyjnej; procedury dotyczące architektury bezpieczeństwa przygotowanej przez programistę oraz rozproszonego projektowania systemu; dokumentacja przetargowa; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja projektowa systemu; dokumentacja architektury bezpieczeństwa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja programisty opisująca rozproszone projektowanie; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-17(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za architekturę bezpieczeństwa informacji]. |

| | | |
|---|---|---|
| **SA-18** | **ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI** | |
| | [WYCOFANE: Włączone do SR-09]. | |

| SA-18(01) | OPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI \| WIELOFAZOWOŚĆ CYKLU ŻYCIA SYSTEMU |
|---|---|
| | [WYCOFANE: Włączone do SR-09(01)]. |

| SA-18(02) | OPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI \| KONTROLA SYSTEMÓW INFORMATYCZNYCH, KOMPONENTÓW LUB URZĄDZEŃ |
|---|---|
| | [WYCOFANE: Włączone do SR-10]. |

| SA-19 | AUTENTYCZNOŚĆ KOMPONENTÓW |
|---|---|
| | [WYCOFANE: Włączone do SR-11]. |

| SA-19(01) | AUTENTYCZNOŚĆ KOMPONENTU \| SZKOLENIE Z ZAKRESU ZAPOBIEGANIA FAŁSZERSTWOM |
|---|---|
| | [WYCOFANE: Włączone do SR-11(01)]. |

| SA-19(02) | AUTENTYCZNOŚĆ KOMPONENTU \| ZABEZPIECZENIE KONFIGURACJI SERWISOWANYCH I NAPRAWIANYCH KOMPONENTÓW |
|---|---|
| | [WYCOFANE: Włączone do SR-11(02)]. |

| SA-19(03) | AUTENTYCZNOŚĆ KOMPONENTÓW \| UTYLIZACJA KOMPONENTÓW |
|---|---|
| | [WYCOFANE: Włączone do SR-12]. |

| | |
|---|---|
| **SA-19(04)** | **AUTENTYCZNOŚĆ KOMPONENTU \| SKANOWANIE ANTYFAŁSZERSKIE** |
| | [WYCOFANE: Włączone do SR-11(03)]. |

| | | |
|---|---|---|
| **SA-20** | **NIESTANDARDOWA (NA ZAMÓWIENIE) ROZBUDOWA KOMPONENTÓW KRYTYCZNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-20_ODP** | ***określono krytyczne komponenty systemu, które mają być ponownie wdrożone lub opracowane na zamówienie;*** |
| | **SA-20** | ***<krytyczne systemy SA-20_ODP>*** są wdrażane ponownie lub opracowywane na zamówienie. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-20-Badanie** | [WYBÓR SPOŚRÓD: Plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemu i usług; procedury dotyczące niestandardowej rozbudowy krytycznych komponentów systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja cyklu życia rozwoju systemu dotycząca niestandardowego rozwoju krytycznych komponentów systemu; dokumentacja zarządzania konfiguracją; dokumentacja dotycząca audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SA-20-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ponowne wdrażanie lub niestandardową rozbudowę krytycznych komponentów systemu]. |

| | | |
|---|---|---|
| **SA-20** | **NIESTANDARDOWA (NA ZAMÓWIENIE) ROZBUDOWA KOMPONENTÓW KRYTYCZNYCH** | |
| | **SA-20-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ponownego wdrażania lub niestandardowej rozbudowy krytycznych komponentów systemu; mechanizmy wspierające lub wdrażające ponowne wdrażanie lub niestandardową rozbudowę krytycznych komponentów systemu]. |

| | | |
|---|---|---|
| **SA-21** | **DOBÓR DEWELOPERÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-21_ODP[01]** | ***określono system, komponent systemu lub usługę systemową, do której ma dostęp twórca;*** |
| | **SA-21_ODP[02]** | ***określono oficjalne obowiązki twórcy wynikające z pełnionej funkcji;*** |
| | **SA-21_ODP[03]** | ***określono dodatkowe kryteria weryfikacji personelu, którym podlega twórca;*** |
| | **SA-21a.** | twórca ***<systemu, komponentu systemu lub usługi systemowej SA-21_ODP[01]>***<br>jest zobowiązany do posiadania odpowiednich uprawnień dostępu określonych na podstawie przydzielonych mu<br>***<oficjalnych obowiązków SA-21_ODP[02]>***; |
| | **SA-21b.** | twórca ***<systemu, komponentu systemu lub usługi systemowej SA-21_ODP[01]>***<br>musi spełniać ***<dodatkowe kryteria weryfikacji personelu SA-21_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **SA-21** | **DOBÓR DEWELOPERÓW** | |
|---|---|---|
| | **SA-21-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemów i usług; polityka i procedury bezpieczeństwa personelu; procedury dotyczące kontroli bezpieczeństwa personelu; dokumentacja projektowa systemu; dokumentacja nabycia; umowy o poziomie usług; umowy o świadczenie usług programowania; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz odpowiednich uprawnień dostępu wymaganych przez programistów systemu; kryteria weryfikacji personelu i związana z nimi dokumentacją;<br>plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-21-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za weryfikację programistów]. |
| | **SA-21-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie weryfikacji programistów; mechanizmy wspierające weryfikację programistów]. |

| **SA-21(01)** | **DOBÓR DEWELOPERÓW \| OCENA PRZEGLĄDU** |
|---|---|
| | [WYCOFANE: Włączone do SA-21]. |

| **SA-22** | **KOMPONENTY SYSTEMU BEZ WSPARCIA** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-22_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {wsparcie wewnętrzne; <wsparcie od dostawców zewnętrznych SA-22_ODP[02]>};*** |

| | | |
|---|---|---|
| **SA-22** | **KOMPONENTY SYSTEMU BEZ WSPARCIA** | |
| | **SA-22_ODP[02]** | ***określono wsparcie zapewniane przez dostawców zewnętrznych (jeśli wybrano);*** |
| | **SA-22a.** | komponenty systemu są zastępowane, jeżeli ich twórcy, sprzedawcy lub producenci nie zapewniają już dla nich wsparcia; |
| | **SA-22b.** | ***<WYBRANA WARTOŚĆ PARAMETRU SA-22_ODP[01]>*** zapewnia alternatywne opcje w zakresie kontynuacji wsparcia dla nieobsługiwanych komponentów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-22-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące zastąpienia lub dalszego użytkowania nieobsługiwanych komponentów systemu; udokumentowane dowody zastąpienia nieobsługiwanych komponentów systemu; udokumentowane zatwierdzenia (wraz z uzasadnieniem) dalszego użytkowania nieobsługiwanych komponentów systemu; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-22-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za cykl życia systemu; personel organizacyjny odpowiedzialny za zastępowanie komponentów]. |
| | **SA-22-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie zastępowania nieobsługiwanych komponentów systemu; mechanizmy wspierające lub wdrażające wymianę nieobsługiwanych komponentów systemu]. |

| | |
|---|---|
| **SA-22(01)** | **KOMPONENTY SYSTEMU BEZ WSPARCIA \| ALTERNATYWNE ŹRÓDŁA STAŁEGO WSPARCIA** |
| | [WYCOFANE: Włączone do SA-22]. |

| | | |
|---|---|---|
| **SA-23** | **SPECJALIZACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SA-23_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {modyfikacja projektu; rozbudowa; rekonfiguracja};*** |
| | **SA-23_ODP[02]** | ***określono systemy lub komponenty systemu wspierające usługi lub funkcje istotne z punktu widzenia misji;*** |
| | **SA-23** | stosuje się ***<WYBRANA WARTOŚĆ PARAMETRU SA-23_ODP[01]>*** w ***<systemach lub komponentach systemu SA-23_ODP[02]>*** wspierających niezbędne usługi lub funkcje w celu zwiększenia wiarygodności takich systemów lub komponentów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SA-23-Badanie** | [WYBÓR SPOŚRÓD: Polityka nabywania systemu i usług; procedury dotyczące modyfikacji projektu, rozbudowy lub rekonfiguracji systemu lub komponentów systemu; udokumentowane dowody modyfikacji projektu, rozbudowy lub rekonfiguracji; plan bezpieczeństwa systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SA-23-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za architekturę bezpieczeństwa; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją]. |

| SA-23 | SPECJALIZACJA | |
|---|---|---|
| | **SA-23-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące modyfikacji projektu, rozbudowy lub rekonfiguracji systemu lub komponentów systemu; mechanizmy wspierające lub wdrażające modyfikację projektu, rozbudowę lub rekonfigurację systemu lub komponentów systemu]. |

# 4.18. KATEGORIA SC - OCHRONA SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH

| | | |
|---|---|---|
| **SC-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-01_ODP[01]** | ***określono personel lub role, wśród których ma być rozpowszechniana polityka ochrony systemów i sieci telekomunikacyjnych;*** |
| | **SC-01_ODP[02]** | ***określono personel lub role, wśród których mają być rozpowszechniane procedury ochrony systemów i sieci telekomunikacyjnych;*** |
| | **SC-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **SC-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami ochrony systemów i sieci telekomunikacyjnych;*** |
| | **SC-01_ODP[05]** | ***określono częstotliwość przeglądu i aktualizacji polityki ochrony systemów i sieci telekomunikacyjnych;*** |
| | **SC-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji polityki ochrony systemów i sieci telekomunikacyjnych;*** |
| | **SC-01_ODP[07]** | ***określono częstotliwość przeglądu i aktualizacji procedur ochrony systemów i sieci telekomunikacyjnych;*** |
| | **SC-01_ODP[08]** | ***określono zdarzenia wymagające przeglądu i aktualizacji obecnych procedur ochrony systemów i sieci telekomunikacyjnych;*** |
| | **SC-01a.[01]** | opracowano i udokumentowano politykę ochrony systemów i sieci telekomunikacyjnych; |
| | **SC-01a.[02]** | polityka ochrony systemów i sieci telekomunikacyjnych jest rozpowszechniana wśród<br>***<personelu lub ról SC-01_ODP[01]>***; |

| SC-01 | POLITYKA I PROCEDURY | |
|---|---|---|
| | **SC-01a.[03]** | opracowano i udokumentowano procedury ochrony systemów i sieci telekomunikacyjnych ułatwiające wdrażanie polityki w tym obszarze oraz stosowanie powiązanych zabezpieczeń; |
| | **SC-01a.[04]** | procedury ochrony systemów i sieci telekomunikacyjnych są rozpowszechniane wśród<br>***<personelu lub ról SC-01_ODP[02]>***; |
| | **SC-01a.01(a)[01]** | polityka ochrony systemów i sieci telekomunikacyjnych ***<WYBRANA WARTOŚĆ PARAMETRU SC-01_ODP[03]>***<br>odnosi się do celu; |
| | **SC-01a.01(a)[02]** | polityka ochrony systemów i sieci telekomunikacyjnych ***<WYBRANA WARTOŚĆ PARAMETRU SC-01_ODP[03]>***<br>odnosi się do zakresu; |
| | **SC-01a.01(a)[03]** | polityka ochrony systemów i sieci telekomunikacyjnych ***<WYBRANA WARTOŚĆ PARAMETRU SC-01_ODP[03]>***<br>odnosi się do ról; |
| | **SC-01a.01(a)[04]** | polityka ochrony systemów i sieci telekomunikacyjnych ***<WYBRANA WARTOŚĆ PARAMETRU SC-01_ODP[03]>***<br>odnosi się do obowiązków; |
| | **SC-01a.01(a)[05]** | polityka ochrony systemów i sieci telekomunikacyjnych ***<WYBRANA WARTOŚĆ PARAMETRU SC-01_ODP[03]>***<br>odnosi się do zaangażowania kierownictwa; |
| | **SC-01a.01(a)[06]** | polityka ochrony systemów i sieci telekomunikacyjnych ***<WYBRANA WARTOŚĆ PARAMETRU SC-01_ODP[03]>***<br>odnosi się do współpracy pomiędzy podmiotami organizacji; |

| | | |
|---|---|---|
| **SC-01** | **POLITYKA I PROCEDURY** | |
| | **SC-01a.01(a)[07]** | polityka ochrony systemów i sieci telekomunikacyjnych ***<WYBRANA WARTOŚĆ PARAMETRU SC-01_ODP[03]>***<br>odnosi się do zgodności; |
| | **SC-01a.01(b)** | polityka ochrony systemów i sieci telekomunikacyjnych ***<WYBRANA WARTOŚĆ PARAMETRU SC-01_ODP[03]>***<br>jest zgodna z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |
| | **SC-01b.** | ***<urzędnik SC-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur ochrony systemów i sieci telekomunikacyjnych; |
| | **SC-01c.01[01]** | polityka ochrony systemów i sieci telekomunikacyjnych jest przeglądana i aktualizowana z<br>***<częstotliwością SC-01_ODP[05]>***; |
| | **SC-01c.01[02]** | polityka ochrony systemów i sieci telekomunikacyjnych jest przeglądana i aktualizowana po***<zdarzeniach SC-01_ODP[06]>***; |
| | **SC-01c.02[01]** | procedury ochrony systemów i sieci telekomunikacyjnych są przeglądane i aktualizowane z ***<częstotliwością SC-01_ODP[07]>***; |
| | **SC-01c.02[02]** | procedury ochrony systemów i sieci telekomunikacyjnych są przeglądane i aktualizowane po***<zdarzeniach SC-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury ochrony systemów i sieci telekomunikacyjnych; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja strategii zarządzania ryzykiem; zapisy z audytu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-01** | **POLITYKA I PROCEDURY** | |
| | **SC-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę systemów i sieci telekomunikacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **SC-02** | **ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU I UŻYTKOWNIKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-02** | funkcje użytkownika, w tym usługi interfejsu użytkownika, są oddzielone od funkcji zarządzania systemem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące oddzielenia aplikacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-02-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-02-Test** | [WYBÓR SPOŚRÓD: Oddzielenie funkcji użytkownika od funkcji zarządzania systemem]. |

| | | |
|---|---|---|
| **SC-02(01)** | **ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU I UŻYTKOWNIKA \| INTERFEJSY DLA UŻYTKOWNIKÓW NIEUPRZYWILEJOWANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-02(01)** | uniemożliwiono wyświetlanie funkcji zarządzania systemem w interfejsach dla użytkowników nieuprzywilejowanych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-02(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące oddzielenia aplikacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-02(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; nieuprzywilejowani użytkownicy systemu; programista systemu]. |
| | **SC-02(01)-Test** | [WYBÓR SPOŚRÓD: Oddzielenie funkcji użytkownika od funkcji zarządzania systemem]. |

| | | |
|---|---|---|
| **SC-02(02)** | **ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU I UŻYTKOWNIKA \| NIEPOŁĄCZALNOŚĆ (DEZASOCJACJA)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-02(02)** | informacje o stanie aplikacji lub oprogramowania są przechowywane oddzielnie od takiej aplikacji bądź oprogramowania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-02(02)** | **ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU I UŻYTKOWNIKA \| NIEPOŁĄCZALNOŚĆ (DEZASOCJACJA)** | |
| | **SC-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące oddzielenia aplikacji i oprogramowania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SC-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; programista systemu]. |
| | **SC-02(02)-Test** | [WYBÓR SPOŚRÓD: Oddzielenie informacji o stanie aplikacji lub oprogramowania od samej aplikacji bądź oprogramowania]. |

| | | |
|---|---|---|
| **SC-03** | **IZOLACJA FUNKCJI BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-03** | funkcje bezpieczeństwa są oddzielone od funkcji niezwiązanych z bezpieczeństwem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące oddzielenia funkcji bezpieczeństwa; wykaz funkcji bezpieczeństwa podlegających oddzieleniu od funkcji niebędących funkcjami bezpieczeństwa; dokumentacja projektowa systemu;<br>konfiguracja systemu i związana z nią dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-03** | **IZOLACJA FUNKCJI BEZPIECZEŃSTWA** | |
| | **SC-03-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-03-Test** | [WYBÓR SPOŚRÓD: Oddzielenie funkcji bezpieczeństwa od funkcji niezwiązanych z bezpieczeństwem systemu]. |

| | | |
|---|---|---|
| **SC-03(01)** | **IZOLACJA FUNKCJI BEZPIECZEŃSTWA \| SEPARACJA SPRZĘTOWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-03(01)** | stosuje się mechanizmy separacji sprzętowej realizujące zasadę oddzielenia funkcji bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące oddzielenia funkcji bezpieczeństwa; dokumentacja projektowa systemu; mechanizmy separacji sprzętowej; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-03(01)-Test** | [WYBÓR SPOŚRÓD: Oddzielenie funkcji bezpieczeństwa od funkcji niezwiązanych z bezpieczeństwem systemu]. |

| | | |
|---|---|---|
| **SC-03(02)** | **IZOLACJA FUNKCJI BEZPIECZEŃSTWA \| FUNKCJE KONTROLI DOSTĘPU I PRZEPŁYWU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-03(02)[01]** | funkcje bezpieczeństwa wymuszające kontrolę dostępu są oddzielone od funkcji niezwiązanych z bezpieczeństwem; |
| | **SC-03(02)[02]** | funkcje bezpieczeństwa wymuszające egzekwowanie kontroli dostępu są oddzielone od innych funkcji bezpieczeństwa; |
| | **SC-03(02)[03]** | funkcje bezpieczeństwa wymuszające egzekwowanie kontroli przepływu informacji są oddzielone od funkcji niezwiązanych z bezpieczeństwem; |
| | **SC-03(02)[04]** | funkcje bezpieczeństwa wymuszające egzekwowanie kontroli przepływu informacji są oddzielone od innych funkcji bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące oddzielenia funkcji bezpieczeństwa; wykaz krytycznych funkcji bezpieczeństwa; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-03(02)-Test** | [WYBÓR SPOŚRÓD: Oddzielenie funkcji bezpieczeństwa wymuszających kontrolę dostępu i przepływu informacji]. |

| | | |
|---|---|---|
| **SC-03(03)** | **IZOLACJA FUNKCJI BEZPIECZEŃSTWA \| MINIMALIZACJA FUNKCJI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-03(03)** | minimalizuje się liczbę funkcji niezwiązanych z bezpieczeństwem zawartych w granicach izolacji zawierających funkcje bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące oddzielenia funkcji bezpieczeństwa; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SC-03(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające granice izolacji]. |

| | | |
|---|---|---|
| **SC-03(04)** | **IZOLACJA FUNKCJI BEZPIECZEŃSTWA \| SPRZĘŻANIE I SPÓJNOŚĆ MODUŁÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-03(04)[01]** | funkcje bezpieczeństwa są wdrażane jako zasadniczo niezależne moduły, maksymalizujące wewnętrzną spójność w obrębie modułów; |
| | **SC-03(04)[02]** | funkcje bezpieczeństwa są wdrażane jako zasadniczo niezależne moduły, minimalizujące sprzężenie między modułami. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SC-03(04) | IZOLACJA FUNKCJI BEZPIECZEŃSTWA \| SPRZĘŻANIE I SPÓJNOŚĆ MODUŁÓW | |
|---|---|---|
| | **SC-03(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące oddzielenia funkcji bezpieczeństwa; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-03(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SC-03(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne maksymalizujące wewnętrzną spójność w obrębie modułów i minimalizujące sprzężenie pomiędzy nimi; mechanizmy wspierające lub wdrażające funkcje bezpieczeństwa jako niezależne moduły]. |

| SC-03(05) | IZOLACJA FUNKCJI BEZPIECZEŃSTWA \| STRUKTURY WARSTWOWE | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-03(05)** | funkcje bezpieczeństwa są wdrażane jako struktura warstwowa, minimalizująca interakcje między warstwami i unikająca zależności niższych warstw od działania lub poprawności warstw wyższych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-03(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące oddzielenia funkcji bezpieczeństwa; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-03(05)** | **IZOLACJA FUNKCJI BEZPIECZEŃSTWA \| STRUKTURY WARSTWOWE** | |
| | **SC-03(05)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SC-03(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne wdrażające funkcje bezpieczeństwa jako strukturę warstwową, minimalizującą interakcje między warstwami i unikającą zależności niższych warstw od działania/poprawności warstw wyższych; mechanizmy wspierające lub wdrażające funkcje bezpieczeństwa jako strukturę warstwową]. |

| | | |
|---|---|---|
| **SC-04** | **INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-04[01]** | zapobiega się nieuprawnionemu przekazywaniu informacji za pośrednictwem współdzielonych zasobów systemowych; |
| | **SC-04[02]** | zapobiega się niezamierzonemu przekazywaniu informacji za pośrednictwem współdzielonych zasobów systemowych; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony informacji we współdzielonych zasobach systemowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-04-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |

| | | |
|---|---|---|
| **SC-04** | **INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH** | |
| | **SC-04-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zapobiegające nieuprawnionemu i niezamierzonemu przekazywaniu informacji za pośrednictwem współdzielonych zasobów systemowych]. |

| | |
|---|---|
| **SC-04(01)** | **INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH \| POZIOMY BEZPIECZEŃSTWA** |
| | [WYCOFANE: Włączone do SC-04]. |

| | | |
|---|---|---|
| **SC-04(02)** | **INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH \| PRZETWARZANIE WIELOPOZIOMOWE LUB OKRESOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-04(02)_ODP** | ***określono procedury zapobiegające nieuprawnionemu przekazywaniu informacji za pośrednictwem zasobów współdzielonych;*** |
| | **SC-04(02)** | zapobiega się nieuprawnionemu przekazywaniu informacji za pośrednictwem zasobów współdzielonych zgodnie z ***<procedurami SC-04(02)_ODP> w*** przypadku gdy podczas przetwarzania system wyraźnie przełącza się między różnymi poziomami klasyfikacji informacji lub kategoriami bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-04(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony informacji we współdzielonych zasobach systemowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-04(02)** | **INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH \| PRZETWARZANIE WIELOPOZIOMOWE LUB OKRESOWE** | |
| | **SC-04(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-04(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zapobiegające nieuprawnionemu przekazywaniu informacji za pośrednictwem współdzielonych zasobów systemowych]. |

| | | |
|---|---|---|
| **SC-05** | **OCHRONA PRZED BLOKADĄ USŁUG (DoS)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-05_ODP[01]** | ***określono rodzaje ataków typu denial-of-service (DoS), przed którymi należy się chronić lub które należy ograniczyć;*** |
| | **SC-05_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {ochrona przed; ograniczanie};*** |
| | **SC-05_ODP[03]** | ***określono zabezpieczenia służące osiągnięciu celu w zakresie ochrony przed atakami typu DoS według rodzaju zdarzenia typu DoS;*** |
| | **SC-05a.** | efekty ***<zdarzeń typu DoS SC-05_ODP[01]>*** są<br>***<WYBRANA WARTOŚĆ PARAMETRU SC-05_ODP[02]>***; |
| | **SC-05b.** | stosuje się ***<zabezpieczenia zgodne z rodzajem zdarzenia DoS SC-05_ODP[03]>*** do osiągnięcia celu w zakresie ochrony przed atakami typu DoS. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-05** | **OCHRONA PRZED BLOKADĄ USŁUG (DoS)** | |
| | **SC-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony przed atakami typu DoS; dokumentacja projektowa systemu; wykaz ataków typu DoS wymagających zastosowania zabezpieczeń w celu ochrony przed takimi atakami lub ograniczenia ich skutków; wykaz zabezpieczeń chroniących przed atakami typu DoS lub ograniczających ich skutki; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-05-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za reagowanie na incydenty; programista systemu]. |
| | **SC-05-Test** | [WYBÓR SPOŚRÓD: Mechanizmy chroniące przed atakami typu DoS lub ograniczające ich skutki]. |

| | | |
|---|---|---|
| **SC-05(01)** | **OCHRONA PRZED BLOKADĄ USŁUG (DOS) \|OGRANICZENIE MOŻLIWOŚCI ATAKOWANIA INNYCH SYSTEMÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-05(01)_ODP** | ***określono ataki typu DoS, których przeprowadzanie przez osoby fizyczne ma być ograniczone;*** |
| | **SC-05(01)** | zdolność osób do przeprowadzania ***<ataków typu DoS SC-05(01)_ODP>*** przeciwko innym systemom jest ograniczona. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-05(01)** | **OCHRONA PRZED BLOKADĄ USŁUG (DOS) \|OGRANICZENIE MOŻLIWOŚCI ATAKOWANIA INNYCH SYSTEMÓW** | |
| | **SC-05(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemu i sieci telekomunikacyjnych; procedury dotyczące ochrony przed atakami typu DoS; dokumentacja projektowa systemu; wykaz ataków typu DoS przeprowadzanych przez osoby fizyczne na systemy; wykaz ataków typu DoS przeprowadzanych przez osoby fizyczne na systemy;<br>ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-05(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za reagowanie na incydenty; programista systemu]. |
| | **SC-05(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy ograniczające możliwość przeprowadzania ataków typu DoS na inne systemy]. |

| | | |
|---|---|---|
| **SC-05(02)** | **OCHRONA PRZED BLOKADĄ USŁUG (DOS) \| PRZEPUSTOWOŚĆ, SZEROKOŚĆ PASMA I NADMIAROWOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-05(02)** | zarządza się przepustowością, pasmem lub innymi nadmiarowymi zasobami w celu ograniczenia skutków ataków typu DoS. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-05(02)** | **OCHRONA PRZED BLOKADĄ USŁUG (DOS) \| PRZEPUSTOWOŚĆ, SZEROKOŚĆ PASMA I NADMIAROWOŚĆ** | |
| | **SC-05(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony przed atakami typu DoS; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-05(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za reagowanie na incydenty; programista systemu]. |
| | **SC-05(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zarządzanie pasmem, przepustowością i nadmiarowymi zasobami systemu w celu ograniczenia skutków ataków typu DoS]. |

| | | |
|---|---|---|
| **SC-05(03)** | **OCHRONA PRZED BLOKADĄ USŁUG (DOS) \| WYKRYWANIE I MONITOROWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-05(03)_ODP[01]** | ***określono narzędzia monitorujące do wykrywania oznak ataków typu DoS;*** |
| | **SC-05(03)_ODP[02]** | ***określono systemowe narzędzia monitorujące służące do ustalenia, czy dostępne są wystarczające zasoby w celu zapobiegania skutecznym atakom typu DoS;*** |
| | **SC-05(03)(a)** | stosuje się ***<narzędzia monitorujące SC-05(03)_ODP[01]>*** do wykrywania oznak ataków typu DoS skierowanych przeciwko systemowi lub z niego uruchamianych; |

| | | |
|---|---|---|
| **SC-05(03)** | **OCHRONA PRZED BLOKADĄ USŁUG (DOS) \| WYKRYWANIE I MONITOROWANIE** | |
| | **SC-05(03)(b)** | stosuje się ***<narzędzia monitorujące SC-05(03)_ODP[01]>***, by ustalić, czy dostępne są wystarczające zasoby w celu zapobiegania skutecznym atakom typu DoS. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-05(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony przed atakiem typu DoS; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-05(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za wykrywanie ataków i monitorowanie]. |
| | **SC-05(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy/narzędzia wdrażające monitorowanie systemu pod kątem ataków typu DoS]. |

| | | |
|---|---|---|
| **SC-06** | **DOSTĘPNOŚĆ ZASOBÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-06_ODP[01]** | ***określono zasoby, które mają być przydzielone w celu ochrony dostępności zasobów;*** |
| | **SC-06_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {priorytet; przydział; <zabezpieczenia SC-06_ODP[03]>};*** |
| | **SC-06_ODP[03]** | ***określono zabezpieczenia chroniące dostępność zasobów (jeśli wybrano);*** |

| | | |
|---|---|---|
| **SC-06** | **DOSTĘPNOŚĆ ZASOBÓW** | |
| | **SC-06** | dostępność zasobów jest chroniona poprzez alokację***<zasobów SC-06_ODP[01]>***.<br>przez ***<WYBRANA WARTOŚĆ PARAMETRU SC-06_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące nadawania priorytetów zasobom systemowym; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-06-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-06-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność do alokacji zasobów; zabezpieczenia stosowane w celu zapewnienia dostępności zasobów]. |

| | | |
|---|---|---|
| **SC-07** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {fizycznie; logicznie};*** |
| | **SC-07a.[01]** | komunikacja na zewnętrznych zarządzanych interfejsach systemu jest monitorowana; |
| | **SC-07a.[02]** | komunikacja na zewnętrznych zarządzanych interfejsach systemu jest kontrolowana; |

| | | |
|---|---|---|
| **SC-07** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH** | |
| | **SC-07a.[03]** | komunikacja na kluczowych wewnętrznych zarządzanych interfejsach systemu jest monitorowana; |
| | **SC-07a.[04]** | komunikacja na kluczowych wewnętrznych zarządzanych interfejsach systemu jest kontrolowana; |
| | **SC-07b.** | podsieci dla publicznie dostępnych komponentów systemu są ***<WYBRANA WARTOŚĆ PARAMETRU SC-07_ODP>*** oddzielone od wewnętrznych sieci organizacyjnych; |
| | **SC-07c.** | podłączenie do zewnętrznych sieci lub systemów ma miejsce wyłącznie poprzez zarządzane interfejsy składające się z urządzeń ochrony brzegowej, rozmieszczonych zgodnie z organizacyjną architekturą bezpieczeństwa i ochrony prywatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony brzegowej; wykaz kluczowych wewnętrznych granic systemu; dokumentacja projektowa systemu; sprzęt i oprogramowanie ochrony brzegowej; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja organizacyjnej architektury bezpieczeństwa; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie ochrony połączeń brzegowych]. |

| SC-07(01) | OCHRONA POŁĄCZEŃ BRZEGOWYCH \| FIZYCZNIE ODDZIELONE PODSIECI |
|---|---|
| | [WYCOFANE: Włączone do SC-07]. |

| SC-07(02) | OCHRONA POŁĄCZEŃ BRZEGOWYCH \| DOSTĘP PUBLICZNY |
|---|---|
| | [WYCOFANE: Włączone do SC-07]. |

| SC-07(03) | OCHRONA POŁĄCZEŃ BRZEGOWYCH \| PUNKTY DOSTĘPOWE | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(03)** | liczba zewnętrznych połączeń sieciowych do systemu jest ograniczona. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie ochrony połączeń brzegowych; dokumentacja dotycząca architektury i konfiguracji systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dzienniki monitorowania komunikacji i ruchu sieciowego; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie ochrony połączeń brzegowych; mechanizmy ograniczające liczbę zewnętrznych połączeń sieciowych do systemu]. |

| | | |
|---|---|---|
| **SC-07(04)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| ZEWNĘTRZNE USŁUGI TELEKOMUNIKACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(04)_ODP** | ***określono częstotliwość, z jaką należy dokonywać przeglądu wyjątków od polityki przepływu ruchu;*** |
| | **SC-07(04)(a)** | dla każdej zewnętrznej usługi telekomunikacyjnej wdrożono zarządzany interfejs; |
| | **SC-07(04)(b)** | dla każdego interfejsu zarządzanego ustalono politykę przepływu ruchu; |
| | **SC-07(04)(c)[01]** | poufność informacji przesyłanych przez każdy interfejs jest chroniona; |
| | **SC-07(04)(c)[02]** | integralność informacji przesyłanych przez każdy interfejs jest chroniona; |
| | **SC-07(04)(d)** | każdy wyjątek od polityki przepływu ruchu jest dokumentowany wraz z uzasadnieniem odnoszącym się do misji lub potrzeby biznesowej oraz określeniem czasu trwania takiej potrzeby; |
| | **SC-07(04)(e)[01]** | wyjątki od polityki przepływu ruchu są przeglądane z ***<częstotliwość SC-07(04)_ODP>***; |
| | **SC-07(04)(e)[02]** | wyjątki od polityki przepływu ruchu, które nie są już uzasadnione przez określoną misję lub potrzebę biznesową, są usuwane; |
| | **SC-07(04)(f)** | zapobiega się nieuprawnionej wymianie ruchu z sieciami zewnętrznymi w obrębie płaszczyzny sterowania; |
| | **SC-07(04)(g)** | publikuje się informacje umożliwiające zdalnym sieciom wykrywanie nieautoryzowanego ruchu z sieci wewnętrznych w płaszczyźnie sterowania; |
| | **SC-07(04)(h)** | nieautoryzowany ruch z sieci zewnętrznych w płaszczyźnie sterowania jest filtrowany. |

| | | |
|---|---|---|
| **SC-07(04)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| ZEWNĘTRZNE USŁUGI TELEKOMUNIKACYJNE** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka przepływu ruchu; polityka zabezpieczenia przepływu informacji; procedury dotyczące ochrony połączeń brzegowych; architektura bezpieczeństwa systemu; dokumentacja projektowa systemu; sprzęt i oprogramowanie ochrony połączeń brzegowych; dokumentacja dotycząca architektury i konfiguracji systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące wyjątków od polityki przepływu ruchu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące dokumentowania i przeglądu wyjątków od stosowania polityki przepływu ruchu; procesy organizacyjne w zakresie usuwania wyjątków od polityki przepływu ruchu; mechanizmy wdrażające zdolności w zakresie ochrony połączeń brzegowych; zarządzane interfejsy wdrażające politykę przepływu ruchu]. |

| | | |
|---|---|---|
| **SC-07(05)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| ODRZUĆ DOMYŚLNIE/POZWÓL NA WYJĄTEK** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(05)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {w zarządzanych interfejsach; <w systemach SC-07(05)_ODP[02]>};*** |

| | | |
|---|---|---|
| **SC-07(05)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| ODRZUĆ DOMYŚLNIE/POZWÓL NA WYJĄTEK** | |
| | **SC-07(05)_ODP[02]** | ***określono systemy, w przypadku których dostęp do komunikacji sieciowej jest domyślnie blokowany i jest dopuszczany tylko w drodze wyjątku (jeśli wybrano).*** |
| | **SC-07(05)[01]** | dostęp do komunikacji sieciowej jest domyślnie blokowany ***<WYBRANA WARTOŚĆ PARAMETRU SC-07(05)_ODP[01]>***; |
| | **SC-07(05)[02]** | dostęp do komunikacji sieciowej jest dozwolony w drodze wyjątku ***<WYBRANA WARTOŚĆ PARAMETRU SC-07(05)_ODP[01]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(05)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zarządzanie ruchem w zarządzanych interfejsach]. |

| | |
|---|---|
| **SC-07(06)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| ODPOWIEDŹ NA ROZPOZNANE AWARIE** |
| | [WYCOFANE: Włączone do SC-07(18)]. |

| | | |
|---|---|---|
| **SC-07(07)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| DZIELONE TUNELOWANIE URZĄDZEŃ ZDALNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(07)_ODP** | ***określono zabezpieczenia umożliwiające bezpieczne udostępnianie dzielonych tuneli;*** |
| | **SC-07(07)** | zapobiega się dzieleniu tuneli pomiędzy urządzeniami zdalnymi łączącymi się z systemami organizacyjnymi, chyba że dzielony tunel jest bezpiecznie udostępniony przy użyciu ***<zabezpieczeń SC-07(07)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(07)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(07)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie ochrony połączeń brzegowych; mechanizmy wspierające/ograniczające połączenia niebędące połączeniami zdalnymi]. |

| | | |
|---|---|---|
| **SC-07(08)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| RUCH TELEKOMUNIKACYJNY DO AUTORYZOWANYCH SERWERÓW PROXY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(08)_ODP[01]** | ***określono wewnętrzny ruch telekomunikacyjny, który ma być kierowany do sieci zewnętrznych;*** |
| | **SC-07(08)_ODP[02]** | ***określono sieci zewnętrzne, do których ma być kierowany wewnętrzny ruch telekomunikacyjny;*** |
| | **SC-07(08)** | ***<wewnętrzny ruch telekomunikacyjny SC-07(08)_ODP[01]>*** jest kierowany do<br>***<sieci zewnętrznych SC-07(08)_ODP[02]>*** poprzez uwierzytelnione serwery proxy w zarządzanych interfejsach. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(08)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(08)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zarządzanie ruchem poprzez uwierzytelnione serwery proxy w zarządzanych interfejsach]. |

| | | |
|---|---|---|
| **SC-07(09)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| OGRANICZENIE ZAGROŻEŃ WYJŚCIOWEGO RUCHU TELEKOMUNIKACYJNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(09)(a)[01]** | ruch wychodzący stanowiący zagrożenie dla systemów zewnętrznych jest wykrywany; |
| | **SC-07(09)(a)[02]** | ruch wychodzący stanowiący zagrożenie dla systemów zewnętrznych jest odrzucany; |
| | **SC-07(09)(b)** | tożsamość użytkowników wewnętrznych związanych z odmową komunikacji jest kontrolowana. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(09)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(09)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie ochrony połączeń brzegowych; mechanizmy wdrażające wykrywanie i odrzucanie ruchu wychodzącego, który stanowi zagrożenie; mechanizmy wdrażające kontrolę ruchu wychodzącego]. |

| | | |
|---|---|---|
| **SC-07(10)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| ZAPOBIEGANIE EKSFILTRACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(10)_ODP** | ***określono częstotliwość przeprowadzania testów dotyczących nieautoryzowanego upublicznienia;*** |
| | **SC-07(10)(a)** | nieautoryzowane upublicznienie informacji jest uniemożliwione; |
| | **SC-07(10)(b)** | testy dotyczące nieautoryzowanego upublicznienia są przeprowadzane z ***<częstotliwością SC-07(10)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(10)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(10)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie ochrony połączeń brzegowych, które zapobiegają nieautoryzowanemu upublicznieniu informacji poprzez zarządzane interfejsy]. |

| | | |
|---|---|---|
| **SC-07(11)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| OGRANICZENIE PRZYCHODZĄCEGO RUCHU KOMUNIKACYJNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(11)_ODP[01]** | ***określono autoryzowane źródła komunikacji przychodzącej;*** |
| | **SC-07(11)_ODP[02]** | ***określono autoryzowane miejsca docelowe, do których może być kierowana komunikacja przychodząca z autoryzowanych źródeł;*** |
| | **SC-07(11)** | tylko komunikacja przychodząca z ***<autoryzowanych źródeł SC-07(11)_ODP[01]>*** może być kierowana do ***<autoryzowanych miejsc docelowych SC-07(11)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(11)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(11)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(11)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie ochrony połączeń brzegowych w zakresie skojarzonych par źródło/miejsce docelowe]. |

| | | |
|---|---|---|
| **SC-07(12)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| SYSTEM OCHRONY KOMPUTERA GŁÓWNEGO TYPU HOST** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(12)_ODP[01]** | ***określono mechanizmy ochrony połączeń brzegowych oparte na hostach, które mają być wdrożone;*** |
| | **SC-07(12)_ODP[02]** | ***określono komponenty systemu, w których mają być wdrożone mechanizmy ochrony połączeń brzegowych oparte na hostach;*** |
| | **SC-07(12)** | ***<mechanizmy ochrony połączeń brzegowych oparte na hostach SC-07(12)_ODP[01]>*** są wdrożone w ***<komponentach systemu SC-07(12)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie ochrony połączeń brzegowych; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(12)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych; użytkownicy systemu]. |
| | **SC-07(12)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie ochrony połączeń brzegowych oparte na hostach]. |

| | | |
|---|---|---|
| **SC-07(13)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| IZOLACJA NARZĘDZI BEZPIECZEŃSTWA/MECHANIZMÓW/KOMPONENTÓW WSPARCIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(13)_ODP** | ***określono narzędzia, mechanizmy i komponenty wspierające bezpieczeństwo informacji, które mają być odizolowane od innych wewnętrznych komponentów systemu;*** |
| | **SC-07(13)** | ***<narzędzia, mechanizmy i komponenty wspierające bezpieczeństwo informacji SC-07(13)_ODP>*** są izolowane od innych wewnętrznych komponentów systemu poprzez wdrożenie fizycznie oddzielonych podsieci z zarządzanymi interfejsami do innych komponentów systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(13)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz narzędzi zabezpieczających i komponentów wspierających, które mają być odizolowane od innych wewnętrznych komponentów systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(13)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(13)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażanie izolację narzędzi, mechanizmów i komponentów wspierających bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SC-07(14)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| OCHRONA PRZED NIEAUTORYZOWANYMI POŁĄCZENIAMI FIZYCZNYMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(14)_ODP** | ***określono zarządzane interfejsy, które mają być chronione przed nieautoryzowanymi połączeniami fizycznymi;*** |
| | **SC-07(14)** | ***<zarządzane interfejsy SC-07(14)_ODP>*** są chronione przed nieautoryzowanymi połączeniami fizycznymi; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(14)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu w zakresie komunikacji i okablowania obiektu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(14)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(14)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające ochronę przed nieautoryzowanymi połączeniami fizycznymi]. |

| | | |
|---|---|---|
| **SC-07(15)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| SIECIOWY DOSTĘP UPRZYWILEJOWANY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(15)[01]** | uprzywilejowane połączenia sieciowe są kierowane poprzez dedykowany, zarządzany interfejs w celu kontroli dostępu; |

| | | |
|---|---|---|
| **SC-07(15)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| SIECIOWY DOSTĘP UPRZYWILEJOWANY** | |
| | **SC-07(15)[02]** | uprzywilejowane połączenia sieciowe są kierowane poprzez dedykowany, zarządzany interfejs w celu audytu; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(15)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(15)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(15)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające routing uprzywilejowanych połączeń poprzez dedykowane, zarządzane interfejsy]. |

| | | |
|---|---|---|
| **SC-07(16)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| ZAPOBIEGANIE WYKRYWANIU KOMPONENTÓW SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(16)** | zapobiega się możliwości wykrycia konkretnych komponentów systemu, które reprezentują zarządzany interfejs. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-07(16)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| ZAPOBIEGANIE WYKRYWANIU KOMPONENTÓW SYSTEMU** | |
| | **SC-07(16)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(16)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(16)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zapobieganie wykrywaniu komponentów systemu w zarządzanych interfejsach]. |

| | | |
|---|---|---|
| **SC-07(17)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| AUTOMATYCZNE EGZEKWOWANIE FORMATÓW PROTOKOŁU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(17)** | egzekwuje się przestrzeganie formatów protokołów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(17)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-07(17)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| AUTOMATYCZNE EGZEKWOWANIE FORMATÓW PROTOKOŁU** | |
| | **SC-07(17)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(17)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające egzekwowanie przestrzegania formatów protokołów]. |

| | | |
|---|---|---|
| **SC-07(18)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \|BŁĄD BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(18)** | w przypadku awarii urządzenia do ochrony połączeń brzegowych uniemożliwia się systemom przejście w stan niezabezpieczony. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(18)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(18)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(18)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażanie zasady bezpiecznej awarii]. |

| | | |
|---|---|---|
| **SC-07(19)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| BLOKOWANIE KOMUNIKACJI Z HOSTAMI SPOZA ORGANIZACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(19)_ODP** | ***określono klientów komunikacyjnych, którzy są niezależnie konfigurowani przez użytkowników końcowych i zewnętrznych dostawców usług;*** |
| | **SC-07(19)[01]** | przychodzący ruch telekomunikacyjny pomiędzy ***<klientami komunikacyjnymi SC-07(19)_ODP>***, którzy są niezależnie konfigurowani przez użytkowników końcowych i zewnętrznych dostawców usług, jest blokowany; |
| | **SC-07(19)[02]** | wychodzący ruch telekomunikacyjny pomiędzy ***<klientami komunikacyjnymi SC-07(19)_ODP>***, którzy są niezależnie konfigurowani przez użytkowników końcowych i zewnętrznych dostawców usług, jest blokowany. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(19)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz klientów komunikacyjnych skonfigurowanych niezależnie przez użytkowników końcowych i zewnętrznych dostawców usług; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(19)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |

| | | |
|---|---|---|
| **SC-07(19)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| BLOKOWANIE KOMUNIKACJI Z HOSTAMI SPOZA ORGANIZACJI** | |
| | **SC-07(19)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające blokowanie ruchu komunikacyjnego przychodzącego i wychodzącego pomiędzy klientami komunikacyjnymi konfigurowanymi niezależnie przez użytkowników końcowych i zewnętrznych dostawców usług]. |

| | | |
|---|---|---|
| **SC-07(20)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| DYNAMICZNA IZOLACJA I SEGREGACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(20)_ODP** | ***określono komponenty systemu, które mają być dynamicznie izolowane od innych komponentów systemu;*** |
| | **SC-07(20)** | zapewniona jest możliwość dynamicznego izolowania ***<komponentów systemu SC-07(20)_ODP> od*** innych komponentów systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(20)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista komponentów systemu, które mają być dynamicznie izolowane/oddzielane od innych komponentów systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(20)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |

| | | |
|---|---|---|
| **SC-07(20)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| DYNAMICZNA IZOLACJA I SEGREGACJA** | |
| | **SC-07(20)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność do dynamicznego izolowania/oddzielania komponentów systemu]. |

| | | |
|---|---|---|
| **SC-07(21)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| IZOLACJA KOMPONENTÓW SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(21)_ODP[01]** | ***określono komponenty systemu, które mają być izolowane przez mechanizmy ochrony połączeń brzegowych;*** |
| | **SC-07(21)_ODP[02]** | ***określono misje lub funkcje biznesowe, które mają być wspierane przez komponenty systemu odizolowane za pomocą mechanizmów ochrony połączeń brzegowych;*** |
| | **SC-07(21)** | stosuje się mechanizmy ochrony połączeń brzegowych w celu odizolowania ***<komponentów systemu SC-07(21)_ODP[01]>*** wspierających ***<misje lub funkcje biznesowe SC-07(21)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(21)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; dokumentacja architektury korporacyjnej; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-07(21)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| IZOLACJA KOMPONENTÓW SYSTEMU** | |
| | **SC-07(21)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(21)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność do oddzielania komponentów systemu wspierających misję organizacji lub funkcje biznesowe]. |

| | | |
|---|---|---|
| **SC-07(22)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| ODDZIELNE PODSIECI DO PODŁĄCZENIA DO RÓŻNYCH DOMEN BEZPIECZEŃSTWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(22)** | wdrożono oddzielne adresy sieciowe w celu połączenia z systemami w różnych domenach bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(22)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(22)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |

| | | |
|---|---|---|
| **SC-07(22)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| ODDZIELNE PODSIECI DO PODŁĄCZENIA DO RÓŻNYCH DOMEN BEZPIECZEŃSTWA** | |
| | **SC-07(22)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające oddzielne adresy sieciowe/odrębne podsieci]. |

| | | |
|---|---|---|
| **SC-07(23)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| WYŁĄCZENIE INFORMACJI ZWROTNEJ NADAWCY W PRZYPADKU AWARII PROTOKOŁU UWIERZYTELNIAJĄCEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(23)** | informacja zwrotna dla nadawców jest wyłączona w przypadku niepowodzenia weryfikacji formatu protokołu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(23)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(23)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(23)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające wyłączenie informacji zwrotnej dla nadawców o niepowodzeniu weryfikacji formatu protokołu]. |

| | | |
|---|---|---|
| **SC-07(24)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| DANE OSOBOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(24)_ODP** | ***określono reguły przetwarzania dla systemów, które przetwarzają dane identyfikacyjne;*** |
| | **SC-07(24)(a)** | stosuje się ***<reguły przetwarzania SC-07(24)_ODP>*** w odniesieniu do elementów danych identyfikacyjnych w systemach, które przetwarzają takie dane; |
| | **SC-07(24)(b)[01]** | dozwolone procesy przetwarzania są monitorowane na zewnętrznych interfejsach systemów, które przetwarzają dane identyfikacyjne; |
| | **SC-07(24)(b)[02]** | dozwolone procesy przetwarzania są monitorowane na kluczowych wewnętrznych granicach systemów, które przetwarzają dane identyfikacyjne; |
| | **SC-07(24)(c)** | w przypadku systemów, które przetwarzają dane identyfikacyjne, dokumentuje się każdy wyjątek w zakresie przetwarzania; |
| | **SC-07(24)(d)[01]** | wyjątki stosowane w systemach przetwarzających dane identyfikacyjne są poddawane przeglądowi; |
| | **SC-07(24)(d)[02]** | w ramach systemów przetwarzających dane identyfikacyjne usuwa się wszelkie wyjątki, które nie są już obsługiwane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-07(24)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| DANE OSOBOWE** | |
| | **SC-07(24)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; polityka przetwarzania danych identyfikacyjnych; wykaz kluczowych wewnętrznych granic systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>dokumentacja architektury bezpieczeństwa i prywatności organizacji; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja dotycząca wykazu danych identyfikacyjnych; dokumentacja dotycząca mapowania danych; inne istotne dokumenty lub zapisy]. |
| | **SC-07(24)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(24)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające zdolności w zakresie ochrony połączeń brzegowych]. |

| | | |
|---|---|---|
| **SC-07(25)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| BEZPIECZNE POŁĄCZENIA KRAJOWYCH SYSTEMÓW JAWNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(25)_ODP[01]** | ***określono jawny, krajowy system bezpieczeństwa, który nie może bezpośrednio łączyć się z siecią zewnętrzną;*** |
| | **SC-07(25)_ODP[02]** | ***określono urządzenie chroniące granicę systemu, wymagane przy bezpośrednim łączeniu z siecią zewnętrzną;*** |

| | | |
|---|---|---|
| **SC-07(25)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| BEZPIECZNE POŁĄCZENIA KRAJOWYCH SYSTEMÓW JAWNYCH** | |
| | **SC-07(25)** | zabronione jest bezpośrednie łączenie się ***<jawnego, krajowego systemu bezpieczeństwa SC-07(25)_ODP[01]>*** z siecią zewnętrzną bez zastosowania ***<urządzenia chroniącego granicę systemu SC-07(25)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(25)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(25)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(25)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zakazujące bezpośredniego podłączania jawnych, krajowych systemów bezpieczeństwa do sieci zewnętrznej]. |

| | | |
|---|---|---|
| **SC-07(26)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| BEZPIECZNE POŁĄCZENIA KRAJOWYCH SYSTEMÓW NIEJAWNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(26)_ODP** | ***określono urządzenie chroniące granicę systemu, wymagane przy bezpośrednim łączeniu z siecią zewnętrzną;*** |

| | | |
|---|---|---|
| **SC-07(26)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| BEZPIECZNE POŁĄCZENIA KRAJOWYCH SYSTEMÓW NIEJAWNYCH** | |
| | **SC-07(26)** | zabronione jest bezpośrednie podłączanie niejawnego, krajowego systemu bezpieczeństwa do sieci zewnętrznej bez użycia ***<urządzenia chroniącego granicę systemu SC-07(26)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(26)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(26)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(26)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zakazujące bezpośredniego podłączania niejawnych, krajowych systemów bezpieczeństwa do sieci zewnętrznej]. |

| | | |
|---|---|---|
| **SC-07(27)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| BEZPIECZNE POŁĄCZENIA TRANSGRANICZNYCH SYSTEMÓW JAWNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(27)_ODP[01]** | ***określono jawny, transgraniczny system bezpieczeństwa, który nie może bezpośrednio łączyć się z siecią zewnętrzną;*** |

| | | |
|---|---|---|
| **SC-07(27)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| BEZPIECZNE POŁĄCZENIA TRANSGRANICZNYCH SYSTEMÓW JAWNYCH** | |
| | **SC-07(27)_ODP[02]** | ***określono urządzenie chroniące granicę systemu wymagane do celów bezpośredniego łączenia się jawnego, transgranicznego systemu bezpieczeństwa z siecią zewnętrzną;*** |
| | **SC-07(27)** | zabronione jest bezpośrednie łączenie się ***<jawnego, transgranicznego systemu bezpieczeństwa SC-07(27)_ODP[01]> z*** siecią zewnętrzną bez użycia ***<urządzenia chroniącego granicę systemu SC-07(27)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(27)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(27)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(27)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zakazujące bezpośredniego łączenia się jawnych, transgranicznych systemów bezpieczeństwa z sieciami zewnętrznymi]. |

| | | |
|---|---|---|
| **SC-07(28)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| POŁĄCZENIA Z SIECIAMI PUBLICZNYMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(28)_ODP** | ***określono system, w przypadku którego zakazano bezpośredniego łączenia się z siecią publiczną;*** |
| | **SC-07(28)** | w przypadku ***<systemu SC-07(28)_ODP>*** zabronione jest bezpośrednie podłączanie się do sieci publicznej. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(28)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(28)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(28)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zakazujące bezpośredniego łączenia się systemów z sieciami zewnętrznymi]. |

| | | |
|---|---|---|
| **SC-07(29)** | **OCHRONA POŁĄCZEŃ BRZEGOWYCH \| SEPARACJA PODSIECI W CELU ODIZOLOWANIA FUNKCJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-07(29)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {fizycznie; logicznie};*** |
| | **SC-07(29)_ODP[02]** | ***określono krytyczne komponenty i funkcje systemu, które mają być odizolowane;*** |
| | **SC-07(29)** | podsieci są oddzielone ***<WYBRANA WARTOŚĆ PARAMETRU SC-07(29)_ODP[01]>***, aby odizolować ***<krytyczne komponenty i funkcje systemu SC-07(29)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-07(29)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu; sprzęt i oprogramowanie systemowe; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; analiza krytyczności; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-07(29)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę połączeń brzegowych]. |
| | **SC-07(29)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy oddzielające krytyczne komponenty i funkcje systemu]. |

| | | |
|---|---|---|
| **SC-08** | **POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-08_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {poufność; integralność};*** |
| | **SC-08** | ***<WYBRANA WARTOŚĆ PARAMETRU SC-08_ODP>*** przekazywanych informacji jest chroniona. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące poufności i integralności transmisji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-08-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-08-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające poufność lub integralność transmisji]. |

| | | |
|---|---|---|
| **SC-08(01)** | **POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI \| OCHRONA KRYPTOGRAFICZNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-08(01)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {zapobieganie nieautoryzowanemu ujawnianiu informacji; wykrywanie zmian w informacjach};*** |

| SC-08(01) | POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI \| OCHRONA KRYPTOGRAFICZNA | |
|---|---|---|
| | **SC-08(01)** | podczas transmisji wdrażane są mechanizmy kryptograficzne w ***<WYBRANA WARTOŚC PARAMETRU SC-08(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-08(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące poufności i integralności transmisji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-08(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-08(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne wspierające lub wdrażające poufność lub integralność transmisji; mechanizmy wspierające lub wdrażające alternatywne zabezpieczenia fizyczne; procesy organizacyjne dotyczące definiowania i wdrażania alternatywnych zabezpieczeń fizycznych]. |

| SC-08(02) | POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI \| OBSŁUGA „PRZED" i „PO" TRANSMISJI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-08(02)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{poufność; integralność};*** |
| | **SC-08(02)[01]** | informacje ***<WYBRANA WARTOŚĆ PARAMETRU SC-08(02)_ODP>*** są zachowywane podczas przygotowania do transmisji; |

| | | |
|---|---|---|
| **SC-08(02)** | **POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI \| OBSŁUGA „PRZED" i „PO" TRANSMISJI** | |
| | **SC-08(02)[02]** | informacje ***<WYBRANA WARTOŚĆ PARAMETRU SC-08(02)_ODP>*** są zachowywane podczas odbioru. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-08(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące poufności i integralności transmisji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-08(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-08(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające poufność lub integralność transmisji]. |

| | | |
|---|---|---|
| **SC-08(03)** | **POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI \| OCHRONA KRYPTOGRAFICZNA ZEWNĘTRZNYCH KOMUNIKATÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-08(03)_ODP** | ***określono alternatywne, fizyczne zabezpieczenia chroniące zewnętrzne komunikaty;*** |
| | **SC-08(03)** | wdrożono mechanizmy kryptograficzne w celu ochrony zewnętrznych komunikatów, chyba że są one chronione w inny sposób przez ***<alternatywne zabezpieczenia fizyczne SC-08(03)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-08(03)** | **POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI \| OCHRONA KRYPTOGRAFICZNA ZEWNĘTRZNYCH KOMUNIKATÓW** | |
| | **SC-08(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące poufności i integralności transmisji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-08(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-08(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne wspierające lub wdrażające poufność lub integralność transmisji zewnętrznych komunikatów; mechanizmy wspierające lub wdrażające alternatywne zabezpieczenia fizyczne; procesy organizacyjne w zakresie definiowania i wdrażania alternatywnych zabezpieczeń fizycznych]. |

| | | |
|---|---|---|
| **SC-08(04)** | **POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI \| KOMUNIKACJA UKRYTA/LOSOWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-08(04)_ODP** | ***określono alternatywne zabezpieczenia fizyczne, chroniące przed nieuprawnionym ujawnieniem schematów komunikacji;*** |
| | **SC-08(04)** | wdrażanie mechanizmów kryptograficznych w celu ukrycia lub nadania losowości schematom komunikacji, chyba że są one w inny sposób chronione przez ***<alternatywne zabezpieczenia fizyczne SC-08(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-08(04)** | **POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI \| KOMUNIKACJA UKRYTA/LOSOWA** | |
| | **SC-08(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące poufności i integralności transmisji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-08(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-08(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne wspierające lub wdrażające poufność lub integralność transmisji w zakresie komunikatów zewnętrznych; mechanizmy wspierające lub wdrażające alternatywne zabezpieczenia fizyczne; procesy organizacyjne w zakresie definiowania i wdrażania alternatywnych zabezpieczeń fizycznych]. |

| | | |
|---|---|---|
| **SC-08(05)** | **POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI \|CHRONIONY SYSTEM DYSTRYBUCJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-08(05)_ODP[01]** | ***określono chroniony system dystrybucji;*** |
| | **SC-08(05)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {zapobieganie nieautoryzowanemu ujawnianiu informacji; wykrywanie zmian w informacjach};*** |
| | **SC-08(05)** | wdrożono ***<chroniony system dystrybucji SC-08(05)_ODP[01]> w*** celu ***<WYBRANA WARTOŚĆ PARAMETRU SC-08(05)_ODP[02]>*** podczas transmisji. |

| | | |
|---|---|---|
| **SC-08(05)** | **POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI \|CHRONIONY SYSTEM DYSTRYBUCJI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-08(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące poufności i integralności transmisji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-08(05)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-08(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne wspomagające lub wdrażające ukrywanie lub randomizowanie schematów komunikacji; mechanizmy wspomagające lub wdrażające chronione systemy dystrybucji]. |

| | | |
|---|---|---|
| **SC-09** | **POUFNOŚĆ TRANSMISJI** | |
| | [WYCOFANE: Włączone do SC-08]. | |

| | | |
|---|---|---|
| **SC-10** | **ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-10_ODP** | ***określono czas bezczynności, po którym system kończy połączenie sieciowe związane z sesją komunikacyjną;*** |
| | **SC-10** | połączenie sieciowe związane z sesją komunikacyjną zostaje zakończone na koniec sesji lub po upływie ***<okresu bezczynności SC-10_ODP>***. |

| | | |
|---|---|---|
| **SC-10** | **ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące zakończenia połączenia sieciowego; dokumentacja projektowa systemu; plan bezpieczeństwa; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-10-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-10-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność do zakończenia połączenia sieciowego]. |

| | | |
|---|---|---|
| **SC-11** | **ZAUFANA ŚCIEŻKA KOMUNIKACYJNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-11_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {fizycznie; logicznie};*** |
| | **SC-11_ODP[02]** | ***określono funkcje bezpieczeństwa systemu;*** |
| | **SC-11a.** | do celów komunikacji pomiędzy użytkownikiem a zaufanymi komponentami systemu zapewniona jest izolowana, zaufana ścieżka komunikacyjna **<*WYBRANA WARTOŚĆ PARAMETRU SC-11_ODP[01]*>**; |

| | | |
|---|---|---|
| **SC-11** | **ZAUFANA ŚCIEŻKA KOMUNIKACYJNA** | |
| | **SC-11b.** | użytkownicy mają możliwość wykorzystania zaufanej ścieżki komunikacyjnej do celów komunikacji z ***<funkcjami bezpieczeństwa SC-11_ODP[02]>*** systemu, w tym co najmniej uwierzytelniania i ponownego uwierzytelniania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-11-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące zaufanych ścieżek komunikacyjnych; plan bezpieczeństwa; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wyniki oceny dokonanej przez niezależne organizacje badawcze; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-11-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-11-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zaufane ścieżki komunikacyjne]. |

| | | |
|---|---|---|
| **SC-11(01)** | **ZAUFANA ŚCIEŻKA KOMUNIKACYJNA\| NIEPODWAŻALNA ŚCIEŻKA KOMUNIKACYJNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-11(01)_ODP** | ***określono funkcje bezpieczeństwa systemu;*** |
| | **SC-11(01)(a)** | zapewniona jest zaufana ścieżka komunikacyjna, która jest w sposób niepodważalny odróżnialna od innych ścieżek komunikacyjnych; |

| | | |
|---|---|---|
| **SC-11(01)** | **ZAUFANA ŚCIEŻKA KOMUNIKACYJNA\| NIEPODWAŻALNA ŚCIEŻKA KOMUNIKACYJNA** | |
| | **SC-11(01)(b)** | do celów komunikacji pomiędzy ***<funkcjami bezpieczeństwa SC-11(01)_ODP>*** systemu a użytkownikiem inicjowana jest zaufana ścieżka komunikacyjna. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-11(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące zaufanych ścieżek komunikacyjnych; plan bezpieczeństwa; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wyniki oceny dokonanej przez niezależne organizacje badawcze; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-11(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-11(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zaufane ścieżki komunikacyjne]. |

| | | |
|---|---|---|
| **SC-12** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-12_ODP** | ***określono wymagania dotyczące generowania, dystrybucji, przechowywania, dostępu i niszczenia kluczy;*** |
| | **SC-12[01]** | klucze kryptograficzne są tworzone w przypadku stosowania w systemie kryptografii zgodnie z ***<wymogami SC-12_ODP>***; |

| | | |
|---|---|---|
| **SC-12** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI** | |
| | **SC-12[02]** | klucze kryptograficzne są zarządzane w przypadku stosowania w systemie kryptografii zgodnie z ***<wymogami SC-12_ODP>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-12-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ustanawiania kluczy kryptograficznych i zarządzania nimi; dokumentacja projektowa systemu; mechanizmy kryptograficzne; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-12-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za tworzenie kluczy kryptograficznych lub zarządzanie nimi]. |
| | **SC-12-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające tworzenie i zarządzanie kluczami kryptograficznymi]. |

| | | |
|---|---|---|
| **SC-12(01)** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI \| DOSTĘPNOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-12(01)** | dostępność informacji jest zachowana w przypadku utraty kluczy kryptograficznych przez użytkowników. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-12(01)** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI \| DOSTĘPNOŚĆ** | |
| | **SC-12(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ustanawiania kluczy kryptograficznych, zarządzania nimi i ich odzyskiwania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-12(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za tworzenie kluczy kryptograficznych lub zarządzanie nimi]. |
| | **SC-12(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające tworzenie i zarządzanie kluczami kryptograficznymi]. |

| | | |
|---|---|---|
| **SC-12(02)** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI \| KLUCZE SYMETRYCZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-12(02)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {zatwierdzone przez organizację; zatwierdzone przez krajową władzę bezpieczeństwa};*** |
| | **SC-12(02)[01]** | symetryczne klucze kryptograficzne są ustanawiane przy użyciu technologii i procesów zarządzania kluczami ***<WYBRANA WARTOŚĆ PARAMETRU SC-12(02)_ODP>***; |
| | **SC-12(02)[02]** | symetryczne klucze kryptograficzne są zarządzane przy użyciu technologii i procesów zarządzania kluczami ***<WYBRANA WARTOŚĆ PARAMETRU SC-12(02)_ODP>***; |

| | | |
|---|---|---|
| **SC-12(02)** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI \| KLUCZE SYMETRYCZNE** | |
| | **SC-12(02)[03]** | symetryczne klucze kryptograficzne są dystrybuowane przy użyciu technologii i procesów zarządzania kluczami ***<WYBRANA WARTOŚĆ PARAMETRU SC-12(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-12(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ustanawiania kluczy kryptograficznych i zarządzania nimi; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; wykaz produktów kryptograficznych zatwierdzonych przez organizację; wykaz produktów kryptograficznych zatwierdzonych przez krajową władzę bezpieczeństwa; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-12(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za tworzenie lub zarządzanie kluczami kryptograficznymi]. |
| | **SC-12(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające ustanawianie i zarządzanie symetrycznymi kluczami kryptograficznymi]. |

| | | |
|---|---|---|
| **SC-12(03)** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI \| KLUCZE ASYMETRYCZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-12(03)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {technologia i procesy zarządzania kluczami zatwierdzone przez organizację; wstępnie przygotowany materiał klucza; zatwierdzone lub wydane certyfikaty infrastruktury klucza publicznego klasy 3; zatwierdzone lub wydane certyfikaty infrastruktury sprzętowej klucza publicznego klasy 3 oraz tokeny bezpieczeństwa sprzętowego, które chronią klucz prywatny użytkownika; certyfikaty wydane zgodnie z wymaganiami określonymi przez organizację};*** |
| | **SC-12(03)[01]** | asymetryczne klucze kryptograficzne są ustanawiane z zastosowaniem ***<WYBRANA WARTOŚĆ PARAMETRU SC-12(03)_ODP>***; |
| | **SC-12(03)[02]** | asymetryczne klucze kryptograficzne są zarządzane z zastosowaniem ***<WYBRANA WARTOŚĆ PARAMETRU SC-12(03)_ODP>***; |
| | **SC-12(03)[03]** | asymetryczne klucze kryptograficzne są dystrybuowane z zastosowaniem ***<WYBRANA WARTOŚĆ PARAMETRU SC-12(03)_ODP>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-12(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ustanawiania kluczy kryptograficznych i zarządzania nimi; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; wykaz zatwierdzonych przez organizację produktów kryptograficznych; wykaz zatwierdzonych certyfikatów infrastruktury klucza publicznego klasy 3 i klasy 4; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-12(03)** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI \| KLUCZE ASYMETRYCZNE** | |
| | **SC-12(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za tworzenie lub zarządzanie kluczami kryptograficznymi; personel organizacyjny odpowiedzialny za certyfikaty infrastruktury klucza publicznego]. |
| | **SC-12(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające tworzenie i zarządzanie asymetrycznymi kluczami kryptograficznymi]. |

| | |
|---|---|
| **SC-12(04)** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI \| CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO** |
| | [WYCOFANE: Włączone do SC-12(03)]. |

| | |
|---|---|
| **SC-12(05)** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI \| CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO/TOKENY SPRZĘTOWE** |
| | [WYCOFANE: Włączone do SC-12(03)]. |

| | | |
|---|---|---|
| **SC-12(06)** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI \| FIZYCZNE ZABEZPIECZENIE KLUCZY KRYPTOGRAFICZNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-12(06)** | klucze kryptograficzne są fizycznie zabezpieczane, jeżeli przechowywane informacje są szyfrowane przez zewnętrznych dostawców usług. |

| | | |
|---|---|---|
| **SC-12(06)** | **GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI \| FIZYCZNE ZABEZPIECZENIE KLUCZY KRYPTOGRAFICZNYCH** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-12(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ustanawiania kluczy kryptograficznych, zarządzania nimi i ich odzyskiwania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-12(06)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za tworzenie kluczy kryptograficznych lub zarządzanie nimi]. |
| | **SC-12(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające tworzenie i zarządzanie kluczami kryptograficznymi]. |

| | | |
|---|---|---|
| **SC-13** | **OCHRONA KRYPTOGRAFICZNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-13_ODP[01]** | ***określono zastosowania kryptograficzne;*** |
| | **SC-13_ODP[02]** | ***określono rodzaje kryptografii wymagane dla każdego określonego zastosowania kryptograficznego;*** |
| | **SC-13a.** | określono ***<zastosowania kryptograficzne SC-13_ODP[01]>***; |

| | | |
|---|---|---|
| **SC-13** | **OCHRONA KRYPTOGRAFICZNA** | |
| | **SC-13b.** | dla każdego określonego zastosowania kryptograficznego (zdefiniowanego w SC-13_ODP[01]) wdrożone są ***<rodzaje kryptografii SC-13_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-13-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony kryptograficznej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; certyfikaty zatwierdzania modułów kryptograficznych; lista modułów kryptograficznych zatwierdzonych przez organizację; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-13-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za ochronę kryptograficzną]. |
| | **SC-13-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające ochronę kryptograficzną]. |

| | |
|---|---|
| **SC-13(01)** | **OCHRONA KRYPTOGRAFICZNA \| KRYPTOGRAFIA KOMERCYJNA** |
| | [WYCOFANE: Włączone do SC-13]. |

| | |
|---|---|
| **SC-13(02)** | **OCHRONA KRYPTOGRAFICZNA \| KRYPTOGRAFIA ZATWIERDZONA PRZEZ KRAJOWĄ WŁADZĘ BEZPIECZEŃSTWA** |
| | [WYCOFANE: Włączone do SC-13]. |

| | |
|---|---|
| **SC-13(03)** | **OCHRONA KRYPTOGRAFICZNA \| OSOBY BEZ FORMALNYCH ZATWIERDZEŃ DOSTĘPU** |
| | [WYCOFANE: Włączone do SC-13]. |

| | |
|---|---|
| **SC-13(04)** | **OCHRONA KRYPTOGRAFICZNA \| PODPISY CYFROWE** |
| | [WYCOFANE: Włączone do SC-13]. |

| | |
|---|---|
| **SC-14** | **OCHRONA DOSTĘPU PUBLICZNEGO** |
| | [WYCOFANE: Włączone do AC-02, AC-03, AC-05, AC-06, SI-03, SI-04, SI-05, SI-07, SI-10]. |

| | | |
|---|---|---|
| **SC-15** | **WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-15_ODP** | ***określono wyjątki, w których dozwolona jest zdalne uruchamianie;*** |
| | **SC-15a.** | zabrania się zdalnego uruchamiania urządzeń i aplikacji do pracy zespołowej, z wyłączeniem ***<wyjątków, w których zdalne uruchamianie ma być dozwolone SC-15_ODP>***; |
| | **SC-15b.** | użytkownikom fizycznie pracującym na urządzeniach przekazywana jest jednoznaczna informacja o sposobie ich użytkowania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-15** | **WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE** | |
| | **SC-15-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące pracy zespołowej; polityka i procedury zabezpieczenia dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-15-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za zarządzanie komputerowymi urządzeniami do pracy zespołowej]. |
| | **SC-15-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zarządzanie zdalną aktywacją komputerowych urządzeń do pracy zespołowej; mechanizmy zapewniające jednoznaczną informację o sposobie użytkowania urządzeń do pracy zespołowej]. |

| | | |
|---|---|---|
| **SC-15(01)** | **WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE \|ODŁĄCZENIE FIZYCZNE LUB LOGICZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-15(01)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {fizyczne; logiczne};*** |
| | **SC-15(01)** | odłączenie urządzeń komputerowych do pracy zespołowej ***<WYBRANA WARTOŚĆ PARAMETRU SC-15(01)_ODP>*** jest realizowane w sposób ułatwiający obsługę. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-15(01)** | **WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE \|ODŁĄCZENIE FIZYCZNE LUB LOGICZNE** | |
| | **SC-15(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące pracy zespołowej; polityka i procedury zabezpieczenia dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-15(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za zarządzanie komputerowymi urządzeniami do pracy zespołowej]. |
| | **SC-15(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające fizyczne odłączenie urządzeń do pracy zespołowej]. |

| | | |
|---|---|---|
| **SC-15(02)** | **WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE \| BLOKOWANIE RUCHU WEJŚCIOWEGO/WYJŚCIOWEGO** | |
| | [WYCOFANE: Włączone do SC-07]. | |

| | | |
|---|---|---|
| **SC-15(03)** | **WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE \| DEZAKTYWACJA/USUWANIE W CHRONIONYCH OBSZARACH PRACY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-15(03)_ODP[01]** | ***określono systemy lub komponenty systemu, w przypadku których urządzenia komputerowe do pracy zespołowej mają być wyłączone lub usunięte;*** |

| | | |
|---|---|---|
| **SC-15(03)** | **WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE \| DEZAKTYWACJA/USUWANIE W CHRONIONYCH OBSZARACH PRACY** | |
| | **SC-15(03)_ODP[02]** | ***określono chronione obszary pracy, w przypadku których urządzenia komputerowe do pracy zespołowej mają być wyłączone lub usunięte z systemu lub komponentów systemu;*** |
| | **SC-15(03)** | urządzenia i aplikacje do pracy zespołowej są wyłączane lub usuwane z ***<systemów lub komponentów systemów SC-15(03)_ODP[01]>*** ***w <bezpiecznych obszarach pracy SC-15(03)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-15(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące pracy zespołowej; polityka i procedury kontroli dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; wykaz bezpiecznych obszarów roboczych; systemy lub komponenty systemu w bezpiecznych obszarach roboczych, w przypadku których urządzenia do pracy zespołowej mają być mają być wyłączone lub usunięte; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-15(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie urządzeniami komputerowymi do pracy zespołowej]. |
| | **SC-15(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie wyłączania urządzeń do pracy zespołowej]. |

| | | |
|---|---|---|
| **SC-15(04)** | **WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE \| WYRAŹNIE WYKAZANIE AKTUALNYCH UŻYTKOWNIKÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-15(04)_ODP** | ***określono spotkania online i telekonferencje, w przypadku których należy jednoznacznie wskazać aktualnych uczestników;*** |
| | **SC-15(04)** | aktualni uczestnicy ***<spotkań online i telekonferencji SC-15(04)_ODP>*** są wyraźnie wskazywani. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-15(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące pracy zespołowej; polityka i procedury kontroli dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>zapisy z audytu systemu; wykaz rodzajów spotkań i telekonferencji wymagających wyraźnego wskazania aktualnych uczestników; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-15(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie urządzeniami do pracy zespołowej]. |
| | **SC-15(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające możliwość wskazywania uczestników spotkań/telekonferencji na urządzeniach do pracy zespołowej]. |

| | | |
|---|---|---|
| **SC-16** | **TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-16_ODP[01]** | ***określono atrybuty bezpieczeństwa, które mają być powiązane z wymienianymi informacjami;*** |
| | **SC-16_ODP[02]** | ***określono atrybuty prywatności, które mają być powiązane z wymienianymi informacjami;*** |
| | **SC-16[01]** | ***<atrybuty bezpieczeństwa SC-16_ODP[01]>*** są powiązane z informacjami wymienianymi pomiędzy systemami; |
| | **SC-16[02]** | ***<atrybuty bezpieczeństwa SC-16_ODP[01]>*** są powiązane z informacjami wymienianymi pomiędzy komponentami systemu; |
| | **SC-16[03]** | ***<atrybuty prywatności SC-16_ODP[02]>*** są powiązane z informacjami wymienianymi pomiędzy systemami; |
| | **SC-16[04]** | ***<atrybuty prywatności SC-16_ODP[02]>*** są powiązane z informacjami wymienianymi pomiędzy komponentami systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-16-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące przekazywania atrybutów bezpieczeństwa i prywatności; polityka i procedury kontroli dostępu; polityka kontroli przepływu informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SC-16-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **SC-16** | **TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **SC-16-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające transmisję atrybutów bezpieczeństwa i prywatności pomiędzy systemami]. |

| | | |
|---|---|---|
| **SC-16(01)** | **TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| WERYFIKACJA INTEGRALNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-16(01)[01]** | integralność przesyłanych atrybutów bezpieczeństwa jest weryfikowana; |
| | **SC-16(01)[02]** | integralność przesyłanych atrybutów prywatności jest weryfikowana. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-16(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemu i sieci telekomunikacyjnych; procedury dotyczące przesyłania atrybutów bezpieczeństwa i prywatności; polityka i procedury kontroli dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SC-16(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SC-16(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające weryfikację integralności przekazywanych atrybutów bezpieczeństwa i prywatności]. |

| | | |
|---|---|---|
| **SC-16(02)** | **TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| MECHANIZMY ANTYSPOOFINGOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-16(02)** | wdrożono mechanizmy antyspoofingowe, aby uniemożliwić atakującym fałszowanie atrybutów bezpieczeństwa wskazujących na pomyślne zastosowanie procesu bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-16(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące przesyłania atrybutów bezpieczeństwa i prywatności; polityka i procedury kontroli dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-16(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SC-16(02)-Test** | [WYBÓR SPOŚRÓD: Administratorzy systemów/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SC-16(03)** | **TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| POWIĄZANIE KRYPTOGRAFICZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-16(03)_ODP** | ***określono mechanizmy lub techniki stosowane w celu powiązania atrybutów bezpieczeństwa i prywatności z przesyłanymi informacjami;*** |
| | **SC-16(03)** | wdrożono ***<mechanizmy lub techniki SC-16(03)_ODP>*** w celu powiązania atrybutów bezpieczeństwa i prywatności z przesyłanymi informacjami. |

| | | |
|---|---|---|
| **SC-16(03)** | **TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| POWIĄZANIE KRYPTOGRAFICZNE** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-16(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące przesyłania atrybutów bezpieczeństwa i prywatności; polityka i procedury kontroli dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-16(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SC-16(03)-Test** | [WYBÓR SPOŚRÓD: Administratorzy systemów/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SC-17** | **CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-17_ODP** | ***określono politykę wydawania certyfikatów klucza publicznego;*** |
| | **SC-17a.** | certyfikaty klucza publicznego są wydawane zgodnie z ***<polityką certyfikatów SC-17_ODP>*** lub są uzyskiwane od zatwierdzonego dostawcy usług; |
| | **SC-17b.** | tylko zatwierdzone kotwice zaufania są włączane do magazynów zaufania lub magazynów certyfikatów zarządzanych przez organizację. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-17** | **CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO** | |
| | **SC-17-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące certyfikatów infrastruktury klucza publicznego; polityka lub polityki dotyczące certyfikatów klucza publicznego; proces wydawania klucza publicznego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-17-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za wydawanie certyfikatów klucza publicznego; dostawcy usług]. |
| | **SC-17-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zarządzanie certyfikatami infrastruktury klucza publicznego]. |

| | | |
|---|---|---|
| **SC-18** | **KOD MOBILNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-18a.[01]** | określono dopuszczalny kod mobilny; |
| | **SC-18a.[02]** | określono niedopuszczalny kod mobilny; |
| | **SC-18a.[03]** | określono dopuszczalne technologie kodów mobilnych; |
| | **SC-18a.[04]** | określono niedopuszczalne technologie kodów mobilnych; |
| | **SC-18b.[01]** | użycie kodu mobilnego w systemie jest dozwolone; |
| | **SC-18b.[02]** | użycie kodu mobilnego w systemie jest monitorowane; |
| | **SC-18b.[03]** | użycie kodu mobilnego w systemie jest kontrolowane; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **SC-18** | **KOD MOBILNY** | |
|---|---|---|
| | **SC-18-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące kodu mobilnego; polityka i procedury wdrażania kodu mobilnego; wykaz dopuszczalnych kodów mobilnych i technologii kodów mobilnych; wykaz niedopuszczalnych kodów mobilnych i technologii mobilnych; zapisy dotyczące zatwierdzania; zapisy dotyczące monitorowania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-18-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie kodem mobilnym]. |
| | **SC-18-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny dotyczący zatwierdzania, monitorowania i zabezpieczania kodu mobilnego; mechanizmy wspierające lub wdrażające proces zarządzania kodem mobilnym; mechanizmy wspierające lub wdrażające monitorowanie kodu mobilnego]. |

| **SC-18(01)** | **KOD MOBILNY \| IDENTYFIKACJA NIEDOPUSZCZALNEGO KODU / PODEJMOWANIE DZIAŁAŃ NAPRAWCZYCH** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-18(01)_ODP[01]** | ***określono niedopuszczalny kod mobilny, który należy identyfikować;*** |
| | **SC-18(01)_ODP[02]** | ***określono działania naprawcze, które należy podjąć w przypadku zidentyfikowania niedopuszczalnego kodu mobilnego;*** |
| | **SC-18(01)[01]** | ***<niedopuszczalny kod mobilny SC-18(01)_ODP[01]>*** jest identyfikowany; |

| | | |
|---|---|---|
| **SC-18(01)** | **KOD MOBILNY \| IDENTYFIKACJA NIEDOPUSZCZALNEGO KODU / PODEJMOWANIE DZIAŁAŃ NAPRAWCZYCH** | |
| | **SC-18(01)[02]** | ***<działania naprawcze SC-18(01)_ODP[02]>*** są podejmowane w przypadku zidentyfikowania nieakceptowalnego kodu mobilnego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-18(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące kodu mobilnego; ograniczenia w wykorzystaniu kodu mobilnego; polityka i procedury wdrażania kodu mobilnego; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz niedopuszczalnego kodu mobilnego; wykaz działań naprawczych podejmowanych w przypadku zidentyfikowania niedopuszczalnego kodu mobilnego; zapisy dotyczące monitorowania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-18(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za zarządzanie kodem mobilnym]. |
| | **SC-18(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania i kontroli kodu mobilnego oraz działań naprawczych]. |

| | | |
|---|---|---|
| **SC-18(02)** | **KOD MOBILNY \| NABYCIE/OPRACOWYWANIE/UŻYTKOWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-18(02)_ODP** | ***określono wymagania w zakresie pozyskiwania, rozwoju i wykorzystania kodu mobilnego, który ma być wdrożony w systemie;*** |

| | | |
|---|---|---|
| **SC-18(02)** | **KOD MOBILNY \| NABYCIE/OPRACOWYWANIE/UŻYTKOWANIE** | |
| | **SC-18(02)[01]** | proces pozyskiwania kodu mobilnego przeznaczonego do wdrożenia w systemie spełnia<br>***<wymagania dotyczące kodu mobilnego SC-18(02)_ODP>***; |
| | **SC-18(02)[02]** | proces opracowywania kodu mobilnego przeznaczonego do wdrożenia w systemie spełnia<br>***<wymagania dotyczące kodu mobilnego SC-18(02)_ODP>***; |
| | **SC-18(02)[03]** | proces wykorzystania kodu mobilnego przeznaczonego do wdrożenia w systemie spełnia ***<wymagania dotyczące kodu mobilnego SC-18(02)_ODP>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-18(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące kodu mobilnego; wymagania dotyczące kodu mobilnego; ograniczenia w wykorzystaniu kodu mobilnego; polityka i procedury wdrażania kodu mobilnego; dokumentacja dotycząca nabywania; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja cyklu życia rozwoju systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-18(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie kodem mobilnym; personel organizacyjny odpowiedzialny za pozyskiwanie i zawieranie umów]. |
| | **SC-18(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące pozyskiwania, rozwoju i wykorzystania kodu mobilnego]. |

| | | |
|---|---|---|
| **SC-18(03)** | **KOD MOBILNY \| ZAPOBIEGANIE POBIERANIU I WYKONYWANIU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-18(03)_ODP** | ***określono niedopuszczalny kod mobilny, którego pobranie i wykonanie należy uniemożliwić;*** |
| | **SC-18(03)[01]** | pobieranie ***<nieakceptowalnego kodu mobilnego SC-18(03)_ODP>*** jest uniemożliwione; |
| | **SC-18(03)[02]** | wykonywanie***<nieakceptowalnego kodu mobilnego SC-18(03)_ODP>*** jest uniemożliwione. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-18(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące kodu mobilnego; ograniczenia w wykorzystaniu kodu mobilnego; polityka i procedury wdrażania kodu mobilnego; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-18(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za zarządzanie kodem mobilnym]. |
| | **SC-18(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zapobiegające pobieraniu i wykonywaniu nieakceptowalnego kodu mobilnego]. |

| | | |
|---|---|---|
| **SC-18(04)** | **KOD MOBILNY \| ZAPOBIEGANIE AUTOMATYCZNEMU WYKONANIU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-18(04)_ODP[01]** | ***określono aplikacje, w których należy zapobiegać automatycznemu wykonywaniu kodu mobilnego;*** |
| | **SC-18(04)_ODP[02]** | ***określono działania wymuszane przez system przed wykonaniem kodu mobilnego;*** |
| | **SC-18(04)[01]** | uniemożliwiono automatyczne wykonywanie kodu mobilnego w ***<aplikacjach SC-18(04)_ODP[01]>***; |
| | **SC-18(04)[02]** | przed wykonaniem kodu mobilnego system wymusza wykonanie ***<działań SC-18(04)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-18(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące kodu mobilnego; ograniczenia w wykorzystaniu kodu mobilnego; polityka i procedury wdrażania kodu mobilnego; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista aplikacji, w których automatyczne wykonywanie kodu mobilnego musi być zabronione; lista czynności wymaganych przed wykonaniem kodu mobilnego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-18(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za zarządzanie kodem mobilnym]. |

| | | |
|---|---|---|
| **SC-18(04)** | **KOD MOBILNY \| ZAPOBIEGANIE AUTOMATYCZNEMU WYKONANIU** | |
| | **SC-18(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy zapobiegające automatycznemu wykonywaniu nieakceptowalnego kodu mobilnego; mechanizmy wymuszające podjęcie działań przed wykonaniem kodu mobilnego]. |

| | | |
|---|---|---|
| **SC-18(05)** | **KOD MOBILNY \| POZWALANIE NA WYKONANIE TYLKO W OGRANICZONYCH ŚRODOWISKACH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-18(05)** | wykonanie dopuszczalnego kodu mobilnego jest dozwolone tylko w ograniczonych środowiskach maszyn wirtualnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-18(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące kodu mobilnego; uprawnienia do wykorzystania kodu mobilnego; ograniczenia w wykorzystaniu kodu mobilnego; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista ograniczonych środowisk maszyn wirtualnych, w których dozwolone jest wykonywanie dopuszczalnego przez organizację kodu mobilnego; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-18(05)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny odpowiedzialny za zarządzanie kodem mobilnym]. |

| | | |
|---|---|---|
| **SC-18(05)** | **KOD MOBILNY \| POZWALANIE NA WYKONANIE TYLKO W OGRANICZONYCH ŚRODOWISKACH** | |
| | **SC-18(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy umożliwiające wykonywanie dozwolonego kodu mobilnego w ograniczonych środowiskach maszyn wirtualnych]. |

| | |
|---|---|
| **SC-19** | **PROTOKÓŁ TRANSMISJI PAKIETOWEJ (VOIP)** |
| | [WYCOFANE. Specyficzne dla danej technologii; adresowane jak każda inna technologia lub protokół]. |

| | | |
|---|---|---|
| **SC-20** | **BEZPIECZEŃSTWO NAZW DOMEN/ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-20a.[01]** | wraz z autorytatywnymi danymi dotyczącymi rozpoznawania nazwy, które system zwraca w odpowiedzi na zewnętrzne zapytania dotyczące rozpoznawania nazwy/adresu, dostarczane są dodatkowe artefakty uwierzytelniania pochodzenia danych; |
| | **SC-20a.[02]** | wraz z autorytatywnymi danymi dotyczącymi rozpoznawania nazwy, które system zwraca w odpowiedzi na zewnętrzne zapytania dotyczące rozpoznawania nazwy/adresu, dostarczane są dodatkowe artefakty weryfikacji integralności; |
| | **SC-20b.[01]** | w przypadku działania w ramach rozproszonej, hierarchicznej przestrzeni nazw zapewnione są środki wskazujące status bezpieczeństwa stref podrzędnych (oraz to, czy taka strefa zapewnia obsługę zabezpieczeń); |

| | | |
|---|---|---|
| **SC-20** | **BEZPIECZEŃSTWO NAZW DOMEN/ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)** | |
| | **SC-20b.[02]** | w przypadku działania w ramach rozproszonej, hierarchicznej przestrzeni nazw zapewnione są środki wskazujące status bezpieczeństwa stref podrzędnych (oraz to, czy taka strefa zapewnia obsługę zabezpieczeń) w celu umożliwienia weryfikacji łańcucha zaufania między domenami nadrzędnymi i podrzędnymi. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-20-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące bezpiecznych usług uwierzytelniania pochodzenia nazw/adresów (autentyczność pochodzenia); dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-20-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie serwerami DNS]. |
| | **SC-20-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające bezpieczne usługi uwierzytelniania pochodzenia nazw/adresów]. |

| | |
|---|---|
| **SC-20(01)** | **BEZPIECZEŃSTWO NAZW DOMEN/ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)\| STREFA PODRZĘDNA (PODPRZESTRZEŃ)** |
| | [WYCOFANE: Włączone do SC-20]. |

| | | |
|---|---|---|
| **SC-20(02)** | **BEZPIECZEŃSTWO NAZW DOMEN/ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA) \| INTEGRALNOŚĆ DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-20(02)[01]** | w przypadku wewnętrznych zapytań dotyczących uwierzytelniania pochodzenia nazw/adresów dostarczane są artefakty dotyczące pochodzenia danych; |
| | **SC-20(02)[02]** | w przypadku wewnętrznych zapytań dotyczących uwierzytelniania pochodzenia nazw/adresów dostarczane są artefakty dotyczące ochrony integralności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-20(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące bezpiecznych usług uwierzytelniania pochodzenia nazw/adresów (autentyczność pochodzenia); dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-20(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie serwerami DNS]. |
| | **SC-20(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające ochronę pochodzenia i integralności danych dla wewnętrznych zapytań o usługi uwierzytelniania pochodzenia nazw/adresów]. |

| | | |
|---|---|---|
| **SC-21** | **BEZPIECZEŃSTWO NAZW DOMEN/USŁUGA USTALANIA ADRESU IP** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-21[01]** | w przypadku odpowiedzi dotyczących uwierzytelniania pochodzenia nazw/adresów, które system otrzymuje z wiarygodnych źródeł, wymagana jest weryfikacja autentyczności danych; |
| | **SC-21[02]** | w przypadku odpowiedzi dotyczących uwierzytelniania pochodzenia nazw/adresów, które system otrzymuje z wiarygodnych źródeł, przeprowadzana jest weryfikacja autentyczności danych; |
| | **SC-21[03]** | w przypadku odpowiedzi dotyczących uwierzytelniania pochodzenia nazw/adresów, które system otrzymuje z wiarygodnych źródeł, wymagana jest weryfikacja integralności danych; |
| | **SC-21[04]** | w przypadku odpowiedzi dotyczących uwierzytelniania pochodzenia nazw/adresów, które system otrzymuje z wiarygodnych źródeł, przeprowadzana jest weryfikacja integralności danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-21-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące bezpiecznych usług uwierzytelniania pochodzenia nazw/adresów (rekurencyjny lub buforujący serwer DNS); dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-21-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie serwerami DNS]. |
| | **SC-21-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające weryfikację pochodzenia i integralności danych dla usług uwierzytelniania pochodzenia nazw/adresów]. |

| | |
|---|---|
| **SC-21(01)** | **BEZPIECZEŃSTWO NAZW DOMEN/USŁUGA USTALANIA ADRESU IP/ADRESÓW (REKURENCYJNA LUB BUFOROWA) \| INTEGRALNOŚĆ** |
| | [WYCOFANE: Włączone do SC-21]. |

| | | |
|---|---|---|
| **SC-22** | **ARCHITEKTURA NAZW DOMEN/ADRESÓW IP/ZAMAWIANIE USŁUGI DNS** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-22[01]** | systemy, które wspólnie zapewniają usługi uwierzytelniania pochodzenia nazw/adresów dla organizacji są odporne na błędy; |
| | **SC-22[02]** | systemy, które wspólnie zapewniają usługi uwierzytelniania pochodzenia nazw/adresów dla organizacji stosują wewnętrzny rozdział ról; |
| | **SC-22[03]** | systemy, które wspólnie zapewniają usługi uwierzytelniania pochodzenia nazw/adresów dla organizacji stosują zewnętrzny rozdział ról. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-22-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące architektury i świadczenia usług w zakresie uwierzytelniania pochodzenia nazw/adresów; polityka i procedury dotyczące zabezpieczenia dostępu; dokumentacja projektowa systemu; wyniki oceny przeprowadzonej przez niezależne organizacje badawcze; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-22-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie serwerami DNS]. |

| | | |
|---|---|---|
| **SC-22** | **ARCHITEKTURA NAZW DOMEN/ADRESÓW IP/ZAMAWIANIE USŁUGI DNS** | |
| | **SC-22-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające usługi uwierzytelniania pochodzenia nazw/adresów w celu zapewnienia odporności na błędy i rozdziału ról]. |

| | | |
|---|---|---|
| **SC-23** | **AUTENTYCZNOŚĆ SESJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-23** | autentyczność sesji komunikacyjnych jest chroniona. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-23-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące autentyczności sesji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-23-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SC-23-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające autentyczność sesji]. |

| | | |
|---|---|---|
| **SC-23(01)** | **AUTENTYCZNOŚĆ SESJI \| UNIEWAŻNIENIE IDENTYFIKATORÓW SESJI PO WYLOGOWANIU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-23(01)** | identyfikatory sesji są unieważniane po wylogowaniu użytkownika lub zakończeniu sesji w inny sposób. |

| | | |
|---|---|---|
| **SC-23(01)** | **AUTENTYCZNOŚĆ SESJI \| UNIEWAŻNIENIE IDENTYFIKATORÓW SESJI PO WYLOGOWANIU** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-23(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące autentyczności sesji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-23(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SC-23(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające unieważnianie identyfikatora sesji po jej zakończeniu]. |

| | |
|---|---|
| **SC-23(02)** | **AUTENTYCZNOŚĆ SESJI \| WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA/WYŚWIETLANIE WIADOMOŚCI** |
| | [WYCOFANE: Włączone do AC-12(01)]. |

| | | |
|---|---|---|
| **SC-23(03)** | **AUTENTYCZNOŚĆ SESJI \| UNIKATOWE IDENTYFIKATORY SESJI GENEROWANE PRZEZ SYSTEM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-23(03)_ODP** | ***określono wymagania w zakresie losowości dotyczące generowania unikalnego identyfikatora dla każdej sesji;*** |
| | **SC-23(03)[01]** | dla każdej sesji generowany jest unikalny identyfikator spełniający ***<wymagania losowości SC-23(03)_ODP>***; |

| | | |
|---|---|---|
| **SC-23(03)** | **AUTENTYCZNOŚĆ SESJI \| UNIKATOWE IDENTYFIKATORY SESJI GENEROWANE PRZEZ SYSTEM** | |
| | **SC-23(03)[02]** | rozpoznawane są tylko identyfikatory sesji generowane przez system. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-23(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące autentyczności sesji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-23(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SC-23(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające, wdrażające, generujące i monitorujące unikatowe identyfikatory sesji; mechanizmy wspierające lub wdrażające wymagania dotyczące losowości]. |

| | |
|---|---|
| **SC-23(04)** | **AUTENTYCZNOŚĆ SESJI \| LOSOWE UNIKALNE IDENTYFIKATORY SESJI** |
| | [WYCOFANE: Włączone do SC-23(03)]. |

| | |
|---|---|
| **SC-23(05)** | **AUTENTYCZNOŚĆ SESJI \| AUTORYZOWANE URZĘDY CERTYFIKACYJNE** |
| | **CEL OCENY:**<br>*Ustalenie, czy:* |

| | | |
|---|---|---|
| **SC-23(05)** | **AUTENTYCZNOŚĆ SESJI \| AUTORYZOWANE URZĘDY CERTYFIKACYJNE** | |
| | **SC-23(05)_ODP** | ***określono urzędy certyfikacyjne, które mają być dopuszczone do weryfikacji ustanowienia sesji chronionych;*** |
| | **SC-23(05)** | do weryfikacji ustanowienia sesji chronionych dopuszcza się wykorzystanie jedynie ***<autoryzowanych urzędów SC-23(05)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-23(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące autentyczności sesji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista urzędów certyfikacyjnych dopuszczonych do weryfikacji ustanowienia sesji chronionych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-23(05)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SC-23(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zarządzanie urzędami certyfikacyjnymi]. |

| | | |
|---|---|---|
| **SC-24** | **PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-24_ODP[01]** | ***określono rodzaje błędów systemu, po których komponenty systemu przechodzą do stanu bezpiecznego;*** |

| | | |
|---|---|---|
| **SC-24** | **PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE** | |
| | **SC-24_ODP[02]** | ***określono stan bezpieczny systemu, do którego przechodzą komponenty systemu w przypadku błędu;*** |
| | **SC-24_ODP[03]** | ***określono informacje o stanie systemu, które mają być zachowane w przypadku błędu systemu;*** |
| | **SC-24** | ***<rodzaje błędów w komponentach systemu SC-24_ODP[01]>*** skutkują przejściem do ***<stanu bezpiecznego SC-24_ODP[02]>*** z zachowaniem ***<informacji o stanie systemu SC-24_ODP[03]>*** w przypadku wystąpienia błędu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-24-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące przejścia systemu do stanu bezpiecznego w przypadku błędu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz błędów wymagających przejścia systemu do stanu bezpiecznego; informacje o stanie, które mają być zachowane w przypadku błędu systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-24-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-24-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające zdolność do przejścia do stanu bezpiecznego; mechanizmy zachowujące informacje o stanie systemu w przypadku błędu systemu]. |

| | | |
|---|---|---|
| **SC-25** | **THIN NODES/TERMINALOWE STACJE ROBOCZE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-25_ODP** | ***określono stosowane komponenty systemu o zminimalizowanej funkcjonalności i ilości miejsca na informacje;*** |
| | **SC-25[01]** | dla ***<komponentów systemu SC-25_ODP>*** wdrożono zminimalizowaną funkcjonalność; |
| | **SC-25[02]** | dla ***<komponentów systemu SC-25_ODP>*** przydzielono minimalną ilość miejsca na informacje. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-25-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące wykorzystania „cienkich klientów" (thin nodes); dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-25-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SC-25-Test** | [WYBÓR SPOŚRÓD: Mechanizm wspierający lub wdrażający stosowanie „cienkich klientów" (thin nodes)]. |

| | | |
|---|---|---|
| **SC-26** | **WABIKI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-26[01]** | w systemach organizacyjnych zawarte są komponenty specjalnie zaprojektowane jako cel ataków, które służą do wykrywania takich ataków; |
| | **SC-26[02]** | w systemach organizacyjnych zawarte są komponenty specjalnie zaprojektowane jako cel ataków, które służą do odpierania takich ataków; |
| | **SC-26[03]** | w systemach organizacyjnych zawarte są komponenty specjalnie zaprojektowane jako cel ataków, które służą do analizowania takich ataków; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-26-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące stosowania wabików; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-26-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-26-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające stosowanie wabików]. |

| | |
|---|---|
| **SC-26(01)** | **WABIKI \| WYKRYWANIE KODU ZŁOŚLIWEGO** |
| | [WYCOFANE: Włączone do SC-35]. |

| | | |
|---|---|---|
| **SC-27** | **WIELOPLATFORMOWOŚĆ APLIKACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-27_ODP** | ***określono aplikacje wieloplatformowe, które mają być włączone do systemów organizacyjnych;*** |
| | **SC-27** | ***<aplikacje wieloplatformowe SC-27_ODP>*** są zawarte w systemach organizacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-27-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące aplikacji wieloplatformowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz aplikacji wieloplatformowych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-27-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-27-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające aplikacje wieloplatformowe]. |

| | | |
|---|---|---|
| **SC-28** | **OCHRONA DANYCH W SKŁADOWANIU/KOPIE KONFIGURACJI SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-28_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{poufność; integralność};*** |
| | **SC-28_ODP[02]** | ***określono przechowywane informacje wymagające ochrony;*** |
| | **SC-28** | ***<WYBRANA WARTOŚĆ PARAMETRU SC-28_ODP[01]>*** z<br>***<przechowywane informacje SC-28_ODP[02]>*** jest objęta ochroną. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-28-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony przechowywanych informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; mechanizmy kryptograficzne i związana z nimi dokumentacja konfiguracyjna; wykaz przechowywanych informacji wymagających ochrony poufności i integralności; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-28-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SC-28-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające ochronę poufności i integralności przechowywanych]. |

| | | |
|---|---|---|
| **SC-28(01)** | **OCHRONA DANYCH W SKŁADOWANIU/KOPIE KONFIGURACJI SYSTEMU \| OCHRONA KRYPTOGRAFICZNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-28(01)_ODP[01]** | ***określono informacje wymagające ochrony kryptograficznej;*** |
| | **SC-28(01)_ODP[02]** | ***określono komponenty systemu lub nośniki wymagające ochrony kryptograficznej;*** |
| | **SC-28(01)[01]** | wdrożono mechanizmy kryptograficzne, aby zapobiec nieuprawnionemu ujawnianiu ***<przechowywanych informacji SC-28(01)_ODP[01]>*** znajdujących się w ***<komponentach systemu lub nośnikach SC-28(01)_ODP[02]>***; |
| | **SC-28(01)[02]** | wdrożono mechanizmy kryptograficzne, aby zapobiec nieuprawnionej modyfikacji***<przechowywanych informacji SC-28(01)_ODP[01]>*** znajdujących się w ***<komponentach systemu lub nośnikach SC-28(01)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-28(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony przechowywanych informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; mechanizmy kryptograficzne i związana z nimi dokumentacja konfiguracyjna; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-28(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |

| | | |
|---|---|---|
| **SC-28(01)** | **OCHRONA DANYCH W SKŁADOWANIU/KOPIE KONFIGURACJI SYSTEMU \| OCHRONA KRYPTOGRAFICZNA** | |
| | **SC-28(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne wdrażające zabezpieczenia w zakresie poufności i integralności dla przechowywanych informacji]. |

| | | |
|---|---|---|
| **SC-28(02)** | **OCHRONA DANYCH W SKŁADOWANIU/KOPIE KONFIGURACJI SYSTEMU \| PRZECHOWYWANIE W TRYBIE OFF-LINE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-28(02)_ODP** | ***określono informacje, które należy usunąć z pamięci online i przechowywać w trybie offline w bezpiecznym miejscu;*** |
| | **SC-28(02)[01]** | ***<informacje SC-28(02)_ODP>*** są usuwane z pamięci online; |
| | **SC-28(02)[02]** | ***<informacje SC-28(02)_ODP>*** są przechowywane w trybie offline w bezpiecznym miejscu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-28(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony przechowywanych informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; mechanizmy kryptograficzne i związana z nimi dokumentacja konfiguracyjna; miejsca przechowywania informacji w trybie offline; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-28(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SC-28(02)** | **OCHRONA DANYCH W SKŁADOWANIU/KOPIE KONFIGURACJI SYSTEMU \| PRZECHOWYWANIE W TRYBIE OFF-LINE** | |
| | **SC-28(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające usuwanie informacji z pamięci masowej online; mechanizmy wspierające lub wdrażające przechowywanie informacji w trybie offline]. |

| | | |
|---|---|---|
| **SC-28(03)** | **OCHRONA DANYCH W SKŁADOWANIU/KOPIE KONFIGURACJI SYSTEMU \| KLUCZE KRYPTOGRAFICZNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-28(03)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {<zabezpieczenia SC-28(03)_ODP[02]>; chroniony sprzętowo magazyn kluczy kryptograficznych};*** |
| | **SC-28(03)_ODP[02]** | ***określono zabezpieczenia stosowane do ochrony magazynu kluczy kryptograficznych (jeśli wybrano);*** |
| | **SC-28(03)** | Ochronę kluczy kryptograficznych zapewnia ***<WYBRANA WARTOŚĆ PARAMETRU SC-28(03)_ODP[01]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-28(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ochrony przechowywanych informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; mechanizmy kryptograficzne i związana z nimi dokumentacja konfiguracyjna; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-28(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SC-28(03)** | **OCHRONA DANYCH W SKŁADOWANIU/KOPIE KONFIGURACJI SYSTEMU \| KLUCZE KRYPTOGRAFICZNE** | |
| | **SC-28(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające chroniony sprzętowo magazyn kluczy]. |

| | | |
|---|---|---|
| **SC-29** | **HETEROGENICZNOŚĆ SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-29_ODP** | ***określono komponenty systemu wymagające zastosowania zróżnicowanego zestawu technologii informatycznych przy wdrażaniu systemu;*** |
| | **SC-29** | stosuje się zróżnicowany zestaw technologii informatycznych dla ***<komponentów systemu SC-29_ODP>*** przy wdrażaniu systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-29-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz technologii wdrożonych w systemie; dokumentacja dotycząca nabywania; umowy nabycia komponentów systemu lub usług; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-29-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zakup, rozwój i wdrażanie systemów]. |
| | **SC-29-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające stosowanie zróżnicowanego zestawu technologii informatycznych]. |

| | | |
|---|---|---|
| **SC-29(01)** | **HETEROGENICZNOŚĆ \| TECHNIKI WIRTUALIZACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-29(01)_ODP** | ***określono częstotliwość, z jaką należy dokonywać zmian w zakresie różnorodności systemów operacyjnych i aplikacji wdrażanych z wykorzystaniem technik wirtualizacji;*** |
| | **SC-29(01)** | stosuje się techniki wirtualizacji w celu wspierania procesu wdrażania różnorodnych systemów operacyjnych i aplikacji, które są zmieniane ***<częstotliwością SC-29(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-29(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; lista systemów operacyjnych i aplikacji wdrożonych przy użyciu technik wirtualizacji;<br>dokumentacja dotycząca zabezpieczania zmian konfiguracji; zapisy dotyczące zarządzania konfiguracją; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-29(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za wdrażanie zatwierdzonych technik wirtualizacji do systemu]. |
| | **SC-29(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające stosowanie zróżnicowanych technologii informatycznych; mechanizmy wspierające lub wdrażające techniki wirtualizacji]. |

| | | |
|---|---|---|
| **SC-30** | **MASKOWANIE I DEZINFORMACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-30_ODP[01]** | ***Określono techniki maskowania i dezinformacji stosowane w celu zmylenia i wprowadzenia w błąd atakujących, którzy mogą potencjalnie zaatakować systemy organizacji;*** |
| | **SC-30_ODP[02]** | ***określono systemy, w których mają być stosowane techniki maskowania i dezinformacji;*** |
| | **SC-30_ODP[03]** | ***określono terminy na wdrożenie technik maskowania i dezinformacji w systemach;*** |
| | **SC-30** | stosuje się ***<techniki maskowania i dezinformacji SC-30_ODP[01]> w <systemach SC-30_ODP[02]>*** przez ***<okres SC-30_ODP[03]>*** w celu zmylenia i wprowadzenia w błąd atakujących. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-30-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące technik maskowania i dezinformacji w systemie; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; wykaz technik maskowania i dezinformacji stosowanych w systemach organizacyjnych; dokumentacja z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-30-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji;<br>personel organizacyjny odpowiedzialny za wdrażanie technik maskowania i dezinformacji w systemie]. |
| | **SC-30-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające techniki maskowania i dezinformacji]. |

| | |
|---|---|
| **SC-30(01)** | **MASKOWANIE I DEZINFORMACJA \| TECHNIKI WIRTUALIZACJI** |
| | [WYCOFANE: Włączone do SC-29(01)]. |

| | | |
|---|---|---|
| **SC-30(02)** | **MASKOWANIE I DEZINFORMACJA \| LOSOWOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-30(02)_ODP** | ***określono techniki stosowane w celu wprowadzenia losowości w operacjach i zasobach organizacji;*** |
| | **SC-30(02)** | stosuje się ***<techniki SC-30(02)_ODP>*** w celu wprowadzenia losowości w operacjach i zasobach organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-30(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące technik maskowania i dezinformacji w systemie; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; wykaz technik stosowanych w celu wprowadzenia losowości w operacjach i zasobach organizacji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-30(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji;<br>personel organizacyjny odpowiedzialny za wdrażanie technik maskowania i dezinformacji w systemie]. |
| | **SC-30(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające losowość jako technikę maskowania i dezinformacji]. |

| | | |
|---|---|---|
| **SC-30(03)** | **MASKOWANIE I DEZINFORMACJA \| ZMIANA LOKALIZACJI PRZETWARZANIA/PRZECHOWYWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-30(03)_ODP[01]** | ***określono lokalizacje przetwarzania lub przechowywania, które mają być zmieniane;*** |
| | **SC-30(03)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {<okres SC-30(03)_ODP[03]>; w przypadkowych odstępach czasu};*** |
| | **SC-30(03)_ODP[03]** | ***określono częstotliwość, z jaką należy zmieniać lokalizację przetwarzania lub przechowywania (jeśli wybrano);*** |
| | **SC-30(03)** | lokalizacja ***<przetwarzania lub przechowywania SC-30(03)_ODP[01]>*** jest zmieniana<br>***<WYBRANA WARTOŚĆ PARAMETRU SC-30(03)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-30(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury zarządzania konfiguracją; procedury dotyczące technik maskowania i dezinformacji w systemie; lista lokalizacji przetwarzania/przechowywania, które mają być zmieniane w odstępach czasu określonych przez organizację; dokumentacja dotycząca zabezpieczania zmian; zapisy dotyczące zarządzania konfiguracją; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-30(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemów/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zmianę lokalizacji przetwarzania lub przechowywania]. |
| | **SC-30(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające proces zmiany lokalizacji przetwarzania lub przechowywania]. |

| | | |
|---|---|---|
| **SC-30(04)** | **MASKOWANIE I DEZINFORMACJA \| INFORMACJE DEZINFORMUJĄCE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-30(04)_ODP** | ***określono komponenty systemu, w przypadku których stosuje się realistyczne, ale dezinformujące informacje o ich stanie bezpieczeństwa lub charakterze zabezpieczeń;*** |
| | **SC-30(04)** | stosuje się realistyczne, ale dezinformujące informacje o stanie bezpieczeństwa lub charakterze zabezpieczeń<br>***<komponentów systemu SC-30(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-30(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury zarządzania konfiguracją; procedury dotyczące technik maskowania i dezinformacji w systemie; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-30(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji;<br>personel organizacyjny odpowiedzialny za określenie i stosowanie realistycznych, ale dezinformujących informacji o charakterze zabezpieczeń komponentów systemu]. |
| | **SC-30(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające stosowanie realistycznych, ale dezinformujących informacji o charakterze zabezpieczeń komponentów systemu]. |

| | | |
|---|---|---|
| **SC-30(05)** | **MASKOWANIE I DEZINFORMACJA \| UKRYWANIE KOMPONENTÓW SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-30(05)_ODP[01]** | ***określono techniki stosowane w celu ukrywania lub maskowania komponentów systemu;*** |
| | **SC-30(05)_ODP[02]** | ***określono komponenty systemu, które mają być ukrywane lub maskowane przy użyciu konkretnych technik (zdefiniowanych w SC-30(05)_ODP[01]);*** |
| | **SC-30(05)** | stosuje się ***<techniki SC-30(05)_ODP[01]>*** w celu ukrywania lub maskowania<br>***<komponentów systemu SC-30(05)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-30(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury zarządzania konfiguracją; procedury dotyczące technik maskowania i dezinformacji w systemie; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz technik stosowanych w celu ukrywania lub maskowania komponentów systemu; wykaz komponentów systemu, które mają być ukrywane lub maskowane; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-30(05)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za maskowanie komponentów systemu]. |
| | **SC-30(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające techniki maskowania komponentów systemu]. |

| | | |
|---|---|---|
| **SC-31** | **ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-31_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:*** ***{przechowywanie;***<br>***synchronizacja};*** |
| | **SC-31a.** | przeprowadza się analizę ukrytych kanałów w celu identyfikacji tych aspektów komunikacji w ramach systemu, które mogą potencjalnie służyć do obsługi ukrytych kanałów ***<WYBRANA WARTOŚĆ PARAMETRU SC-31_ODP>***; |
| | **SC-31b.** | szacowana jest maksymalna szerokość pasma takich kanałów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-31-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące analizy ukrytych kanałów; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dotycząca analizy ukrytych kanałów; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-31-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za analizę ukrytych kanałów; programiści/integratorzy systemu]. |
| | **SC-31-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny w zakresie analizowania ukrytych kanałów; mechanizmy wspierające lub wdrażające analizę ukrytych kanałów; mechanizmy wspierające lub wdrażające zdolność do szacowania szerokości pasma ukrytych kanałów]. |

| | | |
|---|---|---|
| **SC-31(01)** | **ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI \| TESTOWANIE KANAŁÓW UKRYTYCH POD KĄTEM MOŻLIWOŚCI ICH WYKORZYSTANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-31(01)** | w celu określenia kanałów, które można wykorzystać, testuje się podzbiór zidentyfikowanych ukrytych kanałów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-31(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące analizy ukrytych kanałów; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz ukrytych kanałów; dokumentacja dotycząca analizy ukrytych kanałów; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-31(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za analizę ukrytych kanałów]. |
| | **SC-31(01)-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny w zakresie badania ukrytych kanałów; mechanizmy wspierające lub wdrażające testowanie ukrytych kanałów]. |

| | | |
|---|---|---|
| **SC-31(02)** | **ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI \| MAKSYMALNA PRZEPUSTOWOŚĆ ŁĄCZA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-31(02)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {przechowywanie; synchronizacja};*** |
| | **SC-31(02)_ODP[02]** | ***określono maksymalne wartości szerokości pasma dla zidentyfikowanych ukrytych kanałów;*** |
| | **SC-31(02)** | maksymalna szerokość pasma dla zidentyfikowanych ukrytych kanałów ***<WYBRANA WARTOŚĆ PARAMETRU SC-31(02)_ODP[01]>*** jest zmniejszana do ***<wartości SC-31(02)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-31(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące analizy ukrytych kanałów; umowy nabycia systemów lub usług; dokumentacja dotycząca nabywania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dotycząca analizy ukrytych kanałów; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-31(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za analizę ukrytych kanałów; programiści/integratorzy systemu]. |

| | | |
|---|---|---|
| **SC-31(02)** | **ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI \| MAKSYMALNA PRZEPUSTOWOŚĆ ŁĄCZA** | |
| | **SC-31(02)-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny w zakresie analizowania ukrytych kanałów; mechanizmy wspierające lub wdrażające analizę ukrytych kanałów; mechanizmy wspierające lub wdrażające zdolność do zmniejszania przepustowości ukrytych kanałów ]. |

| | | |
|---|---|---|
| **SC-31(03)** | **ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI \| POMIAR PRZEPUSTOWOŚCI W ŚRODOWISKU OPERACYJNYM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-31(03)_ODP** | ***określono podzbiór zidentyfikowanych ukrytych kanałów, których przepustowość ma być mierzona w środowisku operacyjnym systemu;*** |
| | **SC-31(03)** | dokonuje się pomiaru szerokości pasma ***<podzbioru zidentyfikowanych ukrytych kanałów SC-31(03)_ODP>*** w środowisku operacyjnym systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-31(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące analizy ukrytych kanałów; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dotycząca analizy ukrytych kanałów; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-31(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za analizę ukrytych kanałów; programiści/integratorzy systemu]. |

| | | |
|---|---|---|
| **SC-31(03)** | **ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI \| POMIAR PRZEPUSTOWOŚCI W ŚRODOWISKU OPERACYJNYM** | |
| | **SC-31(03)-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny w zakresie analizy ukrytych kanałów; mechanizmy wspierające lub wdrażające analizę ukrytych kanałów; mechanizmy wspierające lub wdrażające zdolności w zakresie pomiaru szerokości pasma ukrytych kanałów]. |

| | | |
|---|---|---|
| **SC-32** | **DZIELENIE SYSTEMU NA PARTYCJE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-32_ODP[01]** | ***określono komponenty systemu, które mają znajdować się w oddzielnych fizycznych lub logicznych domenach lub środowiskach, w oparciu o określone okoliczności dotyczące fizycznego lub logicznego oddzielenia komponentów;*** |
| | **SC-32_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {fizyczne; logiczne};*** |
| | **SC-32_ODP[03]** | ***określono okoliczności fizycznego lub logicznego oddzielenia komponentów;*** |
| | **SC-32** | system jest podzielony na ***<komponenty systemu SC-32_ODP[01]>***, znajdujące się w oddzielnych ***<WYBRANA WARTOŚĆ PARAMETRU SC-32_ODP[02]>*** domenach lub środowiskach w oparciu o ***<okoliczności dotyczące fizycznego lub logicznego oddzielenia komponentów SC-32_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-32** | **DZIELENIE SYSTEMU NA PARTYCJE** | |
| | **SC-32-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące oddzielenia systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; wykaz fizycznych domen (lub środowisk) systemu; schematy obiektów, w których znajduje się system; schematy sieci systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-32-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |
| | **SC-32-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające fizyczne oddzielenie komponentów systemu]. |

| | | |
|---|---|---|
| **SC-32(01)** | **DZIELENIE SYSTEMU NA PARTYCJE \| FIZYCZNIE WYDZIELONE DOMENY DLA FUNKCJI UPRZYWILEJOWANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-32(01)** | Funkcje uprzywilejowane są przypisane do oddzielnych domen fizycznych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-32(01)** | **DZIELENIE SYSTEMU NA PARTYCJE \| FIZYCZNIE WYDZIELONE DOMENY DLA FUNKCJI UPRZYWILEJOWANYCH** | |
| | **SC-32-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące oddzielenia systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; wykaz fizycznych domen (lub środowisk) systemu; schematy obiektów, w których znajduje się system; schematy sieci systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-32-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |
| | **SC-32-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające fizyczne oddzielenie komponentów systemu]. |

| | | |
|---|---|---|
| **SC-33** | **INTEGRALNOŚĆ TRANSMISJI** | |
| | [WYCOFANE: Włączone do SC-08]. | |

| | | |
|---|---|---|
| **SC-34** | **NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-34_ODP[01]** | ***określono komponenty systemu, w przypadku których środowisko operacyjne i aplikacje mają być ładowane i wykonywane z nośników wymuszonych sprzętowo tylko do odczytu;*** |

| | | |
|---|---|---|
| **SC-34** | **NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE** | |
| | **SC-34_ODP[02]** | ***określono aplikacje, które mają być ładowane i wykonywane z nośników wymuszonych sprzętowo, tylko do odczytu;*** |
| | **SC-34a.** | środowisko operacyjne dla ***<komponentów systemu SC-34_ODP[01]>*** jest ładowane i wykonywane z wymuszonego sprzętowo nośnika tylko do odczytu; |
| | **SC-34b.** | ***<aplikacje SC-34_ODP[02]>*** dla ***<komponentów systemu SC-34_ODP[01]>*** są ładowane i wykonywane z wymuszonych sprzętowo nośników tylko do odczytu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-34-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące niemodyfikowalnych programów wykonywalnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; lista komponentów systemu operacyjnego, które mają być ładowane z nośników wymuszonych sprzętowo tylko do odczytu;<br>lista aplikacji, które mają być ładowane z wymuszonych sprzętowo nośników tylko do odczytu; nośniki używane do ładowania i wykonywania środowiska operacyjnego systemu; nośniki używane do ładowania i wykonywania aplikacji systemowych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-34-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |

| | | |
|---|---|---|
| **SC-34** | **NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE** | |
| | **SC-34-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające, ładujące i wykonujące środowisko operacyjne z nośników wymuszonych sprzętowo tylko do odczytu; mechanizmy wspierające lub wdrażające, ładujące i wykonujące aplikacje z nośników wymuszonych sprzętowo tylko do odczytu]. |

| | | |
|---|---|---|
| **SC-34(01)** | **NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE \| NIEZAPISYWALNE PAMIĘCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-34(01)_ODP** | ***określono komponenty systemu stosowane z niezapisywalnymi pamięciami;*** |
| | **SC-34(01)** | ***<komponenty systemu SC-34(01)_ODP>*** są stosowane z niezapisywalną pamięcią, której zawartość pozostaje niezmienna po restarcie komponentu lub włączeniu/wyłączeniu zasilania. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-34(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące niemodyfikowalnych programów wykonywalnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; wykaz komponentów systemu stosowanych z niezapisywalnymi pamięciami; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-34(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |

| | | |
|---|---|---|
| **SC-34(01)** | **NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE \| NIEZAPISYWALNE PAMIĘCI** | |
| | **SC-34(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające stosowanie komponentów bez możliwości zapisu; mechanizmy wspierające lub wdrażające niezapisywalną pamięć, której zawartość pozostaje niezmienna po ponownym uruchomieniu komponentu lub włączeniu/wyłączeniu zasilania]. |

| | | |
|---|---|---|
| **SC-34(02)** | **NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE \| OCHRONA INTEGRALNOŚCI/NOŚNIKI TYLKO DO ODCZYTU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-34(02)[01]** | integralność informacji jest chroniona przed jej zapisem na nośnikach tylko do odczytu; |
| | **SC-34(02)[02]** | nośnik jest zabezpieczany po zapisaniu takiej informacji na nośniku; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-34(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące niemodyfikowalnych programów wykonywalnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-34(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |

| | | |
|---|---|---|
| **SC-34(02)** | **NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE \| OCHRONA INTEGRALNOŚCI/NOŚNIKI TYLKO DO ODCZYTU** | |
| | **SC-34(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolność do ochrony integralności informacji na nośnikach tylko do odczytu przed zapisem i po zapisie informacji na nośniku]. |

| | |
|---|---|
| **SC-34(03)** | **NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE \| OCHRONA SPRZĘTOWA** |
| | [WYCOFANE: Włączone do SC-51]. |

| | | |
|---|---|---|
| **SC-35** | **ZEWNĘTRZNA IDENTYFIKACJA ZŁOŚLIWEGO KODU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-35** | do systemu włączono komponenty, które proaktywnie dążą do identyfikacji złośliwego kodu sieciowego lub złośliwych stron internetowych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-35-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące identyfikacji zewnętrznego złośliwego kodu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; komponenty systemu wdrożone w celu identyfikacji złośliwych stron internetowych lub złośliwego kodu internetowego; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-35-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |

| | | |
|---|---|---|
| **SC-35** | **ZEWNĘTRZNA IDENTYFIKACJA ZŁOŚLIWEGO KODU** | |
| | **SC-35-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspierające lub wdrażające zewnętrzne mechanizmy identyfikacji złośliwego kodu]. |

| | | |
|---|---|---|
| **SC-36** | **PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-36_ODP[01]** | ***określono komponenty przetwarzania, które mają być rozproszone w wielu lokalizacjach/domenach;*** |
| | **SC-36_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {lokalizacje fizyczne; domeny logiczne};*** |
| | **SC-36_ODP[03]** | ***określono komponenty pamięci masowej, które mają być rozproszone w wielu lokalizacjach/domenach;*** |
| | **SC-36_ODP[04]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {lokalizacje fizyczne; domeny logiczne};*** |
| | **SC-36[01]** | ***<komponenty przetwarzania SC-36_ODP[01]>*** są rozproszone w ***<WYBRANA WARTOŚĆ PARAMETRU SC-36_ODP[02]>***; |
| | **SC-36[02]** | ***<komponenty pamięci masowej SC-36_ODP[03]>*** są rozproszone w ***<WYBRANA WARTOŚĆ PARAMETRU SC-36_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SC-36 | PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE | |
|---|---|---|
| | **SC-36-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury planowania awaryjnego; plan awaryjny; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; wykaz fizycznych lokalizacji (lub środowisk) systemu wykorzystywanych do rozproszonego przetwarzania i przechowywania; schematy obiektów, w których znajduje się system; umowy dotyczące miejsc przetwarzania; umowy dotyczące miejsc przechowywania; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-36-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za planowanie awaryjne i wdrażanie planu; programiści/integratorzy systemu]. |
| | **SC-36-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące rozproszonego przetwarzania i przechowywania w wielu lokalizacjach fizycznych; mechanizmy wspierające lub wdrażające zdolność do rozproszonego przetwarzania i przechowywania w wielu lokalizacjach fizycznych]. |

| | | |
|---|---|---|
| **SC-36(01)** | **PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE \| TECHNIKI PRZEGLĄDANIA CYKLICZNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-36(01)_ODP[01]** | ***określono rozproszone komponenty przetwarzania i przechowywania, w przypadku których mają być stosowane techniki cyklicznego przeglądania w celu identyfikacji potencjalnych wad, błędów lub naruszeń bezpieczeństwa;*** |
| | **SC-36(01)_ODP[02]** | ***określono działania, które należy podjąć w odpowiedzi na zidentyfikowane wady, błędy lub naruszenia bezpieczeństwa;*** |
| | **SC-36(01)(a)** | stosuje się techniki cyklicznego przeglądania do identyfikacji potencjalnych wad, błędów lub naruszeń bezpieczeństwa w ***<rozproszonych komponentach przetwarzania i przechowywania SC-36(01)_ODP[01]>***; |
| | **SC-36(01)(b)** | w odpowiedzi na zidentyfikowane wady, błędy lub naruszenia bezpieczeństwa podejmowane są ***<działania SC-36(01)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-36(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; wykaz rozproszonych komponentów przetwarzania i przechowywania danych podlegających cyklicznemu przeglądaniu; techniki cyklicznemu przeglądania systemu i związana z nimi dokumentacja lub zapisy; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-36(01)** | **PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE \| TECHNIKI PRZEGLĄDANIA CYKLICZNEGO** | |
| | **SC-36(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |
| | **SC-36(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające techniki przeglądania cyklicznego]. |

| | | |
|---|---|---|
| **SC-36(02)** | **PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE \| SYNCHRONIZACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-36(02)_ODP** | ***określono zdublowane systemy lub komponenty systemu, które mają być zsynchronizowane;*** |
| | **SC-36(02)** | ***<zdublowane systemy lub komponenty systemu SC-36(02)_ODP>*** są zsynchronizowane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-36(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; wykaz rozproszonych komponentów przetwarzania i przechowywania danych podlegających cyklicznemu przeglądaniu; techniki cyklicznemu przeglądania systemu i związana z nimi dokumentacja lub zapisy; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-36(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |

| | | |
|---|---|---|
| **SC-36(02)** | **PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE \| SYNCHRONIZACJA** | |
| | **SC-36(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające synchronizację zdublowanych systemów lub komponentu systemów]. |

| | | |
|---|---|---|
| **SC-37** | **KANAŁY POZAPASMOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-37_ODP[01]** | ***określono kanały pozapasmowe stosowane do fizycznej dostawy lub elektronicznej transmisji informacji, komponentów systemu lub urządzeń do osób lub systemu;*** |
| | **SC-37_ODP[02]** | ***określono informacje, komponenty systemu lub urządzenia wykorzystujące kanały pozapasmowe do celów fizycznej dostawy lub elektronicznej transmisji;*** |
| | **SC-37_ODP[03]** | ***określono osoby lub systemy, do których za pomocą kanałów pozapasmowych mają zostać fizycznie dostarczone lub elektronicznie przesłane informacje, komponenty systemu lub urządzenia;*** |
| | **SC-37** | stosuje się ***<kanały pozapasmowe SC-37_ODP[01]>*** do celów fizycznej dostawy lub elektronicznej transmisji ***<informacji, komponentów systemu lub urządzeń SC-37_ODP[02]>*** do ***<osób lub systemów SC-37_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-37** | **KANAŁY POZAPASMOWE** | |
| | **SC-37-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące wykorzystania kanałów pozapasmowych; polityka i procedury kontroli dostępu; polityka i procedury identyfikacji i uwierzytelniania; dokumentacja projektowa systemu; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista kanałów pozapasmowych; rodzaje informacji, komponentów systemu lub urządzeń wymagających wykorzystania kanałów pozapasmowych w celu fizycznej dostawy lub elektronicznej transmisji do uprawnionych osób lub systemów; zapisy dotyczące fizycznej dostawy; zapisy dotyczące elektronicznej transmisji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-37-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny zatwierdzający, instalujący, konfigurujący, obsługujący lub używający kanałów pozapasmowych; programiści/integratorzy systemu]. |
| | **SC-37-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykorzystania kanałów pozapasmowych; mechanizmy wspierające lub wdrażające wykorzystanie kanałów pozapasmowych]. |

| | | |
|---|---|---|
| **SC-37(01)** | **KANAŁY POZAPASMOWE \| GWARANTOWANA DOSTAWA/TRANSMISJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-37(01)_ODP[01]** | ***określono zabezpieczenia, które mają być stosowane w celu zapewnienia, że tylko wyznaczone osoby lub systemy otrzymują określone informacje, komponenty systemu lub urządzenia;*** |

| | | |
|---|---|---|
| **SC-37(01)** | **KANAŁY POZAPASMOWE \| GWARANTOWANA DOSTAWA/TRANSMISJA** | |
| | **SC-37(01)_ODP[02]** | ***określono osoby lub systemy wyznaczone do odbioru określonych informacji, komponentów systemu lub urządzeń;*** |
| | **SC-37(01)_ODP[03]** | ***określono informacje, komponenty systemu lub urządzenia, do odbioru których uprawnione są wyłącznie wyznaczone osoby lub systemy;*** |
| | **SC-37(01)** | ***<zabezpieczenia SC-37(01)_ODP[01]>*** są stosowane w celu zapewnienia, że tylko ***<osoby lub systemy SC-37(01)_ODP[02]>*** otrzymują ***<informacje, komponenty systemu lub urządzenia SC-37(01)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-37(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące korzystania z kanałów pozapasmowych; polityka i procedury kontroli dostępu; polityka i procedury identyfikacji i uwierzytelniania; dokumentacja projektowa systemu; architektura systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz zabezpieczeń stosowanych w celu zapewnienia, że określone przez organizację informacje, komponenty systemu lub urządzenia otrzymują tylko wyznaczone osoby; wykaz zabezpieczeń dotyczących dostarczania wyznaczonych informacji, komponentów systemu lub urządzeń do wyznaczonych osób lub systemów; wykaz informacji, komponentów systemu lub urządzeń, które mają być dostarczone do wyznaczonych osób lub systemów; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-37(01)** | **KANAŁY POZAPASMOWE \| GWARANTOWANA DOSTAWA/TRANSMISJA** | |
| | **SC-37(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny zatwierdzający, instalujący, konfigurujący, obsługujący lub używający kanałów pozapasmowych; programiści/integratorzy systemu]. |
| | **SC-37(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykorzystania kanałów pozapasmowych; mechanizmy wspierające lub wdrażające wykorzystanie kanałów pozapasmowych; mechanizmy wspierające/wdrażające zabezpieczenia zapewniające dostawę wyznaczonych informacji, komponentów systemu lub urządzeń do odpowiednich osób lub systemów]. |

| | | |
|---|---|---|
| **SC-38** | **BEZPIECZEŃSTWO OPERACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-38_ODP** | ***opracowano środki bezpieczeństwa operacyjnego, które mają być stosowane w celu ochrony kluczowych informacji organizacyjnych w całym cyklu życia systemu;*** |
| | **SC-38** | stosuje się ***<środki bezpieczeństwa operacyjnego SC-38_ODP>*** w celu ochrony kluczowych informacji organizacyjnych w całym cyklu życia systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-38** | **BEZPIECZEŃSTWO OPERACYJNE** | |
| | **SC-38-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące bezpieczeństwa operacyjnego; plan bezpieczeństwa; wykaz środków bezpieczeństwa operacyjnego; oceny zabezpieczeń; oceny ryzyka; oceny zagrożeń i podatności; plany działania i kamienie milowe; dokumentacja cyklu życia rozwoju systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-38-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |
| | **SC-38-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie ochrony informacji organizacji w całym cyklu życia systemu; mechanizmy wspierające lub wdrażające zabezpieczenia w celu ochrony informacji organizacji w całym cyklu życia systemu]. |

| | | |
|---|---|---|
| **SC-39** | **IZOLACJA PROCESÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-39** | dla każdego systemowego procesu wykonawczego utrzymuje się oddzielną domenę wykonawczą. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-39-Badanie** | [WYBÓR SPOŚRÓD: Dokumentacja projektowa systemu; architektura systemu; dokumentacja dotycząca niezależnej weryfikacji i walidacji; dokumentacja dotycząca testów i oceny; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-39** | **IZOLACJA PROCESÓW** | |
| | **SC-39-Wywiad** | [WYBÓR SPOŚRÓD: Programiści/integratorzy systemu; architekt bezpieczeństwa systemu]. |
| | **SC-39-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające oddzielne domeny wykonawcze dla każdego systemowego procesu wykonawczego]. |

| | | |
|---|---|---|
| **SC-39(01)** | **IZOLACJA PROCESÓW \| SEPARACJA SPRZĘTOWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-39(01)** | w celu ułatwienia izolacji procesów wdrażana jest separacja sprzętowa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-39(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; dokumentacja systemowa dotycząca mechanizmów separacji sprzętowej; dokumentacja systemowa pochodząca od dostawców, producentów lub twórców; dokumentacja dotycząca niezależnej weryfikacji i walidacji; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-39(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |
| | **SC-39(01)-Test** | [WYBÓR SPOŚRÓD: Funkcje systemu wdrażające bazowe mechanizmy sprzętowej separacji procesów]. |

| | | |
|---|---|---|
| **SC-39(02)** | **IZOLACJA PROCESÓW \| ODDZIELNA DOMENA WYKONAWCZA DLA KAŻDEGO WĄTKU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-39(02)_ODP** | ***określono przetwarzanie wielowątkowe, w przypadku którego dla każdego wątku ma być utrzymywana oddzielna domena wykonawcza;*** |
| | **SC-39(02)** | w ramach ***<przetwarzania wielowątkowego SC-39(02)_ODP>*** dla każdego wątku utrzymywana jest oddzielna domena wykonawcza. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-39(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; wykaz systemowych domen wykonawczych dla każdego wątku w przetwarzaniu wielowątkowym; dokumentacja systemowa dotycząca przetwarzania wielowątkowego; dokumentacja systemowa pochodząca od dostawców, producentów lub programistów; dokumentacja dotycząca niezależnej weryfikacji i walidacji; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-39(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |
| | **SC-39(02)-Test** | [WYBÓR SPOŚRÓD: Funkcje systemu wdrażające oddzielną domenę wykonawczą dla każdego wątku w przetwarzaniu wielowątkowym]. |

| | | |
|---|---|---|
| **SC-40** | **OCHRONA ŁĄCZA BEZPRZEWODOWEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-40_ODP[01]** | ***określono zewnętrzne łącza bezprzewodowe, które mają być chronione przed poszczególnymi rodzajami ataków na parametry sygnału;*** |
| | **SC-40_ODP[02]** | ***określono rodzaje ataków na parametry sygnału lub odniesienia do źródeł takich ataków, przed którymi należy chronić zewnętrzne łącza bezprzewodowe;*** |
| | **SC-40_ODP[03]** | ***określono wewnętrzne łącza bezprzewodowe, które mają być chronione przed poszczególnymi rodzajami ataków na parametry sygnału;*** |
| | **SC-40_ODP[04]** | ***określono rodzaje ataków na parametry sygnału lub odniesienia do źródeł takich ataków, przed którymi należy chronić wewnętrzne łącza bezprzewodowe;*** |
| | **SC-40[01]** | zewnętrzne ***<łącza bezprzewodowe SC-40_ODP[01]>*** są chronione przed ***<rodzajami ataków na parametry sygnału lub odniesieniami do źródeł takich ataków SC-40_ODP[02]>***. |
| | **SC-40[02]** | wewnętrzne ***<łącza bezprzewodowe SC-40_ODP[03]>*** są chronione przed ***<rodzajami ataków na parametry sygnału lub odniesieniami do źródeł takich ataków SC-40_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-40-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury kontroli dostępu; procedury dotyczące ochrony łączy bezprzewodowych; dokumentacja projektowa systemu; schematy sieci bezprzewodowych; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; wykaz wewnętrznych i zewnętrznych łączy bezprzewodowych; wykaz ataków na parametry sygnału lub odniesień do źródeł ataków; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-40** | **OCHRONA ŁĄCZA BEZPRZEWODOWEGO** | |
| | **SC-40-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny zatwierdzający, instalujący, konfigurujący lub utrzymujący wewnętrzne i zewnętrzne łącza bezprzewodowe]. |
| | **SC-40-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające ochronę łączy bezprzewodowych]. |

| | | |
|---|---|---|
| **SC-40(01)** | **OCHRONA ŁĄCZA BEZPRZEWODOWEGO \| INTERFERENCJA ELEKTROMAGNETYCZNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-40(01)_ODP** | ***określono wymagany poziom ochrony przed skutkami celowych zakłóceń elektromagnetycznych;*** |
| | **SC-40(01)** | wdrożono mechanizmy kryptograficzne, oferujące ***<poziom ochrony SC-40(01)_ODP>*** przed skutkami celowych zakłóceń elektromagnetycznych. |
| | **SC-40(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury kontroli dostępu; procedury dotyczące ochrony łączy bezprzewodowych; dokumentacja projektowa systemu; schematy sieci bezprzewodowych; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; sprzęt i oprogramowanie komunikacyjne systemu; wyniki kategoryzacji zabezpieczeń; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-40(01)** | **OCHRONA ŁĄCZA BEZPRZEWODOWEGO \| INTERFERENCJA ELEKTROMAGNETYCZNA** | |
| | **SC-40(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny zatwierdzający, instalujący, konfigurujący lub utrzymujący wewnętrzne i zewnętrzne łącza bezprzewodowe]. |
| | **SC-40(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne wymuszające stosowanie zabezpieczeń przed skutkami celowych zakłóceń elektromagnetycznych]. |

| | | |
|---|---|---|
| **SC-40(02)** | **OCHRONA ŁĄCZA BEZPRZEWODOWEGO \| REDUKCJA POTENCJALNEJ DETEKCJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-40(02)_ODP** | ***określono poziom redukcji, jaki należy osiągnąć, aby zmniejszyć możliwość wykrywania łączy bezprzewodowych;*** |
| | **SC-40(02)** | wdrożono mechanizmy kryptograficzne zmniejszające potencjał wykrywania łączy bezprzewodowych do<br>***<poziomu redukcji SC-40(02)_ODP>i*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-40(02)** | **OCHRONA ŁĄCZA BEZPRZEWODOWEGO \| REDUKCJA POTENCJALNEJ DETEKCJI** | |
| | **SC-40(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury kontroli dostępu; procedury dotyczące ochrony łączy bezprzewodowych; dokumentacja projektowa systemu; schematy sieci bezprzewodowych; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; sprzęt i oprogramowanie komunikacyjne systemu; wyniki kategoryzacji zabezpieczeń; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-40(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny zatwierdzający, instalujący, konfigurujący lub utrzymujący wewnętrzne i zewnętrzne łącza bezprzewodowe]. |
| | **SC-40(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne wymuszające stosowanie zabezpieczeń w celu zmniejszenia wykrywalności łączy bezprzewodowych]. |

| | | |
|---|---|---|
| **SC-40(03)** | **OCHRONA ŁĄCZA BEZPRZEWODOWEGO \| NAŚLADOWCZE LUB MANIPULACYJNE OSZUSTWO TELEKOMUNIKACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-40(03)** | wdrożono mechanizmy kryptograficzne w celu identyfikacji i odrzucania transmisji bezprzewodowych będących próbami imitacji lub manipulacji w telekomunikacji na podstawie parametrów sygnału. |

| | | |
|---|---|---|
| **SC-40(03)** | **OCHRONA ŁĄCZA BEZPRZEWODOWEGO \| NAŚLADOWCZE LUB MANIPULACYJNE OSZUSTWO TELEKOMUNIKACYJNE** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-40(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury kontroli dostępu; procedury dotyczące dokumentacji projektowej systemu; schematy sieci bezprzewodowej; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; sprzęt i oprogramowanie komunikacyjne systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-40(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny zatwierdzający, instalujący, konfigurujący lub utrzymujący wewnętrzne i zewnętrzne łącza bezprzewodowe]. |
| | **SC-40(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne wymuszające zabezpieczenie łącza bezprzewodowego przed próbami imitacji lub manipulacji w telekomunikacji]. |

| | | |
|---|---|---|
| **SC-40(04)** | **OCHRONA ŁĄCZA BEZPRZEWODOWEGO \| IDENTYFIKACJA PARAMETRÓW SYGNAŁU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-40(04)_ODP** | ***określono nadajniki bezprzewodowe, w przypadku których mają być stosowane mechanizmy kryptograficzne;*** |

| | | |
|---|---|---|
| **SC-40(04)** | **OCHRONA ŁĄCZA BEZPRZEWODOWEGO \| IDENTYFIKACJA PARAMETRÓW SYGNAŁU** | |
| | **SC-40(04)** | Wdrożono mechanizmy kryptograficzne uniemożliwiające identyfikację ***<nadajników bezprzewodowych SC-40(04)_ODP>*** poprzez wykorzystanie parametrów sygnału nadajnika. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-40(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury kontroli dostępu; procedury dotyczące dokumentacji projektowej systemu; schematy sieci bezprzewodowej; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; sprzęt i oprogramowanie komunikacyjne systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-40(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny zatwierdzający, instalujący, konfigurujący lub utrzymujący wewnętrzne i zewnętrzne łącza bezprzewodowe]. |
| | **SC-40(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne zapobiegające identyfikacji nadajników bezprzewodowych]. |

| | | |
|---|---|---|
| **SC-41** | **DOSTĘP DO PORTÓW I URZĄDZEŃ WEJŚCIA/WYJŚCIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-41_ODP[01]** | ***określono porty połączeniowe lub urządzenia wejścia/wyjścia, które mają zostać wyłączone lub usunięte;*** |

| | | |
|---|---|---|
| **SC-41** | **DOSTĘP DO PORTÓW I URZĄDZEŃ WEJŚCIA/WYJŚCIA** | |
| | **SC-41_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {fizycznie; logicznie};*** |
| | **SC-41_ODP[03]** | ***określono systemy lub komponenty systemu, w przypadku których porty połączeniowe lub urządzenia wejścia/wyjścia mają być wyłączone lub usunięte;*** |
| | **SC-41** | ***<porty połączeniowe lub urządzenia wejścia/wyjścia SC-41_ODP[01]>*** są ***<WYBRANA WARTOŚĆ PARAMETRU SC-41_ODP[02]>*** wyłączane lub usuwane w ***<systemach lub komponentach systemu SC-41_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-41-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury kontroli dostępu; procedury dotyczące dostępu do portów i urządzeń wejścia/wyjścia; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; systemy lub komponenty systemu; wykaz portów połączeniowych lub urządzeń wejścia/wyjścia, które mają być fizycznie wyłączone lub usunięte w systemach lub komponentach systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-41-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system]. |
| | **SC-41-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające wyłączanie portów połączeniowych lub urządzeń wejścia/wyjścia]. |

| | | |
|---|---|---|
| **SC-42** | **CZUJNIKI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-42_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {wykorzystanie urządzeń posiadających <zdolność wykrywania środowiska SC-42_ODP[02]> w <obiektach, obszarach lub systemach SC-42_ODP[03]>; zdalna aktywacja zdolności wykrywania środowiska w systemach organizacyjnych lub komponentach***<br>***systemów z następującymi wyjątkami: <wyjątki zezwalające na zdalną aktywację czujników SC-42_ODP[04]>};*** |
| | **SC-42_ODP[02]** | ***określono zdolności w zakresie wykrywania środowiska w urządzeniach (jeśli wybrano);*** |
| | **SC-42_ODP[03]** | ***określono obiekty, obszary lub systemy, w których zabronione jest stosowanie urządzeń posiadających zdolność wykrywania środowiska (jeśli wybrano);*** |
| | **SC-42_ODP[04]** | ***określono wyjątki, w których dozwolona jest zdalna aktywacja czujników (jeśli wybrano);*** |
| | **SC-42_ODP[05]** | ***określono grupę użytkowników, którym należy zapewnić wyraźną informację o stosowaniu czujników;*** |
| | **SC-42a.** | ***<WYBRANA WARTOŚĆ PARAMETRU SC-42_ODP[01]>*** jest zabronione; |
| | **SC-42b.** | jednoznaczna informacja o stosowaniu czujników jest przekazywana **<grupie użytkowników SC-42_ODP[05]>**. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-42** | **CZUJNIKI** | |
| | **SC-42-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące funkcji czujników i gromadzenia danych; polityka i procedury kontroli dostępu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SC-42-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programista systemu; personel organizacyjny zajmujący się instalacją, konfiguracją lub konserwacją systemu; personel organizacyjny odpowiedzialny za funkcje czujników]. |
| | **SC-42-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające kontrolę dostępu do mechanizmu zdalnej aktywacji funkcji czujników systemowych; mechanizmy wdrażające możliwość sygnalizowania użycia czujników]. |

| | | |
|---|---|---|
| **SC-42(01)** | **CZUJNIKI \| RAPORTOWANIE DO UPOWAŻNIONYCH OSÓB LUB RÓL** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-42(01)_ODP** | ***określono czujniki, które mają być używane do zbierania danych lub informacji;*** |
| | **SC-42(01)** | system jest skonfigurowany tak, że dane lub informacje zebrane przez ***<czujniki SC-42(01)_ODP>*** są zgłaszane tylko do uprawnionych osób lub ról. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SC-42(01) | CZUJNIKI \| RAPORTOWANIE DO UPOWAŻNIONYCH OSÓB LUB RÓL | |
|---|---|---|
| | **SC-42(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury kontroli dostępu; procedury dotyczące funkcji czujników i gromadzenia danych; polityka przetwarzania danych identyfikacyjnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SC-42(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programista systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za funkcje czujników]. |
| | **SC-42(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy ograniczające raportowanie informacji z czujników do osób upoważnionych; możliwości systemu w zakresie zbierania danych z czujników i raportowania]. |

| SC-42(02) | CZUJNIKI \| AUTORYZOWANE UŻYCIE | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-42(02)_ODP** | ***określono środki, które należy zastosować, aby dane lub informacje zebrane przez czujniki były wykorzystywane wyłącznie do dozwolonych celów;*** |
| | **SC-42(02)** | stosuje się ***<środki SC-42(02)_ODP>*** w celu zapewnienia, że dane lub informacje zebrane przez<br>***<czujniki SC-42(01)_ODP>*** są wykorzystywane tylko do dozwolonych celów. |

| | | |
|---|---|---|
| **SC-42(02)** | **CZUJNIKI \| AUTORYZOWANE UŻYCIE** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-42(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury kontroli dostępu; polityka przetwarzania danych identyfikacyjnych; funkcje czujników i możliwości gromadzenia danych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; wykaz środków, które należy zastosować w celu zapewnienia, że dane lub informacje gromadzone przez czujniki są wykorzystywane wyłącznie do dozwolonych celów; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SC-42(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za funkcje czujników]. |
| | **SC-42(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające środki zapewniające, że informacje z czujników są wykorzystywane tylko do dozwolonych celów; zdolność systemu do gromadzenia informacji z czujników]. |

| | |
|---|---|
| **SC-42(03)** | **CZUJNIKI \| ZABRONIONE WYKORZYSTANIE URZĄDZEŃ** |
| | [WYCOFANE: Włączone do SC-42]. |

| | | |
|---|---|---|
| **SC-42(04)** | **CZUJNIKI \| POWIADOMIENIE O ZBIERANIU DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-42(04)_ODP[01]** | ***określono środki ułatwiające poinformowanie osoby fizycznej o gromadzeniu dotyczących jej danych identyfikacyjnych;*** |
| | **SC-42(04)_ODP[02]** | ***określono czujniki, które gromadzą dane identyfikacyjne;*** |
| | **SC-42(04)** | stosuje się ***<środki SC-42(04)_ODP[01]>*** w celu poinformowania osoby fizycznej o gromadzeniu dotyczących jej danych identyfikacyjnych przez<br>***<czujniki SC-42(04)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-42(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury kontroli dostępu; polityka przetwarzania danych identyfikacyjnych; polityka i procedury dotyczące funkcji czujników i ich możliwości gromadzenia danych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dotycząca oceny ryzyka w zakresie ochrony prywatności; oceny wpływu na prywatność; architektura systemu; wykaz środków stosowanych w celu informowania osób fizycznych o gromadzeniu dotyczących ich danych identyfikacyjnych przez czujniki;<br>przykłady powiadomień przekazywanych osobom fizycznym o gromadzeniu dotyczących ich danych identyfikacyjnych przez czujniki; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SC-42(04)** | **CZUJNIKI \| POWIADOMIENIE O ZBIERANIU DANYCH** | |
| | **SC-42(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za funkcje czujników]. |
| | **SC-42(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające środki ułatwiające informowanie osób fizycznych o gromadzeniu dotyczących ich danych identyfikacyjnych przez czujniki; możliwości systemu w zakresie zbierania informacji przez czujniki]. |

| | | |
|---|---|---|
| **SC-42(05)** | **CZUJNIKI \| MINIMALIZACJA GROMADZENIA DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-42(05)_ODP** | ***określono czujniki, które są skonfigurowane tak, aby zminimalizować zbieranie niepotrzebnych informacji o osobach;*** |
| | **SC-42(05)** | stosuje się ***<czujniki SC-42(05)_ODP>*** skonfigurowane tak, aby zminimalizować zbieranie niepotrzebnych informacji o osobach. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-42(05)** | **CZUJNIKI \| MINIMALIZACJA GROMADZENIA DANYCH** | |
| | **SC-42(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; polityka i procedury kontroli dostępu; polityka przetwarzania danych identyfikacyjnych;<br>polityka i procedury dotyczące funkcji czujników i ich możliwości gromadzenia danych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja oceny ryzyka związanego z prywatnością; ocena wpływu na prywatność; architektura systemu;<br>wykaz informacji gromadzonych przez czujniki; wykaz konfiguracji czujników, które minimalizują gromadzenie danych identyfikacyjnych (np. ukrywają cechy wyglądu człowieka); zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SC-42(05)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za funkcje czujników]. |
| | **SC-42(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające środki ułatwiające przegląd informacji zbieranych przez czujniki; możliwości systemu w zakresie zbierania informacji przez czujniki]. |

| | | |
|---|---|---|
| **SC-43** | **OGRANICZENIA UŻYCIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-43_ODP** | ***określono komponenty, dla których należy ustanowić ograniczenia w zakresie użytkowania i wytyczne dotyczące wdrażania;*** |

| | | |
|---|---|---|
| **SC-43** | **OGRANICZENIA UŻYCIA** | |
| | **SC-43a.** | dla ***<komponentów SC-43_ODP>*** ustanowiono ograniczenia w użytkowaniu i wytyczne dotyczące wdrażania; |
| | **SC-43b.[01]** | użycie ***<komponentów SC-43_ODP> w*** ramach systemu jest zatwierdzane; |
| | **SC-43b.[02]** | użycie ***<komponentów SC-43_ODP> w*** ramach systemu jest monitorowane; |
| | **SC-43b.[03]** | użycie ***<komponentów SC-43_ODP> w*** ramach systemu jest kontrolowane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-43-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; ograniczenia użytkowania; procedury dotyczące ograniczeń użytkowania; polityka i procedury wdrażania; zapisy dotyczące autoryzacji; zapisy dotyczące monitorowania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-43-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system]. |
| | **SC-43-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące autoryzacji, monitorowania i kontroli wykorzystania komponentów objętych ograniczeniami użytkowania; mechanizmy wspierające lub wdrażające autoryzację, monitorowanie i kontrolę wykorzystania komponentów objętych ograniczeniami użytkowania]. |

| | | |
|---|---|---|
| **SC-44** | **KOMORY DETONACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-44_ODP** | ***określono system, komponent systemu lub inną lokalizację, w której ma być umiejscowiona komora detonacyjna;*** |
| | **SC-44** | w ramach ***<systemu, komponentu systemu lub lokalizacji SC-44_ODP>*** stosuje się komorę detonacyjną. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-44-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące komór detonacyjnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-44-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system]. |
| | **SC-44-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające zdolności w zakresie stosowania komór detonacyjnych]. |

| | | |
|---|---|---|
| **SC-45** | **SYNCHRONIZACJA CZASU SYSTEMOWEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-45** | synchronizacja zegarów systemowych odbywa się wewnątrz systemu oraz pomiędzy systemami i komponentami systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-45** | **SYNCHRONIZACJA CZASU SYSTEMOWEGO** | |
| | **SC-45-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące synchronizacji czasu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-45-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system]. |
| | **SC-45-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające synchronizację czasu w ramach systemu]. |

| | | |
|---|---|---|
| **SC-45(01)** | **SYNCHRONIZACJA CZASU SYSTEMOWEGO \| SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-45(01)_ODP[01]** | ***określono częstotliwość porównywania wewnętrznych zegarów systemowych z wiarygodnym źródłem czasu;*** |
| | **SC-45(01)_ODP[02]** | ***określono wiarygodne źródło czasu, z którym mają być porównywane wewnętrzne zegary systemowe;*** |
| | **SC-45(01)_ODP[03]** | ***określono okres, w którym wewnętrzne zegary systemowe są porównywane z wiarygodnym źródłem czasu;*** |
| | **SC-45(01)(a)** | wewnętrzne zegary systemowe są porównywane z ***<częstotliwością SC-45(01)_ODP[01]>*** z<br>***<wiarygodnym źródłem czasu SC-45(01)_ODP[02]>***; |

| | | |
|---|---|---|
| **SC-45(01)** | **SYNCHRONIZACJA CZASU SYSTEMOWEGO \| SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA** | |
| | **SC-45(01)(b)** | wewnętrzne zegary systemowe są synchronizowane z wiarygodnym źródłem czasu, gdy różnica czasu jest większa niż ***<okres SC-45(01)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-45(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące synchronizacji czasu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-45(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system]. |
| | **SC-45(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające synchronizację czasu w ramach systemu]. |

| | | |
|---|---|---|
| **SC-45(02)** | **SYNCHRONIZACJA CZASU SYSTEMOWEGO \| WTÓRNE ŹRÓDŁO CZASU ODNIESIENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-45(02)(a)** | zidentyfikowano wtórne wiarygodne źródło czasu, które znajduje się w innym regionie geograficznym niż główne wiarygodne źródło czasu; |
| | **SC-45(02)(b)** | wewnętrzne zegary systemowe są synchronizowane z wtórnym wiarygodnym źródłem czasu, jeśli główne źródło czasu jest niedostępne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-45(02)** | **SYNCHRONIZACJA CZASU SYSTEMOWEGO \| WTÓRNE ŹRÓDŁO CZASU ODNIESIENIA** | |
| | **SC-45(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące synchronizacji czasu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-45(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system]. |
| | **SC-45(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające synchronizację czasu systemu z wtórnymi wiarygodnymi źródłami czasu]. |

| | | |
|---|---|---|
| **SC-46** | **EGZEKWOWANIE POLITYKI MIĘDZYDOMENOWEJ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-46_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {fizycznie; logicznie};*** |
| | **SC-46** | wdrożono ***<WYBRANA WARTOŚĆ PARAMETRU SC-46_ODP>*** mechanizm egzekwowania polityki pomiędzy fizycznymi lub sieciowymi interfejsami do celów łączenia domen bezpieczeństwa. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-46** | **EGZEKWOWANIE POLITYKI MIĘDZYDOMENOWEJ** | |
| | **SC-46-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące egzekwowania polityki międzydomenowej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-46-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system]. |
| | **SC-46-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające egzekwowanie stosowania polityki międzydomenowej]. |

| | | |
|---|---|---|
| **SC-47** | **ALTERNATYWNE ŚCIEŻKI KOMUNIKACYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-47_ODP** | ***określono alternatywne ścieżki komunikacyjne dla operacji systemowych oraz dla procesu zarządzania i kontroli nad operacjami systemowymi;*** |
| | **SC-47** | dla operacji systemowych oraz dla procesu zarządzania i kontroli operacyjnej ustanowiono ***<alternatywne ścieżki komunikacyjne SC-47_ODP>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-47** | **ALTERNATYWNE ŚCIEŻKI KOMUNIKACYJNE** | |
| | **SC-47-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące ścieżek komunikacyjnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-47-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu]. |
| | **SC-47-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające alternatywne ścieżki komunikacyjne dla operacji systemowych]. |

| | | |
|---|---|---|
| **SC-48** | **ROZMIESZCZENIE CZUJNIKÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-48_ODP[01]** | ***określono czujniki i narzędzia do monitorowania, które mają zostać przemieszczone do odpowiednich lokalizacji;*** |
| | **SC-48_ODP[02]** | ***określono lokalizacje, do których mają zostać przemieszczone czujniki i narzędzia do monitorowania;*** |
| | **SC-48_ODP[03]** | ***określono warunki lub okoliczności przemieszczenia czujników i narzędzi do monitorowania;*** |
| | **SC-48** | ***<czujniki i narzędzia do monitorowania SC-48_ODP[01]>*** są przemieszczane do<br>***<lokalizacji SC-48_ODP[02]> w <warunkach lub okolicznościach SC-48_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-48** | **ROZMIESZCZENIE CZUJNIKÓW** | |
| | **SC-48-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące przemieszczania czujników i narzędzi do monitorowania; wykaz czujników/narzędzi do monitorowania, które mają być przemieszczone; zapisy dotyczące zabezpieczania zmian konfiguracji; zapisy dotyczące zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-48-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system]. |
| | **SC-48-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające przemieszczanie czujników]. |

| | | |
|---|---|---|
| **SC-48(01)** | **ROZMIESZCZENIE CZUJNIKÓW \| DYNAMICZNE PRZEMIESZCZANIE CZUJNIKÓW LUB URZĄDZEŃ MONITORUJĄCYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-48(01)_ODP[01]** | ***określono czujniki i narzędzia do monitorowania, które mają być dynamicznie przemieszczane;*** |
| | **SC-48(01)_ODP[02]** | ***określono lokalizacje, do których mają być dynamicznie przemieszczane czujniki i narzędzia do monitorowania;*** |
| | **SC-48(01)_ODP[03]** | ***określono warunki lub okoliczności dynamicznego przemieszczenia czujników i narzędzi do monitorowania;*** |

| | | |
|---|---|---|
| **SC-48(01)** | **ROZMIESZCZENIE CZUJNIKÓW \| DYNAMICZNE PRZEMIESZCZANIE CZUJNIKÓW LUB URZĄDZEŃ MONITORUJĄCYCH** | |
| | **SC-48(01)** | ***<czujniki i narzędzia do monitorowania SC-48(01)_ODP[01]>*** są dynamicznie przenoszone do ***<lokalizacji SC-48(01)_ODP[02]>*** w ***<warunkach lub okolicznościach SC-48(01)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-48(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące przemieszczania czujników i narzędzi do monitorowania; wykaz czujników/narzędzi do monitorowania, które mają być przemieszczone; zapisy dotyczące zabezpieczania zmian konfiguracji; zapisy dotyczące zarządzania konfiguracją; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-48(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system]. |
| | **SC-48(01)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające przemieszczanie czujników]. |

| | | |
|---|---|---|
| **SC-49** | **EGZEKWOWANIE SEPARACJI SPRZĘTOWEJ/POLITYKA EGZEKWOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-49_ODP** | ***określono domeny bezpieczeństwa wymagające separacji sprzętowej oraz mechanizmów egzekwowania polityki;*** |
| | **SC-49** | pomiędzy ***<domenami bezpieczeństwa SC-49_ODP>*** wdrożono wymuszane sprzętowo mechanizmy separacji i egzekwowania polityki. |

| | | |
|---|---|---|
| **SC-49** | **EGZEKWOWANIE SEPARACJI SPRZĘTOWEJ/POLITYKA EGZEKWOWANIA** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-49-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące egzekwowania polityki międzydomenowej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-49-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system]. |
| | **SC-49-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające wymuszaną sprzętowo separację domen bezpieczeństwa i egzekwowanie polityki]. |

| | | |
|---|---|---|
| **SC-50** | **EGZEKWOWANIE SEPARACJI PROGRAMOWEJ/POLITYKA EGZEKWOWANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-50_ODP** | ***określono domeny bezpieczeństwa wymagające separacji programowej oraz mechanizmów egzekwowania polityki;*** |
| | **SC-50** | pomiędzy ***<domenami bezpieczeństwa SC-50_ODP>*** wdrożono wymuszane programowo mechanizmy separacji i egzekwowania polityki. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SC-50** | **EGZEKWOWANIE SEPARACJI PROGRAMOWEJ/POLITYKA EGZEKWOWANIA** | |
| | **SC-50-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące egzekwowania polityki międzydomenowej; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-50-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system]. |
| | **SC-50-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające separację programową i egzekwowanie polityki]. |

| | | |
|---|---|---|
| **SC-51** | **OCHRONA SPRZĘTOWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SC-51_ODP[01]** | |
| | **SC-51_ODP[02]** | ***określono osoby upoważnione zaznajomione z procedurami wyłączania i ponownego włączania sprzętowej ochrony przed zapisem;*** |
| | **SC-51a.** | w ***<komponentach oprogramowania układowego systemu SC-51_ODP[01]>*** stosuje się sprzętową ochronę przed zapisem; |
| | **SC-51b.[01]** | wdrożono są specjalne procedury dla ***<upoważnionych osób SC-51_ODP[02]>***, umożliwiające ręczne wyłączenie sprzętowej ochrony przed zapisem w celu modyfikacji oprogramowania układowego; |
| | **SC-51b.[02]** | wdrożono są specjalne procedury dla ***<upoważnionych osób SC-51_ODP[02]>***, umożliwiające ręczne ponowne włączenie sprzętowej ochrony przed zapisem przed powrotem do trybu pracy. |

| | | |
|---|---|---|
| **SC-51** | **OCHRONA SPRZĘTOWA** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SC-51-Badanie** | [WYBÓR SPOŚRÓD: Polityka ochrony systemów i sieci telekomunikacyjnych; procedury dotyczące modyfikacji oprogramowania układowego; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; architektura systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SC-51-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; programiści/integratorzy systemu]. |
| | **SC-51-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące modyfikacji oprogramowania układowego; mechanizmy wspierające lub wdrażające sprzętową ochronę przed zapisem dla oprogramowania układowego]. |

## 4.19. KATEGORIA SI - INTEGRALNOŚĆ SYSTEMU I INFORMACJI

| | | |
|---|---|---|
| **SI-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-01_ODP[01]** | ***określono personel lub role, którym należy przekazać politykę integralności systemu i informacji;*** |
| | **SI-01_ODP[02]** | ***określono personel lub role, którym należy przekazać procedury integralności systemu i informacji;*** |
| | **SI-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **SI-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie polityką i procedurami integralności systemu i informacji;*** |
| | **SI-01_ODP[05]** | ***określono częstotliwość, z jaką polityka integralności systemu i informacji jest przeglądana i aktualizowana;*** |
| | **SI-01_ODP[06]** | ***określono zdarzenia wymagające przeglądu i aktualizacji polityki integralności systemu i informacji;*** |
| | **SI-01_ODP[07]** | ***określono częstotliwość, z jaką dokonuje się przeglądu i aktualizacji procedur integralności systemu i informacji;*** |
| | **SI-01_ODP[08]** | ***określono zdarzenia skutkujące koniecznością przeprowadzenia przeglądu i aktualizacji procedur integralności systemu i informacji;*** |
| | **SI-01a.[01]** | opracowano i udokumentowano politykę integralności systemu i informacji; |
| | **SI-01a.[02]** | polityka integralności systemu i informacji jest rozpowszechniana wśród ***<personelu lub ról SI-01_ODP[01]>***; |

| **SI-01** | **POLITYKA I PROCEDURY** | |
|---|---|---|
| | **SI-01a.[03]** | opracowano i udokumentowano procedury integralności systemu i informacji ułatwiające wdrażanie polityki w tym zakresie oraz związanych z nią zabezpieczeń integralności systemu i informacji; |
| | **SI-01a.[04]** | procedury integralności systemu i informacji są rozpowszechniane wśród<br>***<personelu lub ról SI-01_ODP[02]>***; |
| | **SI-01a.01(a)[01]** | polityka integralności systemu i informacji ***<WYBRANA WARTOŚĆ PARAMETRU SI-01_ODP[03]>*** odnosi się do celu; |
| | **SI-01a.01(a)[02]** | polityka integralności systemu i informacji ***<WYBRANA WARTOŚĆ PARAMETRU SI-01_ODP[03]>*** odnosi się do zakresu; |
| | **SI-01a.01(a)[03]** | polityka integralności systemu i informacji ***<WYBRANA WARTOŚĆ PARAMETRU SI-01_ODP[03]>*** odnosi się do ról; |
| | **SI-01a.01(a)[04]** | polityka integralności systemu i informacji ***<WYBRANA WARTOŚĆ PARAMETRU SI-01_ODP[03]>*** odnosi się do obowiązków; |
| | **SI-01a.01(a)[05]** | polityka integralności systemu i informacji ***<WYBRANA WARTOŚĆ PARAMETRU SI-01_ODP[03]>*** odnosi się do zaangażowania kierownictwa; |
| | **SI-01a.01(a)[06]** | polityka integralności systemu i informacji ***<WYBRANA WARTOŚĆ PARAMETRU SI-01_ODP[03]>*** odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **SI-01a.01(a)[07]** | polityka integralności systemu i informacji ***<WYBRANA WARTOŚĆ PARAMETRU SI-01_ODP[03]>*** odnosi się do zgodności; |
| | **SI-01a.01(b)** | polityka integralności systemu i informacji***<WYBRANA WARTOŚĆ PARAMETRU SI-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |

| | | |
|---|---|---|
| **SI-01** | **POLITYKA I PROCEDURY** | |
| | **SI-01b.** | ***<urzędnik SI-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur integralności systemu i informacji; |
| | **SI-01c.01[01]** | polityka integralności systemu i informacji jest przeglądana i aktualizowana z ***<częstotliwością SI-01_ODP[05]>***; |
| | **SI-01c.01[02]** | polityka integralności systemu i informacji jest przeglądana i aktualizowana po ***<zdarzeniach SI-01_ODP[06]>***; |
| | **SI-01c.02[01]** | procedury integralności systemu i informacji są rozpowszechniane z ***<częstotliwością SI-01_ODP[07]>***; |
| | **SI-01c.02[02]** | procedury integralności systemu i informacji są rozpowszechniane po ***<zdarzeniach SI-01_ODP[08]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za integralność systemu i informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **SI-02** | **USUWANIE USTEREK** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-02_ODP** | ***określono okres, w którym należy zainstalować udostępnione aktualizacje oprogramowania istotne dla bezpieczeństwa;*** |

| | | |
|---|---|---|
| **SI-02** | **USUWANIE USTEREK** | |
| | **SI-02a.[01]** | usterki w systemie są identyfikowane; |
| | **SI-02a.[02]** | usterki w systemie są zgłaszane; |
| | **SI-02a.[03]** | usterki w systemie są korygowane; |
| | **SI-02b.[01]** | aktualizacje oprogramowania usuwające usterki są testowane pod kątem skuteczności przed instalacją; |
| | **SI-02b.[02]** | aktualizacje oprogramowania usuwające usterki są testowane pod kątem potencjalnych niepożądanych skutków przed instalacją; |
| | **SI-02b.[03]** | aktualizacje oprogramowania układowego usuwające usterki są testowane pod kątem skuteczności przed instalacją; |
| | **SI-02b.[04]** | aktualizacje oprogramowania układowego usuwające usterki są testowane pod kątem potencjalnych niepożądanych skutków przed instalacją; |
| | **SI-02c.[01]** | aktualizacje oprogramowania istotne dla bezpieczeństwa są instalowane w ciągu ***<okresu SI-02_ODP>*** od ich wydania; |
| | **SI-02c.[02]** | aktualizacje oprogramowania układowego istotne dla bezpieczeństwa są instalowane w ciągu ***<okresu SI-02_ODP>*** od ich wydania; |
| | **SI-02d.** | usuwanie usterek jest włączone do organizacyjnego procesu zarządzania konfiguracją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SI-02 | USUWANIE USTEREK | |
|---|---|---|
| | **SI-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące usuwania usterek; procedury dotyczące zarządzania konfiguracją; wykaz usterek i podatności w zabezpieczeniach potencjalnie wpływających na system; wykaz ostatnio przeprowadzonych w systemie działań związanych z usuwaniem luk w zabezpieczeniach (np. wykaz zainstalowanych poprawek, dodatków Service Pack, poprawek hot fix i innych aktualizacji oprogramowania mających na celu usunięcie usterek w systemie);<br><br>wyniki testów dotyczących instalacji aktualizacji oprogramowania i oprogramowania układowego w celu usunięcia usterek w systemie; zapisy dotyczące kontroli instalacji/zmian oprogramowania i oprogramowania układowego mających znaczenie dla bezpieczeństwa; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-02-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za usuwanie usterek; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją]. |
| | **SI-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące identyfikowania, zgłaszania i korygowania usterek w systemie; proces organizacyjny dotyczący instalowania aktualizacji oprogramowania i oprogramowania układowego; mechanizmy wspierające lub wdrażające zgłaszanie i korygowanie usterek w systemie; mechanizmy wspierające lub wdrażające testowanie aktualizacji oprogramowania i oprogramowania układowego]. |

| | |
|---|---|
| **SI-02(01)** | **USUWANIE USTEREK \| ZARZĄDZANIE CENTRALNE** |
| | [WYCOFANE: Włączone do PL-09]. |

| | | |
|---|---|---|
| **SI-02(02)** | **USUWANIE USTEREK \| ZAUTOMATYZOWANE USUWANIE USTEREK** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-02(02)_ODP[01]** | ***określono automatyczne mechanizmy pozwalające stwierdzić, czy w komponentach systemu zainstalowane są odpowiednie aktualizacje oprogramowania i oprogramowania układowego dotyczące bezpieczeństwa;*** |
| | **SI-02(02)_ODP[02]** | ***określono częstotliwość, z jaką należy określać, czy w komponentach systemu zainstalowane są odpowiednie aktualizacje oprogramowania i oprogramowania układowego dotyczące bezpieczeństwa;*** |
| | **SI-02(02)** | w komponentach systemu instalowane są odpowiednie aktualizacje oprogramowania i oprogramowania układowego dotyczące bezpieczeństwa z ***<częstotliwością SI-02(02)_ODP[02]>*** przy użyciu ***<mechanizmów automatycznych SI-02(02)_ODP[01]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-02(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące usuwania wad; automatyczne mechanizmy wspierające scentralizowane zarządzanie procesem usuwania usterek;<br>dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-02(02)** | **USUWANIE USTEREK \| ZAUTOMATYZOWANE USUWANIE USTEREK** | |
| | **SI-02(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za usuwanie usterek]. |
| | **SI-02(02)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wykorzystywane do określania stanu komponentów systemu w odniesieniu do usuwania usterek]. |

| | | |
|---|---|---|
| **SI-02(03)** | **USUWANIE USTEREK \| CZAS DO USUNIĘCIA USTERKI/STANDARDY DZIAŁAŃ NAPRAWCZYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-02(03)_ODP** | ***określono wzorce dotyczące podejmowania działań naprawczych;*** |
| | **SI-02(03)(a)** | mierzony jest czas pomiędzy identyfikacją wady a jej usunięciem; |
| | **SI-02(03)(b)** | ustanowiono ***<wzorce SI-02(03)_ODP>*** dotyczące podejmowania działań naprawczych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-02(03)** | **USUWANIE USTEREK \| CZAS DO USUNIĘCIA USTERKI/STANDARDY DZIAŁAŃ NAPRAWCZYCH** | |
| | **SI-02(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące usuwania wad; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz wzorców służących do podejmowania działań naprawczych w odniesieniu do zidentyfikowanych wad;<br>zapisy zawierające znaczniki czasu do celów identyfikacji wad i późniejszych działań związanych z ich usuwaniem; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-02(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za usuwanie usterek]. |
| | **SI-02(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące identyfikacji, zgłaszania i usuwania wad systemu; mechanizmy stosowane do pomiaru czasu pomiędzy identyfikacją wady a jej usunięciem]. |

| | | |
|---|---|---|
| **SI-02(04)** | **USUWANIE USTEREK \| AUTOMATYCZNE ŚCIEŻKI ZARZĄDZANIA NARZĘDZIAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-02(04)_ODP** | ***określono komponenty systemu wymagające narzędzi do automatycznego zarządzania poprawkami w celu ułatwienia usuwania luk w zabezpieczeniach;*** |

| | | |
|---|---|---|
| **SI-02(04)** | **USUWANIE USTEREK \| AUTOMATYCZNE ŚCIEŻKI ZARZĄDZANIA NARZĘDZIAMI** | |
| | **SI-02(04)** | stosuje się automatyczne narzędzia do zarządzania poprawkami, aby ułatwić usuwanie luk bezpieczeństwa w ***<komponentach SI-02(04)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-02(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące usuwania wad; mechanizmy wspierające usuwanie wad i automatyczne aktualizacje oprogramowania układowego;<br>dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz usterek w systemie; zapisy dotyczące ostatnich aktualizacji oprogramowania i oprogramowania układowego dotyczących bezpieczeństwa, które są automatycznie instalowane w komponentach systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-02(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za usuwanie usterek]. |
| | **SI-02(04)-Test** | [WYBÓR SPOŚRÓD: Automatyczne narzędzia do zarządzania poprawkami; mechanizmy wdrażające automatyczne aktualizacje oprogramowania układowego; mechanizmy ułatwiające usuwanie usterek w komponentach systemu]. |

| | | |
|---|---|---|
| **SI-02(05)** | **USUWANIE USTEREK \| AUTOMATYCZNE AKTUALIZACJE APLIKACJI/OPROGRAMOWANIA UKŁADOWEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-02(05)_ODP[01]** | ***określono aktualizacje oprogramowania i oprogramowania układowego dotyczące bezpieczeństwa, które mają być automatycznie instalowane w komponentach systemu;*** |
| | **SI-02(05)_ODP[02]** | ***określono komponenty systemu, które wymagają automatycznego instalowania aktualizacji oprogramowania i oprogramowania układowego dotyczących bezpieczeństwa;*** |
| | **SI-02(05)** | ***<aktualizacje oprogramowania i oprogramowania układowego dotyczące bezpieczeństwa SI-02(05)_ODP[01]>*** są instalowane automatyczne w ***<komponentach systemu SI-02(05)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-02(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące usuwania wad; mechanizmy wspierające usuwanie wad i automatyczne aktualizacje oprogramowania układowego;<br>dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy ostatnich aktualizacji oprogramowania i oprogramowania układowego dotyczących bezpieczeństwa, zainstalowanych automatycznie w komponentach systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-02(05)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za usuwanie usterek]. |

| | | |
|---|---|---|
| **SI-02(05)** | **USUWANIE USTEREK \| AUTOMATYCZNE AKTUALIZACJE APLIKACJI/OPROGRAMOWANIA UKŁADOWEGO** | |
| | **SI-02(05)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wdrażające automatyczne aktualizacje oprogramowania/oprogramowania układowego]. |

| | | |
|---|---|---|
| **SI-02(06)** | **USUWANIE USTEREK \| USUWANIE POPRZEDNICH WERSJI APLIKACJI/OPROGRAMOWANIA UKŁADOWEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-02(06)_ODP** | ***określono komponenty oprogramowania i oprogramowania układowego, które należy usunąć po zainstalowaniu zaktualizowanych wersji;*** |
| | **SI-02(06)** | poprzednie wersje ***<komponentów oprogramowania i oprogramowania układowego SI-02(06)_ODP>*** są usuwane po zainstalowaniu zaktualizowanych wersji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-02(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące usuwania usterek; mechanizmy wspierające usuwanie usterek; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące usuwania oprogramowania i komponentów układowych po zainstalowaniu zaktualizowanych wersji; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-02(06)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za usuwanie usterek]. |

| | | |
|---|---|---|
| **SI-02(06)** | **USUWANIE USTEREK \| USUWANIE POPRZEDNICH WERSJI APLIKACJI/OPROGRAMOWANIA UKŁADOWEGO** | |
| | **SI-02(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające usuwanie poprzednich wersji oprogramowania/oprogramowania układowego]. |

| | | |
|---|---|---|
| **SI-03** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-03_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {sygnaturowy; niesygnaturowy};*** |
| | **SI-03_ODP[02]** | ***określono częstotliwość, z jaką mechanizmy ochrony przed złośliwym kodem wykonują skanowanie;*** |
| | **SI-03_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {punkt końcowy; punkty wejścia i wyjścia z sieci};*** |
| | **SI-03_ODP[04]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {blokowanie złośliwego kodu; poddawanie złośliwego kodu kwarantannie; podejmowanie <działań SI-03_ODP[05]>};*** |
| | **SI-03_ODP[05]** | ***określono działania, które mają być podjęte w odpowiedzi na wykrycie złośliwego kodu (jeśli wybrano);*** |
| | **SI-03_ODP[06]** | ***określono personel lub role, które mają być ostrzegane w przypadku wykrycia złośliwego kodu;*** |
| | **SI-03a.[01]** | mechanizmy ochrony przed złośliwym kodem ***<WYBRANA WARTOŚĆ PARAMETRU SI-03_ODP[01]>*** są wdrożone w punktach wejścia i wyjścia z systemu w celu wykrywania złośliwego kodu; |

| | | |
|---|---|---|
| **SI-03** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM** | |
| | **SI-03a.[02]** | mechanizmy ochrony przed złośliwym kodem ***<WYBRANA WARTOŚĆ PARAMETRU SI-03_ODP[01]>*** są wdrożone w punktach wejścia i wyjścia z systemu w celu usuwania złośliwego kodu; |
| | **SI-03b.** | mechanizmy ochrony przed złośliwym kodem są aktualizowane automatycznie w miarę dostępności nowych wersji zgodnie z organizacyjną polityką i procedurami zarządzania konfiguracją; |
| | **SI-03c.01[01]** | mechanizmy ochrony przed złośliwym kodem są skonfigurowane tak, aby wykonywać okresowe skany systemu z ***<częstotliwością SI-03_ODP[02]>***; |
| | **SI-03c.01[02]** | mechanizmy ochrony przed złośliwym kodem są skonfigurowane tak, aby w czasie rzeczywistym skanować pliki ze źródeł zewnętrznych w ***<WYBRANA WARTOŚĆ PARAMETRU SI-03_ODP[03]>***, gdy pliki te są pobierane, otwierane lub wykonywane zgodnie z polityką organizacyjną; |
| | **SI-03c.02[01]** | mechanizmy ochrony przed złośliwym kodem są skonfigurowane tak, aby w odpowiedzi na wykrycie złośliwego kodu podejmować działanie ***<WYBRANA WARTOŚĆ PARAMETRU SI-03_ODP[04]>***; |
| | **SI-03c.02[02]** | mechanizmy ochrony przed złośliwym kodem są skonfigurowane tak, aby wysyłać alerty do ***<personelu lub ról SI-03_ODP[06]> w*** odpowiedzi na wykrycie złośliwego kodu; |
| | **SI-03d.** | uwzględniono kwestię możliwych fałszywych alarmów podczas wykrywania i usuwania złośliwego kodu oraz wynikający z tego potencjalny wpływ na dostępność systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SI-03 | ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | |
|---|---|---|
| | **SI-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka i procedury zarządzania konfiguracją; procedury dotyczące ochrony przed złośliwym kodem; mechanizmy ochrony przed złośliwym kodem; zapisy dotyczące aktualizacji ochrony przed złośliwym kodem; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wyniki skanowania z mechanizmów ochrony przed złośliwym kodem; zapisy działań zainicjowanych przez mechanizmy ochrony przed złośliwym kodem w odpowiedzi na wykrycie złośliwego kodu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-03-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za ochronę przed złośliwym kodem; personel organizacyjny odpowiedzialny za zarządzanie konfiguracją]. |
| | **SI-03-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania, aktualizowania i konfigurowania mechanizmów ochrony przed złośliwym kodem; procesy organizacyjne dotyczące rozwiązywania problemów związanych z fałszywymi alarmami i wynikającymi z nich potencjalnymi skutkami; mechanizmy wspierające lub wdrażające, aktualizujące i konfigurujące mechanizmy ochrony przed złośliwym kodem; mechanizmy wspierające lub wdrażające skanowanie złośliwego kodu i działania następcze]. |

| SI-03(01) | ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| ZARZĄDZANIE CENTRALNE |
|---|---|
| | [WYCOFANE: Włączone do PL-09]. |

| | |
|---|---|
| **SI-03(02)** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| AUTOMATYCZNE AKTUALIZACJE** |
| | [WYCOFANE: Włączone do SI-03]. |

| | |
|---|---|
| **SI-03(03)** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| NIEUPRZYWILEJOWANI UŻYTKOWNICY** |
| | [WYCOFANE: Włączone do AC-06(10)]. |

| | | |
|---|---|---|
| **SI-03(04)** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| AKTUALIZACJE WYŁĄCZNIE PRZEZ UPRAWNIONYCH UŻYTKOWNIKÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-03(04)** | mechanizmy ochrony przed złośliwym kodem są aktualizowane wyłącznie na polecenie uprzywilejowanego użytkownika. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-03(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące ochrony przed złośliwym kodem;<br>lista uprzywilejowanych użytkowników systemu; dokumentacja projektowa systemu; mechanizmy ochrony przed złośliwym kodem; zapisy dotyczące aktualizacji ochrony przed złośliwym kodem; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-03(04)** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| AKTUALIZACJE WYŁĄCZNIE PRZEZ UPRAWNIONYCH UŻYTKOWNIKÓW** | |
| | **SI-03(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za ochronę przed złośliwym kodem]. |
| | **SI-03(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające zdolności w zakresie ochrony przed złośliwym kodem]. |

| | | |
|---|---|---|
| **SI-03(05)** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE** | |
| | [WYCOFANE: Włączone do MP-07]. | |

| | | |
|---|---|---|
| **SI-03(06)** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| TESTOWANIE I WERYFIKACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-03(06)_ODP** | ***określono częstotliwość, z jaką należy testować mechanizmy ochrony przed złośliwym kodem;*** |
| | **SI-03(06)(a)** | mechanizmy ochrony przed złośliwym kodem są testowane z ***<częstotliwością SI-03(06)_ODP>*** poprzez wprowadzenie do systemu znanego, nieszkodliwego kodu; |
| | **SI-03(06)(b)[01]** | następuje wykrycie (nieszkodliwego kodu testowego); |
| | **SI-03(06)(b)[02]** | następuje zgłoszenie związanego z tym incydentu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SI-03(06) | ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| TESTOWANIE I WERYFIKACJA | |
|---|---|---|
| | **SI-03(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące ochrony przed złośliwym kodem;<br>dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; testy bezpieczeństwa; zapisy stanowiące dowód przeprowadzenia testów bezpieczeństwa na mechanizmach ochrony przed złośliwym kodem; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-03(06)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za ochronę przed złośliwym kodem]. |
| | **SI-03(06)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające testowanie i weryfikację możliwości ochrony przed złośliwym kodem]. |

| SI-03(07) | ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| WYKRYWANIE BEZSYGNATUROWE |
|---|---|
| | [WYCOFANE: Włączone do SI-03]. |

| | | |
|---|---|---|
| **SI-03(08)** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| WYKRYWANIE NIEAUTORYZOWANYCH KOMEND** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-03(08)_ODP[01]** | ***określono komponenty sprzętowe systemu, w przypadku których nieautoryzowane polecenia systemu operacyjnego mają być wykrywane poprzez interfejs programowania aplikacji jądra;*** |
| | **SI-03(08)_ODP[02]** | ***określono nieautoryzowane polecenia systemu operacyjnego, które mają być wykrywane;*** |
| | **SI-03(08)_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {wydawanie ostrzeżeń; kontrolowanie wykonania polecenia; uniemożliwianie wykonania polecenia};*** |
| | **SI-03(08)(a)** | ***<nieautoryzowane polecenia systemu operacyjnego SI-03(08)_ODP[01]>*** są wykrywane poprzez interfejs programowania aplikacji jądra w ***<komponentach sprzętowych systemu SI-03(08)_ODP[02]>***; |
| | **SI-03(08)(b)** | ***<WYBRANA WARTOŚĆ PARAMETRU SI-03(08)_ODP[03]>*** jest wykonywane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-03(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące ochrony przed złośliwym kodem; dokumentacja projektowa systemu; mechanizmy ochrony przed złośliwym kodem; komunikaty ostrzegawcze wysyłane po wykryciu wykonania nieuprawnionego polecenia systemu operacyjnego; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-03(08)** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| WYKRYWANIE NIEAUTORYZOWANYCH KOMEND** | |
| | **SI-03(08)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za ochronę przed złośliwym kodem]. |
| | **SI-03(08)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspomagające lub wdrażające zdolności w zakresie ochrony przed złośliwym kodem; mechanizmy wspomagające lub wdrażające wykrywanie nieautoryzowanych poleceń systemu operacyjnego poprzez interfejs programowania aplikacji jądra]. |

| | | |
|---|---|---|
| **SI-03(09)** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| ZDALNE POLECENIA AUTENTYFIKACYJNE** | |
| | [WYCOFANE: Włączone do AC-17(10)]. | |

| | | |
|---|---|---|
| **SI-03(10)** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| ANALIZA KODU ZŁOŚLIWEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-03(10)_ODP** | ***określono narzędzia i techniki, które należy stosować do analizy cech i zachowania złośliwego kodu;*** |
| | **SI-03(10)(a)** | stosuje się ***<narzędzia i techniki SI-03(10)_ODP> do*** analizy cech i zachowania złośliwego kodu; |
| | **SI-03(10)(b)[01]** | wyniki analizy złośliwego kodu są włączane do organizacyjnych procesów reagowania na incydenty; |
| | **SI-03(10)(b)[02]** | wyniki analizy złośliwego kodu są włączane do organizacyjnych procesów usuwania usterek. |

| | | |
|---|---|---|
| **SI-03(10)** | **ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM \| ANALIZA KODU ZŁOŚLIWEGO** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-03(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące ochrony przed złośliwym kodem; procedury dotyczące reagowania na incydenty; procedury dotyczące usuwania usterek; dokumentacja projektowa systemu; mechanizmy, narzędzia i techniki ochrony przed złośliwym kodem; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wyniki analiz złośliwego kodu; zapisy dotyczące zdarzeń związanych z usuwaniem usterek wynikających z analizy złośliwego kodu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-03(10)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za ochronę przed złośliwym kodem; personel organizacyjny odpowiedzialny za usuwanie usterek; personel organizacyjny odpowiedzialny za reagowanie na incydenty lub zarządzanie nimi]. |
| | **SI-03(10)-Test** | [WYBÓR SPOŚRÓD: Proces organizacyjny w zakresie reagowania na incydenty; proces organizacyjny w zakresie usuwania usterek; mechanizmy wspierające lub wdrażające zdolności w zakresie ochrony przed złośliwym kodem; narzędzia i techniki analizy cech i zachowań złośliwego kodu]. |

| | | |
|---|---|---|
| **SI-04** | **MONITOROWANIE SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04_ODP[01]** | ***określono cele monitorowania, obejmujące wykrywanie ataków oraz oznaki potencjalnych ataków na system;*** |
| | **SI-04_ODP[02]** | ***określono techniki i metody stosowane do identyfikacji nieautoryzowanego użycia systemu;*** |
| | **SI-04_ODP[03]** | ***określono informacje dotyczące monitorowania systemu, które mają być przekazywane wyznaczonemu personelowi lub rolom;*** |
| | **SI-04_ODP[04]** | ***określono personel lub role, którym należy przekazywać informacje dotyczące monitorowania systemu;*** |
| | **SI-04_ODP[05]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{w zależności od potrzeb;***<br>***<częstotliwość SI-04_ODP[06]>};*** |
| | **SI-04_ODP[06]** | ***określono częstotliwość dostarczania informacji dotyczących monitorowania systemu personelowi lub rolom (jeśli wybrano);*** |
| | **SI-04a.01** | system jest monitorowany w celu wykrycia ataków i oznak potencjalnych ataków zgodnie z ***<celami monitorowania SI-04_ODP[01]>***; |
| | **SI-04a.02[01]** | system jest monitorowany w celu wykrycia nieautoryzowanych połączeń lokalnych; |
| | **SI-04a.02[02]** | system jest monitorowany w celu wykrycia nieautoryzowanych połączeń sieciowych; |
| | **SI-04a.02[03]** | system jest monitorowany w celu wykrycia nieautoryzowanych połączeń zdalnych; |

| | | |
|---|---|---|
| **SI-04** | **MONITOROWANIE SYSTEMU** | |
| | **SI-04b.** | nieautoryzowane użycie systemu jest identyfikowane za pomocą ***<technik i metod SI-04_ODP[02]>***; |
| | **SI-04c.01** | w celu zebrania określonych przez organizację istotnych informacji uruchamiane są wewnętrzne funkcje monitorowania lub też wykorzystuje się urządzenia monitorujące rozmieszczone strategicznie w systemie; |
| | **SI-04c.02** | w celu śledzenia określonych rodzajów transakcji będących przedmiotem zainteresowania organizacji uruchamiane są wewnętrzne funkcje monitorowania lub też wykorzystuje się urządzenia monitorujące rozmieszczone doraźnie w systemie; |
| | **SI-04d.[01]** | wykryte zdarzenia są analizowane; |
| | **SI-04d.[02]** | wykryte anomalie są analizowane; |
| | **SI-04e.** | poziom aktywności monitorowania systemu jest dostosowywany w przypadku zmiany ryzyka dotyczącego operacji i aktywów organizacji, osób, innych organizacji lub Państwa; |
| | **SI-04f.** | uzyskano opinię prawną dotyczącą działań związanych z monitorowaniem systemu; |
| | **SI-04g.** | ***<informacje dotyczące monitorowania systemu SI-04_ODP[03]>*** są przekazywane ***<personelowi lub rolom SI-04_ODP[04]> <WYBRANA WARTOŚĆ PARAMETRU SI-04_ODP[05]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| **SI-04** | **MONITOROWANIE SYSTEMU** | |
|---|---|---|
| | **SI-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; strategia ciągłego monitorowania; schemat/plan obiektu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; lokalizacje systemowe, w których rozmieszczone są urządzenia monitorujące; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu]. |
| | **SI-04-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie monitorowania systemu]. |

| **SI-04(01)** | **MONITOROWANIE SYSTEMU \| SYSTEM WYKRYWANIA WŁAMAŃ** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(01)[01]** | poszczególne narzędzia do wykrywania włamań są połączone w jeden system wykrywania włamań, obejmujący cały system informatyczny; |
| | **SI-04(01)[02]** | poszczególne narzędzia do wykrywania włamań są skonfigurowane w ramach jednego systemu wykrywania włamań, obejmującego cały system informatyczny; |

| | | |
|---|---|---|
| **SI-04(01)** | **MONITOROWANIE SYSTEMU \| SYSTEM WYKRYWANIA WŁAMAŃ** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |
| | **SI-04(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemów; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań]. |

| | | |
|---|---|---|
| **SI-04(02)** | **MONITOROWANIE SYSTEMU \| AUTOMATYCZNE NARZĘDZIA I MECHANIZMY ANALIZY W CZASIE RZECZYWISTYM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(02)** | stosuje się automatyczne narzędzia i mechanizmy wspierające analizę zdarzeń w czasie zbliżonym do rzeczywistego. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-04(02)** | **MONITOROWANIE SYSTEMU \| AUTOMATYCZNE NARZĘDZIA I MECHANIZMY ANALIZY W CZASIE RZECZYWISTYM** | |
| | **SI-04(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dotycząca audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; plan programu ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca zarządzania ryzykiem w zakresie ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-04(02)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za reagowanie na incydenty lub zarządzanie nimi]. |
| | **SI-04(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące analizy zdarzeń w czasie zbliżonym do rzeczywistego; procesy organizacyjne dotyczące monitorowania systemu; mechanizmy wspierające<br>lub wdrażające monitorowanie systemu; mechanizmy/narzędzia wspierające lub wdrażające analizę zdarzeń]. |

| | | |
|---|---|---|
| **SI-04(03)** | **MONITOROWANIE SYSTEMU \| AUTOMATYCZNA INTEGRACJA NARZĘDZI I MECHANIZMÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(03)[01]** | do integracji narzędzi i mechanizmów wykrywania włamań z mechanizmami kontroli dostępu wykorzystuje się automatyczne narzędzia i mechanizmy; |
| | **SI-04(03)[02]** | do integracji narzędzi i mechanizmów wykrywania włamań z mechanizmami kontroli przepływu informacji wykorzystuje się automatyczne narzędzia i mechanizmy. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka i procedury kontroli dostępu; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(03)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |

| | | |
|---|---|---|
| **SI-04(03)** | **MONITOROWANIE SYSTEMU \| AUTOMATYCZNA INTEGRACJA NARZĘDZI I MECHANIZMÓW** | |
| | **SI-04(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemu; mechanizmy i narzędzia wspierające lub wdrażające zdolności w zakresie kontroli dostępu i przepływu; mechanizmy i narzędzia wspierające lub wdrażające integrację narzędzi wykrywania włamań z mechanizmami kontroli dostępu i kontroli przepływu informacji]. |

| | | |
|---|---|---|
| **SI-04(04)** | **MONITOROWANIE SYSTEMU \| WEJŚCIOWY/WYJŚCIOWY RUCH TELEKOMUNIKACYJNY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(04)_ODP[01]** | ***określono częstotliwość monitorowania przychodzącego ruchu telekomunikacyjnego pod kątem nietypowych lub nieuprawnionych działań bądź warunków;*** |
| | **SI-04(04)_ODP[02]** | ***określono nietypowe lub nieautoryzowane działania bądź warunki, pod kątem których monitoruje się przychodzący ruch telekomunikacyjny;*** |
| | **SI-04(04)_ODP[03]** | ***określono częstotliwość monitorowania wychodzącego ruchu telekomunikacyjnego pod kątem nietypowych lub nieuprawnionych działań bądź warunków;*** |
| | **SI-04(04)_ODP[04]** | ***określono nietypowe lub nieautoryzowane działania bądź warunki, pod kątem których monitoruje się wychodzący ruch telekomunikacyjny;*** |
| | **SI-04(04)(a)[01]** | określono kryteria nietypowych lub nieuprawnionych działań bądź warunków dla przychodzącego ruchu telekomunikacyjnego; |

| | | |
|---|---|---|
| **SI-04(04)** | **MONITOROWANIE SYSTEMU \| WEJŚCIOWY/WYJŚCIOWY RUCH TELEKOMUNIKACYJNY** | |
| | **SI-04(04)(a)[02]** | określono kryteria nietypowych lub nieuprawnionych działań bądź warunków dla wychodzącego ruchu telekomunikacyjnego; |
| | **SI-04(04)(b)[01]** | przychodzący ruch telekomunikacyjny jest monitorowany z ***<częstotliwością SI-04(04)_ODP[01]>*** pod kątem ***<nietypowych lub nieautoryzowanych działań bądź warunków SI-04(04)_ODP[02]>***; |
| | **SI-04(04)(b)[02]** | wychodzący ruch telekomunikacyjny jest monitorowany z ***<częstotliwością SI-04(04)_ODP[03]>*** pod kątem ***<nietypowych lub nieautoryzowanych działań bądź warunków SI-04(04)_ODP[04]>***; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; protokoły systemowe; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(04)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |

| | | |
|---|---|---|
| **SI-04(04)** | **MONITOROWANIE SYSTEMU \| WEJŚCIOWY/WYJŚCIOWY RUCH TELEKOMUNIKACYJNY** | |
| | **SI-04(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające monitorowanie przychodzącego i wychodzącego ruchu telekomunikacyjnego]. |

| | | |
|---|---|---|
| **SI-04(05)** | **MONITOROWANIE SYSTEMU \| ALERTY SYSTEMOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(05)_ODP[01]** | ***określono personel lub role, które należy zaalarmować w przypadku wystąpienia oznak naruszenia bezpieczeństwa lub potencjalnego naruszenia bezpieczeństwa;*** |
| | **SI-04(05)_ODP[02]** | ***określono oznaki wskazujące na wystąpienie naruszenia bezpieczeństwa;*** |
| | **SI-04(05)** | ***<personel lub role SI-04(05)_ODP[01]>*** otrzymują alert w przypadku wystąpienia<br>***<oznak naruszenia bezpieczeństwa SI-04(05)_ODP[02]>*** generowanych przez system. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-04(05)** | **MONITOROWANIE SYSTEMU \| ALERTY SYSTEMOWE** | |
| | **SI-04(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz personelu wyznaczonego do otrzymywania alertów; dokumentacja dotycząca alertów generowanych na podstawie oznak naruszenia bezpieczeństwa; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-04(05)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny otrzymujący alerty systemowe; personel organizacyjny odpowiedzialny za system wykrywania włamań] |
| | **SI-04(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające alerty dotyczące oznak naruszenia bezpieczeństwa]. |

| | |
|---|---|
| **SI-04(06)** | **MONITOROWANIE SYSTEMU \| OGRANICZANIE NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW** |
| | [WYCOFANE: Włączone do AC-06(10)]. |

| | | |
|---|---|---|
| **SI-04(07)** | **MONITOROWANIE SYSTEMU \| AUTOMATYCZNA ODPOWIEDŹ NA PODEJRZANE ZDARZENIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(07)_ODP[01]** | ***określono personel odpowiedzialny za reagowanie na incydenty (zidentyfikowany z imienia i nazwiska lub pełnionej funkcji), który ma być powiadamiany o wykrytych podejrzanych zdarzeniach;*** |
| | **SI-04(07)_ODP[02]** | ***określono działania najmniej zakłócające pracę systemu, podejmowane w celu wyeliminowania podejrzanych zdarzeń;*** |
| | **SI-04(07)(a)** | powiadomienie o wykrytych podejrzanych zdarzeniach otrzymuje ***<personel reagujący na incydenty SI-04(07)_ODP[01]>***; |
| | **SI-04(07)(b)** | po wykryciu podejrzanych zdarzeń podejmowane są ***<działania najmniej zakłócające pracę systemu SI-04(07)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; alerty i powiadomienia generowane na podstawie wykrytych podejrzanych zdarzeń; zapisy działań podjętych w celu eliminacji podejrzanych zdarzeń; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(07)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programiści systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |

| | | |
|---|---|---|
| **SI-04(07)** | **MONITOROWANIE SYSTEMU \| AUTOMATYCZNA ODPOWIEDŹ NA PODEJRZANE ZDARZENIA** | |
| | **SI-04(07)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające alerty dla personelu reagującego na incydenty; mechanizmy wspierające lub wdrażające działania mające na celu eliminację podejrzanych zdarzeń]. |

| | |
|---|---|
| **SI-04(08)** | **MONITOROWANIE SYSTEMU \| OCHRONA INFORMACJI O MONITOROWANIU** |
| | [WYCOFANE: Włączone do SI-04]. |

| | | |
|---|---|---|
| **SI-04(09)** | **MONITOROWANIE SYSTEMU \| TESTOWANIE NARZĘDZI I MECHANIZMÓW MONITORUJĄCYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(09)_ODP** | ***określono częstotliwość, z jaką należy testować narzędzia i mechanizmy do monitorowania włamań;*** |
| | **SI-04(09)** | narzędzia i mechanizmy do monitorowania włamań są testowane z ***<częstotliwością SI-04(09)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-04(09)** | **MONITOROWANIE SYSTEMU \| TESTOWANIE NARZĘDZI I MECHANIZMÓW MONITORUJĄCYCH** | |
| | **SI-04(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące testowania narzędzi i technik monitorowania systemu; dokumentacja stanowiąca dowód przeprowadzenia testów narzędzi do monitorowania włamań; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(09)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |
| | **SI-04(09)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemów; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemów; mechanizmy wspierające lub wdrażające testowanie narzędzi do monitorowania włamań]. |

| | | |
|---|---|---|
| **SI-04(10)** | **MONITOROWANIE SYSTEMU \| INSPEKCJA ZASZYFROWANYCH KOMUNIKATÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(10)_ODP[01]** | ***określono zaszyfrowany ruch telekomunikacyjny, który ma być widoczny dla narzędzi i mechanizmów monitorowania systemu;*** |
| | **SI-04(10)_ODP[02]** | ***określono narzędzia do monitorowania systemu oraz mechanizmy zapewniające dostęp do zaszyfrowanego ruchu telekomunikacyjnego;*** |

| | | |
|---|---|---|
| **SI-04(10)** | **MONITOROWANIE SYSTEMU \| INSPEKCJA ZASZYFROWANYCH KOMUNIKATÓW** | |
| | **SI-04(10)** | wdrożono środki, dzięki którym ***<zaszyfrowany ruch telekomunikacyjny SI-04(10)_ODP[01]>*** jest widoczny dla ***<narzędzi i mechanizmów monitorowania systemu SI-04(10)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; protokoły systemowe; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(10)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |
| | **SI-04(10)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające widoczność zaszyfrowanego ruchu telekomunikacyjnego dla narzędzi monitorujących]. |

| | | |
|---|---|---|
| **SI-04(11)** | **MONITOROWANIE SYSTEMU \| ANALIZA ANOMALII RUCHU TELEKOMUNIKACYJNEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(11)_ODP** | ***w systemie określono punkty wewnętrzne, w których ma być analizowany ruch telekomunikacyjny;*** |
| | **SI-04(11)[01]** | wychodzący ruch telekomunikacyjny jest analizowany na zewnętrznych interfejsach systemu w celu wykrywania anomalii; |
| | **SI-04(11)[02]** | wychodzący ruch telekomunikacyjny jest analizowany w ***<punktach wewnętrznych SI-04(11)_ODP>*** w celu wykrywania anomalii. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(11)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; schemat sieci; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dzienniki lub zapisy dotyczące monitorowania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(11)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |

| | | |
|---|---|---|
| **SI-04(11)** | **MONITOROWANIE SYSTEMU \| ANALIZA ANOMALII RUCHU TELEKOMUNIKACYJNEGO** | |
| | **SI-04(11)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające analizę ruchu telekomunikacyjnego]. |

| | | |
|---|---|---|
| **SI-04(12)** | **MONITOROWANIE SYSTEMU \| AUTOMATYCZNE ALERTY GENEROWANE PRZEZ ORGANIZACJĘ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(12)_ODP[01]** | ***określono personel lub role, które należy zaalarmować w przypadku wystąpienia oznak nieodpowiedniego lub nietypowego działania mającego wpływ na bezpieczeństwo lub prywatność;*** |
| | **SI-04(12)_ODP[02]** | ***określono automatyczne mechanizmy używane do alarmowania wyznaczonego personelu lub ról;*** |
| | **SI-04(12)_ODP[03]** | ***określono działania, które skutkują zaalarmowaniem wyznaczonego personelu lub ról;*** |
| | **SI-04(12)** | ***<personel lub role SI-04(12)_ODP[01]>*** są alarmowane przy użyciu ***<automatycznych mechanizmów SI-04(12)_ODP[02]>***, jeżeli ***<działania wywołujące alerty SI-04(12)_ODP[03]>*** wskazują na wystąpienie niewłaściwych lub nietypowych działań mających wpływ na bezpieczeństwo lub prywatność. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-04(12)** | **MONITOROWANIE SYSTEMU \| AUTOMATYCZNE ALERTY GENEROWANE PRZEZ ORGANIZACJĘ** | |
| | **SI-04(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>wykaz nieodpowiednich lub nietypowych działań mających wpływ na bezpieczeństwo i prywatność, które wywołują alerty; raporty o podejrzanych działaniach; alerty przekazywane personelowi ds. bezpieczeństwa i prywatności; dzienniki lub zapisy dotyczące monitorowania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-04(12)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programiści systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |
| | **SI-04(12)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemu; automatyczne mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemu; automatyczne mechanizmy wspierające lub wdrażające automatyczne alerty dla personelu ds. bezpieczeństwa]. |

| | | |
|---|---|---|
| **SI-04(13)** | **MONITOROWANIE SYSTEMU \| ANALIZA MODELU RUCHU/ZDARZEŃ TELEKOMUNIKACYJNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(13)(a)[01]** | ruch telekomunikacyjny systemu jest analizowany; |
| | **SI-04(13)(a)[02]** | schematy zdarzeń systemu są analizowane; |
| | **SI-04(13)(b)[01]** | profile odzwierciedlające wspólny ruch są opracowywane; |
| | **SI-04(13)(b)[02]** | profile odzwierciedlające schematy zdarzeń są opracowywane; |
| | **SI-04(13)(c)[01]** | profile ruchu są wykorzystywane do konfigurowania urządzeń monitorujących system; |
| | **SI-04(13)(c)[02]** | profile zdarzeń są wykorzystywane do konfigurowania urządzeń monitorujących system; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(13)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz profili reprezentujących typowe schematy ruchu lub zdarzeń; dokumentacja dotycząca protokołów systemowych; wykaz dopuszczalnych odsetków wyników fałszywie dodatnich i ujemnych; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(13)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |

| | | |
|---|---|---|
| **SI-04(13)** | **MONITOROWANIE SYSTEMU \| ANALIZA MODELU RUCHU/ZDARZEŃ TELEKOMUNIKACYJNYCH** | |
| | **SI-04(13)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające analizę ruchu telekomunikacyjnego i schematów zdarzeń]. |

| | | |
|---|---|---|
| **SI-04(14)** | **MONITOROWANIE SYSTEMU \| WYKRYWANIE ATAKÓW BEZPRZEWODOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(14)[01]** | stosuje się system wykrywania włamań do sieci bezprzewodowej w celu identyfikacji nieautoryzowanych urządzeń bezprzewodowych; |
| | **SI-04(14)[02]** | stosuje się system wykrywania włamań do sieci bezprzewodowej w celu wykrywania prób ataku na system; |
| | **SI-04(14)[03]** | stosuje się system wykrywania włamań do sieci bezprzewodowej w celu wykrywania potencjalnych naruszeń bezpieczeństwa lub włamań do systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(14)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; protokoły systemowe; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-04(14)** | **MONITOROWANIE SYSTEMU \| WYKRYWANIE ATAKÓW BEZPRZEWODOWYCH** | |
| | **SI-04(14)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |
| | **SI-04(14)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań; mechanizmy wspierające lub wdrażające zdolność do wykrywania włamań do sieci bezprzewodowej]. |

| | | |
|---|---|---|
| **SI-04(15)** | **MONITOROWANIE SYSTEMU \| TELEKOMUNIKACJA BEZPRZEWODOWA/PRZEWODOWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(15)** | stosuje się system wykrywania włamań do monitorowania ruchu telekomunikacyjnego w sieciach bezprzewodowych przy transmitowaniu ruchu pomiędzy siecią bezprzewodową a przewodową. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(15)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja dotycząca protokołów systemowych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-04(15)** | **MONITOROWANIE SYSTEMU \| TELEKOMUNIKACJA BEZPRZEWODOWA/PRZEWODOWA** | |
| | **SI-04(15)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |
| | **SI-04(15)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające możliwości wykrywania włamań do sieci bezprzewodowych]. |

| | | |
|---|---|---|
| **SI-04(16)** | **MONITOROWANIE SYSTEMU \| KORELOWANIE INFORMACJI MONITORUJĄCYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(16)** | informacje pochodzące z narzędzi i mechanizmów monitorowania stosowanych w całym systemie są korelowane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(16)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dzienniki lub zapisy dotyczące korelacji zdarzeń; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-04(16)** | **MONITOROWANIE SYSTEMU \| KORELOWANIE INFORMACJI MONITORUJĄCYCH** | |
| | **SI-04(16)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |
| | **SI-04(16)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające korelację informacji z narzędzi monitorujących]. |

| | | |
|---|---|---|
| **SI-04(17)** | **MONITOROWANIE SYSTEMU \| ZINTEGROWANA ŚWIADOMOŚĆ SYTUACYJNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(17)** | informacje z monitorowania działań fizycznych, cybernetycznych i łańcucha dostaw są korelowane w celu uzyskania zintegrowanej świadomości sytuacyjnej w całej organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SI-04(17) | MONITOROWANIE SYSTEMU \| ZINTEGROWANA ŚWIADOMOŚĆ SYTUACYJNA | |
|---|---|---|
| | **SI-04(17)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dzienniki korelacji zdarzeń lub zapisy wynikające z działań fizycznych, cybernetycznych oraz dotyczących łańcucha dostaw;<br>zapisy z audytu systemu; plan zarządzania ryzykiem łańcucha dostaw; inne istotne dokumenty lub zapisy]. |
| | **SI-04(17)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |
| | **SI-04(17)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające korelację informacji z narzędzi monitorujących]. |

| SI-04(18) | MONITOROWANIE SYSTEMU \| ANALIZA RUCHU/ZAPOBIEGANIE EKSFILTRACJI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(18)_ODP** | ***w systemie określono punkty wewnętrzne, w których ma być analizowany ruch telekomunikacyjny;*** |

| | | |
|---|---|---|
| **SI-04(18)** | **MONITOROWANIE SYSTEMU \| ANALIZA RUCHU/ZAPOBIEGANIE EKSFILTRACJI** | |
| | **SI-04(18)[01]** | wychodzący ruch telekomunikacyjny jest analizowany na zewnętrznych interfejsach systemu w celu wykrycia nieautoryzowanego upublicznienia informacji; |
| | **SI-04(18)[02]** | wychodzący ruch telekomunikacyjny jest analizowany w ***<punktach wewnętrznych SI-04(18)_ODP>*** w celu wykrycia nieautoryzowanego upublicznienia informacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(18)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; schemat sieci; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dzienniki lub zapisy dotyczące monitorowania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(18)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; personel organizacyjny odpowiedzialny za system wykrywania włamań]. |
| | **SI-04(18)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające możliwości wykrywania włamań i monitorowania systemu; mechanizmy wspierające lub wdrażające analizę wychodzącego ruchu telekomunikacyjnego]. |

| | | |
|---|---|---|
| **SI-04(19)** | **MONITOROWANIE SYSTEMU \| RYZYKO ZE STRONY OSÓB** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(19)_ODP[01]** | ***określono dodatkowe narzędzia do monitorowania osób, które zostały zidentyfikowane jako stwarzające podwyższony poziom ryzyka;*** |
| | **SI-04(19)_ODP[02]** | ***określono źródła identyfikujące osoby, które stwarzają podwyższony poziom ryzyka;*** |
| | **SI-04(19)** | wdrożono ***<dodatkowe narzędzia do monitorowania SI-04(19)_ODP[01]>*** osób, które zostały zidentyfikowane przez ***<źródła SI-04(19)_ODP[02]>*** jako stwarzające podwyższony poziom ryzyka. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(19)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące monitorowania systemu; dokumentacja projektowa systemu; dokumentacja narzędzi i technik monitorowania; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-04(19)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu; radca prawny; urzędnicy ds. zasobów ludzkich; personel organizacyjny odpowiedzialny za bezpieczeństwo personelu]. |
| | **SI-04(19)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie monitorowania systemu]. |

| | | |
|---|---|---|
| **SI-04(20)** | **MONITOROWANIE SYSTEMU \| UPRZYWILEJOWANI UŻYTKOWNICY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(20)_ODP** | ***określono dodatkowe narzędzia do monitorowania użytkowników uprzywilejowanych;*** |
| | **SI-04(20)** | wdrożono ***<dodatkowe narzędzia do monitorowania SI-04(20)_ODP>*** użytkowników uprzywilejowanych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(20)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dzienniki lub zapisy monitorowania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(20)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu]. |
| | **SI-04(20)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie monitorowania systemu]. |

| | | |
|---|---|---|
| **SI-04(21)** | **MONITOROWANIE SYSTEMU \| OKRESY PRÓBNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(21)_ODP[01]** | ***określono dodatkowe narzędzia do monitorowania, które należy stosować wobec osób zatrudnionych na okres próbny;*** |
| | **SI-04(21)_ODP[02]** | ***określono okres próbny dla poszczególnych osób;*** |
| | **SI-04(21)** | stosuje się ***<dodatkowy monitoring SI-04(21)_ODP[01]>*** osób podczas ***<okresu próbnego SI-04(21)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(21)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dzienniki lub zapisy dotyczące monitorowania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(21)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu]. |
| | **SI-04(21)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie monitorowania systemu]. |

| | | |
|---|---|---|
| **SI-04(22)** | **MONITOROWANIE SYSTEMU \| NIEAUTORYZOWANE USŁUGI SIECIOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(22)_ODP[01]** | ***określono procesy autoryzacji lub zatwierdzania usług sieciowych;*** |
| | **SI-04(22)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {przeprowadzanie audytu; alarmowanie <personelu lub ról SI-04(22)_ODP[03]>};*** |
| | **SI-04(22)_ODP[03]** | ***określono personel lub role alarmowane w przypadku wykrycia usług sieciowych, które nie zostały autoryzowane lub zatwierdzone w ramach procesów autoryzacji lub zatwierdzania (jeśli wybrano);*** |
| | **SI-04(22)(a)** | usługi sieciowe, które nie zostały autoryzowane lub zatwierdzone w ramach ***<procesów autoryzacji lub zatwierdzania SI-04(22)_ODP[01]>*** są wykrywane; |
| | **SI-04(22)(b)** | w przypadku wykrycia usług sieciowych, które nie zostały autoryzowane lub zatwierdzone w ramach procesów autoryzacji lub zatwierdzania, inicjuje się ***<WYBRANA WARTOŚĆ PARAMETRU SI-04(22)_ODP[02]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-04(22)** | **MONITOROWANIE SYSTEMU \| NIEAUTORYZOWANE USŁUGI SIECIOWE** | |
| | **SI-04(22)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; udokumentowana autoryzacja/zatwierdzenie usług sieciowych; powiadomienia lub alerty o nieautoryzowanych usługach sieciowych; dzienniki lub zapisy dotyczące monitorowania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(22)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie systemu]. |
| | **SI-04(22)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie monitorowania systemu; mechanizmy audytu usług sieciowych; mechanizmy dostarczania alertów]. |

| | | |
|---|---|---|
| **SI-04(23)** | **MONITOROWANIE SYSTEMU \| KOMPUTER GŁÓWNY (HOST)** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(23)_ODP[01]** | ***określono mechanizmy monitorowania oparte na hostach, które mają być wdrożone w komponentach systemu;*** |
| | **SI-04(23)_ODP[02]** | ***określono komponenty systemu, w których mają być wdrożone mechanizmy monitorowania oparte na hostach;*** |

| | | |
|---|---|---|
| **SI-04(23)** | **MONITOROWANIE SYSTEMU \| KOMPUTER GŁÓWNY (HOST)** | |
| | **SI-04(23)** | ***<mechanizmy monitorowania oparte na hostach SI-04(23)_ODP[01]>*** są wdrożone w ***<elementach systemu SI-04(23)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(23)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu; dokumentacja projektowa systemu; mechanizmy monitorowania oparte na hostach; dokumentacja dotycząca narzędzi i technik monitorowania systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista komponentów systemu wymagających monitorowania opartego na hostach; dzienniki lub zapisy z monitorowania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(23)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny instalujący,<br>konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie hostów systemu]. |
| | **SI-04(23)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania systemu; mechanizmy wspierające lub wdrażające zdolności w zakresie monitorowania opartego na hostach]. |

| | | |
|---|---|---|
| **SI-04(24)** | **MONITOROWANIE SYSTEMU \| WSKAŹNIKI RYZYKA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(24)_ODP[01]** | ***określono źródła, które dostarczają wskaźników ryzyka;*** |

| | | |
|---|---|---|
| **SI-04(24)** | **MONITOROWANIE SYSTEMU \| WSKAŹNIKI RYZYKA** | |
| | **SI-04(24)_ODP[02]** | ***określono personel lub role, którym przekazywane są wskaźniki ryzyka;*** |
| | **SI-04(24)[01]** | wskaźniki ryzyka dostarczane przez ***<źródła SI-04(24)_ODP[01]>*** są wykrywane; |
| | **SI-04(24)[02]** | wskaźniki ryzyka dostarczane przez ***<źródła SI-04(24)_ODP[01]>*** są gromadzone; |
| | **SI-04(24)[03]** | wskaźniki ryzyka dostarczane przez ***<źródła SI-04(24)_ODP[01]>*** są przekazywane do ***<personelu lub ról SI-04(24)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(24)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dzienniki lub zapisy dotyczące monitorowania systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(24)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie hostów systemu]. |
| | **SI-04(24)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania systemu; procesy organizacyjne dotyczące wykrywania, gromadzenia, dystrybucji i wykorzystywania wskaźników ryzyka; mechanizmy wspierające lub wdrażające zdolności w zakresie monitorowania systemu; mechanizmy wspierające lub wdrażające mechanizmy odkrywania, gromadzenia, dystrybucji i wykorzystywania wskaźników ryzyka]. |

| | | |
|---|---|---|
| **SI-04(25)** | **MONITOROWANIE SYSTEMU \| ANALIZY OPTYMALIZACJI RUCHU SIECIOWEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-04(25)[01]** | zapewniony jest dostęp do informacji o ruchu sieciowym na zewnętrznych interfejsach systemu w celu optymalizacji działania urządzeń monitorujących; |
| | **SI-04(25)[02]** | zapewniony jest dostęp do informacji o ruchu sieciowym na wewnętrznych interfejsach systemu w celu optymalizacji działania urządzeń monitorujących. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-04(25)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące monitorowania systemu; dokumentacja projektowa systemu; dokumentacja dotycząca narzędzi i technik monitorowania; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dzienniki lub zapisy dotyczące monitorowania systemu; architektura systemu; zapisy z audytu systemu; raporty dotyczące ruchu sieciowego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-04(25)-Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu; personel organizacyjny instalujący, konfigurujący lub utrzymujący system; personel organizacyjny odpowiedzialny za monitorowanie hostów systemu]. |

| | | |
|---|---|---|
| **SI-04(25)** | **MONITOROWANIE SYSTEMU \| ANALIZY OPTYMALIZACJI RUCHU SIECIOWEGO** | |
| | **SI-04(25)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące monitorowania systemu; procesy organizacyjne dotyczące wykrywania, gromadzenia, dystrybucji i wykorzystywania wskaźników ryzyka; mechanizmy wspierające lub wdrażające zdolności w zakresie monitorowania systemu; mechanizmy wspierające lub wdrażające mechanizmy odkrywania, gromadzenia, dystrybucji i wykorzystywania wskaźników ryzyka]. |

| | | |
|---|---|---|
| **SI-05** | **ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-05_ODP[01]** | ***określono organizacje zewnętrzne, od których organizacja na bieżąco otrzymuje alerty, porady i dyrektywy dotyczące bezpieczeństwa systemu;*** |
| | **SI-05_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{<personel lub role SI-05_ODP[03]>; <elementy SI-05_ODP[04]>; <organizacje zewnętrzne SI-05_ODP[05]>};*** |
| | **SI-05_ODP[03]** | ***określono personel lub role, które mają otrzymywać alerty, porady i dyrektywy dotyczące bezpieczeństwa (jeśli wybrano);*** |
| | **SI-05_ODP[04]** | ***określono elementy w ramach organizacji, do których mają być przekazywane alerty, porady i dyrektywy dotyczące bezpieczeństwa (jeśli wybrano);*** |
| | **SI-05_ODP[05]** | ***określono organizacje zewnętrzne, do których mają być przekazywane alerty, porady i dyrektywy dotyczące bezpieczeństwa (jeśli wybrano);*** |
| | **SI-05a.** | alerty, porady i dyrektywy dotyczące bezpieczeństwa systemu otrzymywane są na bieżąco od ***<organizacji zewnętrznych SI-05_ODP[01]>***; |

| | | |
|---|---|---|
| **SI-05** | **ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY** | |
| | **SI-05b.** | w razie potrzeby generowane są wewnętrzne alerty, porady i dyrektywy dotyczące bezpieczeństwa; |
| | **SI-05c.** | alerty, porady i dyrektywy dotyczące bezpieczeństwa są przekazywane do ***<WYBRANA WARTOŚĆ PARAMETRU SI-05_ODP[02]>***; |
| | **SI-05d.** | dyrektywy dotyczące bezpieczeństwa są wdrażane w ustalonych ramach czasowych lub w przypadku powiadomienia organizacji wydającej o zakresie występujących niezgodności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące alertów, porad i dyrektyw dotyczących bezpieczeństwa; zapisy dotyczące alertów, porad i dyrektyw dotyczących bezpieczeństwa; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za alerty i porady w zakresie bezpieczeństwa; personel organizacyjny wdrażający, obsługujący, utrzymujący i eksploatujący system; personel organizacyjny, elementy organizacyjne lub organizacje zewnętrzne, do których mają być przekazywane alerty, porady i dyrektywy; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SI-05-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania, otrzymywania, generowania, rozpowszechniania i przestrzegania alertów, porad i dyrektyw dotyczących bezpieczeństwa; mechanizmy wspierające lub wdrażające definiowanie, otrzymywanie, generowanie i rozpowszechnianie alertów, porad i dyrektyw dotyczących bezpieczeństwa; mechanizmy wspierające lub wdrażające dyrektywy dotyczące bezpieczeństwa]. |

| | | |
|---|---|---|
| **SI-05(01)** | **ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY \| AUTOMATYCZNE ALERTY I PORADY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-05(01)_ODP** | ***określono automatyczne mechanizmy wykorzystywane do udostępniania informacji o alertach i poradach dotyczących bezpieczeństwa w całej organizacji;*** |
| | **SI-05(01)** | do udostępniania informacji o alertach i poradach dotyczących bezpieczeństwa w całej organizacji wykorzystuje się ***<mechanizmy automatyczne SI-05(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-05(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące alertów, porad i dyrektyw dotyczących bezpieczeństwa; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; automatyczne mechanizmy wspierające proces udostępniania informacji o alertach i poradach dotyczących bezpieczeństwa; zapisy dotyczące alertów i porad dotyczących bezpieczeństwa; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-05(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za alerty i porady dotyczące bezpieczeństwa; personel organizacyjny wdrażający, obsługujący, utrzymujący i eksploatujący system; personel organizacyjny, elementy organizacyjne lub organizacje zewnętrzne, do których mają być przekazywane alerty i porady;<br>administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |

| | | |
|---|---|---|
| **SI-05(01)** | **ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY \| AUTOMATYCZNE ALERTY I PORADY** | |
| | **SI-05(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania, otrzymywania, generowaniu i rozpowszechniania alertów i porad dotyczących bezpieczeństwa; automatyczne mechanizmy wspierające lub wdrażające rozpowszechnianie alertów i porad dotyczących bezpieczeństwa]. |

| | | |
|---|---|---|
| **SI-06** | **WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-06_ODP[01]** | ***określono funkcje bezpieczeństwa, które mają być weryfikowane pod kątem poprawności działania;*** |
| | **SI-06_ODP[02]** | ***określono funkcje ochrony prywatności, które mają być weryfikowane pod kątem poprawności działania;*** |
| | **SI-06_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{<stany przejściowe systemu SI-06_ODP[04]>; na polecenie użytkownika z odpowiednimi uprawnieniami; <częstotliwość SI-06_ODP[05]>};*** |
| | **SI-06_ODP[04]** | ***określono stany przejściowe systemu wymagające weryfikacji funkcji bezpieczeństwa i ochrony prywatności (jeśli wybrano);*** |
| | **SI-06_ODP[05]** | ***określono częstotliwość, z jaką należy sprawdzać prawidłowe działanie funkcji bezpieczeństwa i ochrony prywatności (jeśli wybrano);*** |
| | **SI-06_ODP[06]** | ***określono personel lub role, które mają być powiadamiane o nieudanych testach funkcji bezpieczeństwa i ochrony prywatności;*** |
| | **SI-06_ODP[07]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {wyłączenie systemu; ponowne uruchomienie systemu; <działania alternatywne SI-06_ODP[08]>};*** |

| | | |
|---|---|---|
| **SI-06** | **WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **SI-06_ODP[08]** | ***określono działania alternatywne, które mają być wykonane w przypadku wykrycia anomalii (jeśli wybrano);*** |
| | **SI-06a.[01]** | ***<funkcje bezpieczeństwa SI-06_ODP[01]>*** są weryfikowane pod kątem poprawności działania; |
| | **SI-06a.[02]** | ***<funkcje ochrony prywatności SI-06_ODP[02]>*** są weryfikowane pod kątem poprawności działania; |
| | **SI-06b.[01]** | ***<funkcje bezpieczeństwa SI-06_ODP[01]>*** są weryfikowane ***<WYBRANA WARTOŚĆ PARAMETRU SI-06_ODP[03]>;*** |
| | **SI-06b.[02]** | ***<funkcje ochrony prywatności SI-06_ODP[02]>*** są weryfikowane ***<WYBRANA WARTOŚĆ PARAMETRU SI-06_ODP[03]>;*** |
| | **SI-06c.[01]** | ***<personel lub role SI-06_ODP[06]>*** otrzymują powiadomienie o nieudanych testach funkcji bezpieczeństwa; |
| | **SI-06c.[02]** | ***<personel lub role SI-06_ODP[06]>*** otrzymują powiadomienie o nieudanych testach funkcji ochrony prywatności; |
| | **SI-06d.** | w przypadku wykrycia anomalii inicjuje się ***<WYBRANA WARTOŚĆ PARAMETRU SI-06_ODP[07]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące weryfikacji funkcji bezpieczeństwa i prywatności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; alerty/powiadomienia o nieudanych testach funkcji bezpieczeństwa; wykaz stanów przejściowych systemu wymagających weryfikacji funkcji bezpieczeństwa; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-06** | **WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI** | |
| | **SI-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację funkcji bezpieczeństwa i prywatności; personel organizacyjny wdrażający, obsługujący i utrzymujący system; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; programista systemu]. |
| | **SI-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące weryfikacji funkcji bezpieczeństwa i ochrony prywatności; mechanizmy wspierające lub wdrażające zdolności w zakresie weryfikacji funkcji bezpieczeństwa i ochrony prywatności]. |

| | |
|---|---|
| **SI-06(01)** | **WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| POWIADOMIENIE O NIEUDANYCH TESTACH BEZPIECZEŃSTWA** |
| | [WYCOFANE: Włączone do SI-06]. |

| | | |
|---|---|---|
| **SI-06(02)** | **WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| WSPARCIE AUTOMATYZACYJNE BADAŃ ROZPROSZONYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-06(02)[01]** | wdrożono automatyczne mechanizmy wspierające zarządzanie rozproszonymi testami funkcji bezpieczeństwa; |
| | **SI-06(02)[02]** | wdrożono automatyczne mechanizmy wspierające zarządzanie rozproszonymi testami funkcji ochrony prywatności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-06(02)** | **WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| WSPARCIE AUTOMATYZACYJNE BADAŃ ROZPROSZONYCH** | |
| | **SI-06(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące weryfikacji funkcji bezpieczeństwa i prywatności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-06(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację funkcji bezpieczeństwa i prywatności; personel organizacyjny wdrażający, obsługujący i utrzymujący system; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-06(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące weryfikacji funkcji bezpieczeństwa i ochrony prywatności; automatyczne mechanizmy wspierające lub wdrażające zarządzanie rozproszonymi testami funkcji bezpieczeństwa i ochrony prywatności]. |

| | | |
|---|---|---|
| **SI-06(03)** | **WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| RAPORT Z WYNIKÓW WERYFIKACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-06(03)_ODP** | ***określono personel lub role wyznaczone do odbioru wyników weryfikacji funkcji bezpieczeństwa i ochrony prywatności;*** |
| | **SI-06(03)[01]** | wyniki weryfikacji funkcji bezpieczeństwa są zgłaszane do ***<personelu lub ról SI-06(03)_ODP>***; |

| | | |
|---|---|---|
| **SI-06(03)** | **WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI \| RAPORT Z WYNIKÓW WERYFIKACJI** | |
| | **SI-06(03)[02]** | wyniki weryfikacji funkcji ochrony prywatności są zgłaszane do ***<personelu lub ról SI-06(03)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-06(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące weryfikacji funkcji bezpieczeństwa i ochrony prywatności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; sprawozdania z wyników weryfikacji funkcji bezpieczeństwa i ochrony prywatności; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-06(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację funkcji bezpieczeństwa i ochrony prywatności; personel organizacyjny otrzymujący sprawozdania z weryfikacji funkcji bezpieczeństwa i ochrony prywatności; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-06(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące raportowania wyników weryfikacji funkcji bezpieczeństwa i ochrony prywatności; mechanizmy wspierające lub wdrażające raportowanie wyników weryfikacji funkcji bezpieczeństwa i ochrony prywatności]. |

| | | |
|---|---|---|
| **SI-07** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07_ODP[01]** | ***określono oprogramowanie wymagające stosowania narzędzi do weryfikacji integralności w celu wykrywania nieautoryzowanych zmian;*** |

| SI-07 | APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | |
|---|---|---|
| | **SI-07_ODP[02]** | ***określono oprogramowanie układowe wymagające stosowania narzędzi do weryfikacji integralności w celu wykrywania nieautoryzowanych zmian;*** |
| | **SI-07_ODP[03]** | ***określono informacje wymagające stosowania narzędzi do weryfikacji integralności w celu wykrywania nieautoryzowanych zmian;*** |
| | **SI-07_ODP[04]** | ***określono działania, które należy podjąć w przypadku wykrycia nieautoryzowanych zmian w oprogramowaniu;*** |
| | **SI-07_ODP[05]** | ***określono działania, które należy podjąć w przypadku wykrycia nieautoryzowanych zmian w oprogramowaniu układowym;*** |
| | **SI-07_ODP[06]** | ***określono działania, które należy podjąć w przypadku wykrycia nieautoryzowanych zmian w informacji;*** |
| | **SI-07a.[01]** | stosuje się narzędzia do weryfikacji integralności w celu wykrywania nieautoryzowanych zmian w ***<oprogramowaniu SI-07_ODP[01]>***; |
| | **SI-07a.[02]** | stosuje się narzędzia do weryfikacji integralności w celu wykrywania nieautoryzowanych zmian w ***<oprogramowaniu układowym SI-07_ODP[02]>***; |
| | **SI-07a.[03]** | stosuje się narzędzia do weryfikacji integralności w celu wykrywania nieautoryzowanych zmian w ***<informacji SI-07_ODP[03]>***; |
| | **SI-07b.[01]** | w przypadku wykrycia nieautoryzowanych zmian w oprogramowaniu podejmowane są ***<działania SI-07_ODP[04]>***; |
| | **SI-07b.[02]** | w przypadku wykrycia nieautoryzowanych zmian w oprogramowaniu układowym podejmowane są ***<działania SI-07_ODP[05]>***; |
| | **SI-07b.[03]** | w przypadku wykrycia nieautoryzowanych zmian w informacji podejmowane są ***<działania SI-07_ODP[06]>***; |

| | | |
|---|---|---|
| **SI-07** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące integralności oprogramowania, oprogramowania układowego i informacji; polityka przetwarzania danych identyfikacyjnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; narzędzia do weryfikacji integralności i związana z nimi dokumentacja; zapisy generowane lub inicjowane przez narzędzia do weryfikacji integralności dotyczące nieautoryzowanych zmian w oprogramowaniu, oprogramowaniu układowym i informacjach; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oprogramowanie, oprogramowanie układowe lub integralność informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu/sieci]. |
| | **SI-07-Test** | [WYBÓR SPOŚRÓD: Narzędzia do weryfikacji oprogramowania, oprogramowania układowego i integralności informacji]. |

| | | |
|---|---|---|
| **SI-07(01)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| KONTROLE INTEGRALNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(01)_ODP[01]** | ***określono oprogramowanie, które ma być poddawane kontroli integralności;*** |

| | | |
|---|---|---|
| **SI-07(01)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| KONTROLE INTEGRALNOŚCI** | |
| | **SI-07(01)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {przy uruchomieniu; przy <stanach przejściowych lub zdarzeniach dotyczących bezpieczeństwa SI-07(01)_ODP[03]>; <częstotliwość SI-07(01)_ODP[04]>};*** |
| | **SI-07(01)_ODP[03]** | ***określono stany przejściowe lub zdarzenia dotyczące bezpieczeństwa wymagające kontroli integralności (w oprogramowaniu) (jeśli wybrano);*** |
| | **SI-07(01)_ODP[04]** | ***określono częstotliwość, z jaką ma być przeprowadzana kontrola integralności (w oprogramowaniu) (jeśli wybrano);*** |
| | **SI-07(01)_ODP[05]** | ***określono oprogramowanie układowe, w którym ma być przeprowadzona kontrola integralności;*** |
| | **SI-07(01)_ODP[06]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {przy uruchomieniu; przy <stanach przejściowych lub zdarzeniach dotyczących bezpieczeństwa SI-07(01)_ODP[07]>; <częstotliwość SI-07(01)_ODP[08]>};*** |
| | **SI-07(01)_ODP[07]** | ***określono stany przejściowe lub zdarzenia dotyczące bezpieczeństwa, wymagające kontroli integralności (w oprogramowaniu układowym) (jeśli wybrano);*** |
| | **SI-07(01)_ODP[08]** | ***określono częstotliwość, z jaką ma być przeprowadzana kontrola integralności (w oprogramowaniu układowym) (jeśli wybrano);*** |
| | **SI-07(01)_ODP[09]** | ***określono informacje, które mają być objęte kontrolą integralności;*** |
| | **SI-07(01)_ODP[10]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {przy uruchamianiu; przy <SI-07(01)_ODP[11] stanach przejściowych lub zdarzeniach istotnych dla bezpieczeństwa>; <częstotliwość SI-07(01)_ODP[12]>};*** |

| | | |
|---|---|---|
| **SI-07(01)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| KONTROLE INTEGRALNOŚCI** | |
| | **SI-07(01)_ODP[11]** | ***określono stany przejściowe lub zdarzenia dotyczące bezpieczeństwa, wymagające kontroli integralności (informacji) (jeśli wybrano);*** |
| | **SI-07(01)_ODP[12]** | ***określono częstotliwość, z jaką należy przeprowadzać kontrolę integralności (informacji) (jeśli wybrano);*** |
| | **SI-07(01)[01]** | przeprowadzana jest kontrola integralności ***<oprogramowania SI-07(01)_ODP[01]>*** ***<WYBRANA WARTOŚĆ PARAMETRU SI-07(01)_ODP[02]>***; |
| | **SI-07(01)[02]** | przeprowadzana jest kontrola integralności ***<oprogramowania układowego SI-07(01)_ODP[05]>*** ***<WYBRANA WARTOŚĆ PARAMETRU SI-07(01)_ODP[06]>***; |
| | **SI-07(01)[03]** | przeprowadzana jest kontrola integralności ***<informacji SI-07(01)_ODP[09]>*** ***<WYBRANA WARTOŚĆ PARAMETRU SI-07(01)_ODP[10]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące testowania oprogramowania, oprogramowania układowego i integralności informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; narzędzia do weryfikacji integralności i związana z nimi dokumentacja; zapisy dotyczące skanowania integralności; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-07(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oprogramowanie, oprogramowanie układowe lub integralność informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |

| | | |
|---|---|---|
| **SI-07(01)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| KONTROLE INTEGRALNOŚCI** | |
| | **SI-07(01)-Test** | [WYBÓR SPOŚRÓD: Narzędzia do weryfikacji oprogramowania, oprogramowania układowego i integralności informacji]. |

| | | |
|---|---|---|
| **SI-07(02)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| AUTOMATYCZNE POWIADOMIENIA O NARUSZENIACH INTEGRALNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(02)_ODP** | ***określono personel lub role, do których należy kierować powiadomienia o wykryciu rozbieżności podczas weryfikacji integralności;*** |
| | **SI-07(02)** | stosuje się automatyczne narzędzia, które dostarczają powiadomienia dla ***<personelu lub ról SI-07(02)_ODP>***<br>w przypadku wykrycia rozbieżności przy weryfikacji integralności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące oprogramowania, oprogramowania układowego i integralności informacji; polityka przetwarzania danych identyfikacyjnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; narzędzia do weryfikacji integralności i związana z nimi dokumentacja; zapisy dotyczące skanowania integralności; automatyczne narzędzia wspierające alarmy i powiadomienia o rozbieżnościach w zakresie integralności; powiadomienia przekazywane po wykryciu rozbieżności podczas weryfikacji integralności; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-07(02)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| AUTOMATYCZNE POWIADOMIENIA O NARUSZENIACH INTEGRALNOŚCI** | |
| | **SI-07(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oprogramowanie, oprogramowanie układowe lub integralność informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy systemu; twórcy oprogramowania]. |
| | **SI-07(02)-Test** | [WYBÓR SPOŚRÓD: Narzędzia do weryfikacji integralności oprogramowania, oprogramowania układowego i informacji; mechanizmy zapewniające powiadomienia o rozbieżnościach w zakresie integralności]. |

| | | |
|---|---|---|
| **SI-07(03)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| NARZĘDZIA DO CENTRALNEGO ZARZĄDZANIA INTEGRALNOŚCIĄ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(03)** | stosuje się centralnie zarządzane narzędzia do weryfikacji integralności. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące oprogramowania, oprogramowania układowego i integralności informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>narzędzia do weryfikacji integralności i związana z nimi dokumentacja; zapisy dotyczące skanowania integralności; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-07(03)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| NARZĘDZIA DO CENTRALNEGO ZARZĄDZANIA INTEGRALNOŚCIĄ** | |
| | **SI-07(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za centralne zarządzanie narzędziami weryfikacji integralności; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SI-07(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające centralne zarządzanie narzędziami weryfikacji integralności]. |

| | | |
|---|---|---|
| **SI-07(04)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| OCHRONA PRZED NARUSZENIAMI** | |
| | [WYCOFANE: Włączone do SR-09]. | |

| | | |
|---|---|---|
| **SI-07(05)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| AUTOMATYCZNA ODPOWIEDŹ NA NARUSZENIA INTEGRALNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(05)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {wyłączenie systemu; ponowne uruchomienie systemu; wdrożenie <zabezpieczeń SI-07(05)_ODP[02]>};*** |
| | **SI-07(05)_ODP[02]** | ***określono zabezpieczenia, które mają być wdrażane automatycznie w przypadku wykrycia naruszeń integralności (jeśli wybrano);*** |
| | **SI-07(05)** | następuje automatyczne wykonanie ***<WYBRANA WARTOŚĆ PARAMETRU SI-07(05)_ODP[01]>***<br>w przypadku wykrycia naruszeń integralności. |

| | | |
|---|---|---|
| **SI-07(05)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| AUTOMATYCZNA ODPOWIEDŹ NA NARUSZENIA INTEGRALNOŚCI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące oprogramowania, oprogramowania układowego i integralności informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>narzędzia do weryfikacji integralności i związana z nimi dokumentacja; zapisy dotyczące skanowania integralności; zapisy dotyczące kontroli integralności i reakcji na naruszenia integralności; zapisy z audytów; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-07(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oprogramowanie, oprogramowanie układowe lub integralność informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-07(05)-Test** | [WYBÓR SPOŚRÓD: Narzędzia do weryfikacji oprogramowania, oprogramowania układowego i integralności informacji; mechanizmy zapewniające automatyczną reakcję na naruszenia integralności; mechanizmy wspierające lub wdrażające zabezpieczenia, które mają być stosowane w przypadku wykrycia naruszeń integralności]. |

| | | |
|---|---|---|
| **SI-07(06)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| OCHRONA KRYPTOGRAFICZNA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(06)[01]** | wdrożono mechanizmy kryptograficzne w celu wykrycia nieautoryzowanych zmian w oprogramowaniu; |
| | **SI-07(06)[02]** | wdrożono mechanizmy kryptograficzne w celu wykrycia nieautoryzowanych zmian w oprogramowaniu układowym; |
| | **SI-07(06)[03]** | wdrożono mechanizmy kryptograficzne w celu wykrycia nieautoryzowanych zmian w informacjach; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące oprogramowania, oprogramowania układowego i integralności informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>mechanizmy kryptograficzne i związana z nimi dokumentacja; zapisy wykrytych nieautoryzowanych zmian w oprogramowaniu, oprogramowaniu sprzętowym i informacjach; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-07(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oprogramowanie, oprogramowanie układowe lub integralność informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |

| | | |
|---|---|---|
| **SI-07(06)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| OCHRONA KRYPTOGRAFICZNA** | |
| | **SI-07(06)-Test** | [WYBÓR SPOŚRÓD: Narzędzia weryfikacji oprogramowania, oprogramowania układowego i integralności informacji; mechanizmy kryptograficzne wdrażające integralność oprogramowania, oprogramowania układowego i informacji]. |

| | | |
|---|---|---|
| **SI-07(07)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| INTEGRACJA WYKRYWANIA I ODPOWIEDZI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(07)_ODP** | ***określono zmiany w systemie dotyczące bezpieczeństwa;*** |
| | **SI-07(07)** | wykrywanie ***<zmian SI-07(07)_ODP>*** stanowi element zdolności organizacji do reagowania na incydenty. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące oprogramowania, oprogramowania układowego i integralności informacji; procedury dotyczące reagowania na incydenty; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące reagowania na incydenty; zapisy z audytów; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-07(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za integralność oprogramowania, oprogramowania układowego i informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za reagowanie na incydenty]. |

| | | |
|---|---|---|
| **SI-07(07)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| INTEGRACJA WYKRYWANIA I ODPOWIEDZI** | |
| | **SI-07(07)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne mające na celu włączenie wykrywania nieuprawnionych zmian dotyczących bezpieczeństwa do organizacyjnych zdolności reagowania na incydenty; narzędzia weryfikacji oprogramowania, oprogramowania układowego i integralności informacji; mechanizmy wspierające lub wdrażające włączenie wykrywania nieuprawnionych zmian dotyczących bezpieczeństwa do organizacyjnych zdolności reagowania na incydenty]. |

| | | |
|---|---|---|
| **SI-07(08)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| ZDOLNOŚĆ AUDYTU ISTOTNYCH ZDARZEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(08)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {wygenerowanie zapisu z audytu; ostrzeżenie aktualnego użytkownika; ostrzeżenie <personelu lub ról SI-07(08)_ODP[02]>;***<br>***<inne działania SI-07(08)_ODP[03]>};*** |
| | **SI-07(08)_ODP[02]** | ***określono personel lub role, które mają być ostrzegane po wykryciu potencjalnego naruszenia integralności (jeśli wybrano);*** |
| | **SI-07(08)_ODP[03]** | ***określono inne działania, które należy podjąć po wykryciu potencjalnego naruszenia integralności (jeśli wybrano);*** |
| | **SI-07(08)[01]** | zapewniona jest możliwość audytu zdarzenia po wykryciu potencjalnego naruszenia integralności; |
| | **SI-07(08)[02]** | po wykryciu potencjalnego naruszenia integralności inicjuje się ***<WYBRANA WARTOŚĆ PARAMETRU SI-07(08)_ODP[01]>***. |

| | | |
|---|---|---|
| **SI-07(08)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| ZDOLNOŚĆ AUDYTU ISTOTNYCH ZDARZEŃ** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące oprogramowania, oprogramowania układowego i integralności informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>narzędzia do weryfikacji integralności i związana z nimi dokumentacja; zapisy dotyczące skanowania integralności; zapisy dotyczące reagowania na incydenty; wykaz zmian w systemie dotyczących bezpieczeństwa; automatyczne narzędzia wspierające alarmy i powiadomienia w przypadku wykrycia nieautoryzowanych zmian dotyczących bezpieczeństwa; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-07(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oprogramowanie, oprogramowanie układowe lub integralność informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-07(08)-Test** | [WYBÓR SPOŚRÓD: Narzędzia do weryfikacji oprogramowania, oprogramowania układowego i integralności informacji; mechanizmy wspierające lub wdrażające zdolność do audytu potencjalnych naruszeń integralności; mechanizmy wspierające lub wdrażające alarmowanie o potencjalnych naruszeniach integralności]. |

| | | |
|---|---|---|
| **SI-07(09)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| WERYFIKACJA PROCESU URUCHAMIANIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(09)_ODP** | ***określono komponenty systemu wymagające weryfikacji integralności procesu uruchamiania;*** |
| | **SI-07(09)** | integralność procesu uruchamiania ***<komponentów systemu SI-07(09)_ODP>*** jest weryfikowana. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(09)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące oprogramowania, oprogramowania układowego i integralności informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>narzędzia do weryfikacji integralności i związana z nimi dokumentacja; dokumentacja; zapisy dotyczące skanowania weryfikacji integralności; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-07(09)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oprogramowanie, oprogramowanie układowe lub integralność informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; programista systemu]. |
| | **SI-07(09)-Test** | [WYBÓR SPOŚRÓD: Narzędzia do weryfikacji integralności oprogramowania, oprogramowania układowego i informacji; mechanizmy wspierające lub wdrażające weryfikację integralności procesu uruchamiania]. |

| | | |
|---|---|---|
| **SI-07(10)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| OCHRONA URUCHAMIANIA OPROGRAMOWANIA UKŁADOWEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(10)_ODP[01]** | ***określono mechanizmy, które należy wdrażać w celu ochrony integralności oprogramowania rozruchowego w komponentach systemu;*** |
| | **SI-07(10)_ODP[02]** | ***określono komponenty systemu wymagające mechanizmów ochrony oprogramowania rozruchowego;*** |
| | **SI-07(10)** | wdrożono ***<mechanizmy SI-07(10)_ODP[01]> w*** celu ochrony integralności oprogramowania rozruchowego w ***<komponentach systemu SI-07(10)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(10)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące oprogramowania, oprogramowania układowego i integralności informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>narzędzia do weryfikacji integralności i związana z nimi dokumentacja; zapisy dotyczące skanowania w celu weryfikacji integralności; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-07(10)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oprogramowanie, oprogramowanie układowe lub integralność informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |

| | | |
|---|---|---|
| **SI-07(10)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| OCHRONA URUCHAMIANIA OPROGRAMOWANIA UKŁADOWEGO** | |
| | **SI-07(10)-Test** | [WYBÓR SPOŚRÓD: Narzędzia do weryfikacji integralności oprogramowania, oprogramowania układowego i informacji; mechanizmy wspierające lub wdrażające ochronę integralności oprogramowania rozruchowego; zabezpieczenia wdrażające ochronę integralności oprogramowania rozruchowego]. |

| | |
|---|---|
| **SI-07(11)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| ZAMKNIĘTE ŚRODOWISKO Z OGRANICZONYMI UPRAWNIENIAMI** |
| | [WYCOFANE: Włączone do CM-07(06)]. |

| | | |
|---|---|---|
| **SI-07(12)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| WERYFIKACJA INTEGRALNOŚCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(12)_ODP** | ***określono oprogramowanie instalowane przez użytkownika, wymagające weryfikacji integralności przed wykonaniem;*** |
| | **SI-07(12)** | integralność ***<oprogramowania instalowanego przez użytkownika SI-07(12)_ODP>*** jest weryfikowana przed wykonaniem. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-07(12)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| WERYFIKACJA INTEGRALNOŚCI** | |
| | **SI-07(12)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące integralności oprogramowania, oprogramowania układowego i informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy dotyczące weryfikacji integralności; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-07(12)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za integralność oprogramowania, oprogramowania układowego i informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SI-07(12)-Test** | [WYBÓR SPOŚRÓD: Narzędzia do weryfikacji integralności oprogramowania, oprogramowania układowego i informacji; mechanizmy wspierające lub wdrażające weryfikację integralności oprogramowania instalowanego przez użytkownika przed wykonaniem]. |

| | |
|---|---|
| **SI-07(13)** | **OPROGRAMOWANIE, FIRMWARE I INTEGRALNOŚĆ INFORMACJI \| WYKONANIE KODU W ŚRODOWISKACH CHRONIONYCH** |
| | [WYCOFANE: Włączone do CM-07(07)]. |

| | |
|---|---|
| **SI-07(14)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| KOD WYKONYWALNY BINARNY LUB MASZYNOWY** |
| | [WYCOFANE: Włączone do CM-07(08)]. |

| | | |
|---|---|---|
| **SI-07(15)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| AUTORYZACJA KODU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(15)_ODP** | ***określono komponenty oprogramowania lub oprogramowania układowego, które mają być uwierzytelniane za pomocą mechanizmów kryptograficznych przed instalacją;*** |
| | **SI-07(15)** | wdrożono mechanizmy kryptograficzne w celu uwierzytelnienia ***<komponentów oprogramowania lub oprogramowania układowego SI-07(15)_ODP>*** przed instalacją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(15)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące oprogramowania, oprogramowania układowego i integralności informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>mechanizmy kryptograficzne i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-07(15)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oprogramowanie, oprogramowanie układowe lub integralność informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-07(15)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy kryptograficzne uwierzytelniające oprogramowanie i oprogramowanie układowe przed instalacją]. |

| | | |
|---|---|---|
| **SI-07(16)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(16)_ODP** | ***określono maksymalny czas wykonywania procesów bez nadzoru;*** |
| | **SI-07(16)** | wykonywanie procesów bez nadzoru przez okres dłuższy niż ***<okres SI-07(16)_ODP>*** jest uniemożliwione; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(16)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące integralności oprogramowania i informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-07(16)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oprogramowanie, oprogramowanie układowe lub integralność informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-07(16)-Test** | [WYBÓR SPOŚRÓD: Narzędzia do weryfikacji integralności oprogramowania, oprogramowania układowego i informacji; mechanizmy wspierające lub wdrażające ograniczenia czasowe dla wykonywania procesów bez nadzoru]. |

| | | |
|---|---|---|
| **SI-07(17)** | **APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI \| SAMOOCHRONA APLIKACJI ŚRODOWISKA WYKONAWCZEGO** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-07(17)_ODP** | ***określono zabezpieczenia, które należy wdrożyć w celu zapewnienia samoochrony dla aplikacji w środowisku wykonawczym;*** |
| | **SI-07(17)** | stosuje się ***<zabezpieczenia SI-07(17)_ODP>*** w celu zapewnienia samoochrony dla aplikacji w środowisku wykonawczym. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-07(17)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące oprogramowania i informacji;<br>dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz znanych słabych punktów zabezpieczanych przy użyciu instrumentów środowiska wykonawczego; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-07(17)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za oprogramowanie, oprogramowanie układowe lub integralność informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-07(17)-Test** | [WYBÓR SPOŚRÓD: Narzędzia weryfikacji integralności oprogramowania, oprogramowania układowego i informacji; mechanizmy wspierające lub wdrażające samoochronę aplikacji w środowisku wykonawczym]. |

| | | |
|---|---|---|
| **SI-08** | **OCHRONA PRZED SPAMEM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-08a.[01]** | w punktach wejścia do systemu stosuje się mechanizmy ochrony przed spamem, które wykrywają niechciane wiadomości; |
| | **SI-08a.[02]** | w punktach wyjścia z systemu stosuje się mechanizmy ochrony przed spamem, które wykrywają niechciane wiadomości; |
| | **SI-08a.[03]** | w punktach wejścia do systemu stosuje się mechanizmy ochrony przed spamem, które reagują na niechciane wiadomości; |
| | **SI-08a.[04]** | w punktach wyjścia z systemu stosuje się mechanizmy ochrony przed spamem, które reagują na niechciane wiadomości; |
| | **SI-08b.** | mechanizmy ochrony przed spamem są aktualizowane w momencie udostępnienia ich nowych wersji zgodnie z organizacyjnymi zasadami i procedurami zarządzania konfiguracją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka i procedury zarządzania konfiguracją (CM-01); procedury dotyczące ochrony przed spamem; mechanizmy ochrony przed spamem;<br>zapisy dotyczące aktualizacji ochrony przed spamem; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę przed spamem; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |

| | | |
|---|---|---|
| **SI-08** | **OCHRONA PRZED SPAMEM** | |
| | **SI-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wdrażania ochrony przed spamem; mechanizmy wspierające lub wdrażające ochronę przed spamem]. |

| | |
|---|---|
| **SI-08(01)** | **OCHRONA PRZED SPAMEM \| ZARZĄDZANIE CENTRALNE** |
| | [WYCOFANE: Włączone do PL-09]. |

| | | |
|---|---|---|
| **SI-08(02)** | **OCHRONA PRZED SPAMEM \| AUTOMATYCZNE AKTUALIZACJE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-08(02)_ODP** | ***określono częstotliwość automatycznej aktualizacji mechanizmów ochrony przed spamem;*** |
| | **SI-08(02)** | mechanizmy ochrony przed spamem są automatycznie aktualizowane z ***<częstotliwością SI-08(02)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-08(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące ochrony przed spamem; mechanizmy ochrony przed spamem; zapisy dotyczące aktualizacji ochrony przed spamem; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-08(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę przed spamem; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |

| | | |
|---|---|---|
| **SI-08(02)** | **OCHRONA PRZED SPAMEM \| AUTOMATYCZNE AKTUALIZACJE** | |
| | **SI-08(02)-Test** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę przed spamem; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |

| | | |
|---|---|---|
| **SI-08(03)** | **OCHRONA PRZED SPAMEM \| ZDOLNOŚĆ DO CIĄGŁEGO UCZENIA SIĘ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-08(03)** | w celu skuteczniejszej identyfikacji legalnego ruchu telekomunikacyjnego stosuje się mechanizmy ochrony przed spamem zdolne do uczenia się. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-08(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące ochrony przed spamem; mechanizmy ochrony przed spamem; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-08(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę przed spamem; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-08(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ochrony przed spamem; mechanizmy wspierające lub wdrażające mechanizmy ochrony przed spamem ze zdolnością do uczenia się]. |

| | |
|---|---|
| **SI-09** | **OGRANICZENIA WPROWADZANIA INFORMACJI** |
| | [WYCOFANE: Włączone do AC-02, AC-03, AC-05, AC-06]. |

| | | |
|---|---|---|
| **SI-10** | **WERYFIKACJA WPROWADZANYCH INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-10_ODP** | ***określono dane wejściowe wprowadzane do systemu, które wymagają weryfikacji;*** |
| | **SI-10** | ***<dane wejściowe SI-10_ODP>*** są weryfikowane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka i procedury kontroli dostępu; polityka i procedury rozdziału obowiązków; procedury dotyczące weryfikacji danych wejściowych; dokumentacja dotycząca automatycznych narzędzi i aplikacji do weryfikacji informacji; wykaz danych wejściowych wymagających weryfikacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-10-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację danych wejściowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-10-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wspierające lub wdrażające weryfikację danych wejściowych]. |

| | | |
|---|---|---|
| **SI-10(01)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| RĘCZNE ZASTĘPOWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-10(01)_ODP** | ***określono osoby upoważnione, które mogą korzystać z funkcji ręcznego zastępowania;*** |
| | **SI-10(01)(a)** | zapewniono możliwość ręcznego zastępowania w zakresie ***<danych wejściowych SI-10_ODP>.*** |
| | **SI-10(01)(b)** | z możliwości ręcznego zastępowania korzystać mogą wyłącznie ***<osoby upoważnione SI-10(01)_ODP>***; |
| | **SI-10(01)(c)** | wykorzystanie możliwości ręcznego zastępowania podlega kontroli. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-10(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka i procedury kontroli dostępu; polityka i procedury rozdziału obowiązków; procedury dotyczące weryfikacji danych wejściowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-10(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację danych wejściowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |

| | | |
|---|---|---|
| **SI-10(01)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| RĘCZNE ZASTĘPOWANIE** | |
| | **SI-10(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące korzystania z możliwości ręcznego zastępowania; mechanizmy wspierające lub wdrażające możliwość ręcznego zastępowania w zakresie weryfikacji danych wejściowych; mechanizmy wspierające lub wdrażające kontrolę korzystania z możliwości ręcznego zastępowania]. |

| | | |
|---|---|---|
| **SI-10(02)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| PRZEGLĄD/USUWANIE BŁĘDÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-10(02)_ODP[01]** | ***określono okres, w którym należy dokonać przeglądu błędów w zakresie weryfikacji danych wejściowych;*** |
| | **SI-10(02)_ODP[02]** | ***określono okres na usunięcie błędów w zakresie weryfikacji danych wejściowych;*** |
| | **SI-10(02)[01]** | błędy w zakresie weryfikacji danych wejściowych są analizowane w ciągu ***<okresu SI-10(02)_ODP[01]>***; |
| | **SI-10(02)[02]** | błędy w zakresie weryfikacji danych wejściowych są rozwiązywane w ciągu ***<okresu SI-10(02)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-10(02)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| PRZEGLĄD/USUWANIE BŁĘDÓW** | |
| | **SI-10(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące weryfikacji danych wejściowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja;<br>zapisy z przeglądów błędów weryfikacji danych wejściowych i zastosowanych rozwiązań; dzienniki lub zapisy dotyczące błędów w weryfikacji danych wejściowych; zapisy z audytów systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-10(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację danych wejściowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **SI-10(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przeglądów i rozwiązywania błędów w zakresie weryfikacji danych wejściowych; mechanizmy wspierające lub wdrażające przeglądy i rozwiązywanie błędów w zakresie weryfikacji danych wejściowych]. |

| | | |
|---|---|---|
| **SI-10(03)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| PRZEWIDYWALNE ZACHOWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-10(03)[01]** | zachowanie systemu w przypadku otrzymania nieprawidłowych danych wejściowych jest przewidywalne; |

| | | |
|---|---|---|
| **SI-10(03)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| PRZEWIDYWALNE ZACHOWANIE** | |
| | **SI-10(03)[02]** | zachowanie systemu w przypadku otrzymania nieprawidłowych danych wejściowych jest udokumentowane; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-10(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące weryfikacji danych wejściowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-10(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację danych wejściowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-10(03)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspierające lub wdrażające przewidywalne zachowanie w przypadku otrzymania nieprawidłowych danych wejściowych]. |

| | | |
|---|---|---|
| **SI-10(04)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| INTERAKCJE CZASOWE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-10(04)** | przy określaniu odpowiednich reakcji na nieprawidłowe dane wejściowe uwzględniane są interakcje czasowe pomiędzy komponentami systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-10(04)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| INTERAKCJE CZASOWE** | |
| | **SI-10(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące weryfikacji danych wejściowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-10(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację danych wejściowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-10(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne służące do określania odpowiednich reakcji na nieprawidłowe dane wejściowe; automatyczne mechanizmy wspierające lub wdrażające reakcje na nieprawidłowe dane wejściowe]. |

| | | |
|---|---|---|
| **SI-10(05)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| OGRANICZANIE DANYCH WEJŚCIOWYCH DO ZAUFANYCH ŹRÓDEŁ I ZATWIERDZONYCH FORMATÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-10(05)_ODP[01]** | ***określono zaufane źródła, z których muszą pochodzić wykorzystywane dane wejściowe;*** |
| | **SI-10(05)_ODP[02]** | ***określono formaty, w których muszą być zapisane wykorzystywane dane wejściowe;*** |
| | **SI-10(05)** | Stosuje się wyłącznie dane wejściowe pochodzące z ***<zaufanych źródeł SI-10(05)_ODP[01]>***<br>i zapisane w ***<formatach SI-10(05)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-10(05)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| OGRANICZANIE DANYCH WEJŚCIOWYCH DO ZAUFANYCH ŹRÓDEŁ I ZATWIERDZONYCH FORMATÓW** | |
| | **SI-10(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące weryfikacji danych wejściowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz zaufanych źródeł danych wejściowych; wykaz dopuszczalnych formatów danych wejściowych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-10(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację danych wejściowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-10(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące ograniczeń w stosowaniu danych wejściowych; automatyczne mechanizmy wspierające lub wdrażające ograniczania w stosowaniu danych wejściowych]. |

| | | |
|---|---|---|
| **SI-10(06)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| ZAPOBIEGANIE WSTRZYKIWANIU NIEZAUFANYCH DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-10(06)** | wstrzykiwanie niezaufanych danych jest uniemożliwione. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-10(06)** | **WERYFIKACJA WPROWADZANYCH INFORMACJI \| ZAPOBIEGANIE WSTRZYKIWANIU NIEZAUFANYCH DANYCH** | |
| | **SI-10(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące weryfikacji danych wejściowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz zaufanych źródeł danych wejściowych; wykaz dopuszczalnych formatów danych wejściowych; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-10(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację danych wejściowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-10(06)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zapobiegające wstrzykiwaniu niezaufanych danych; automatyczne mechanizmy wspierające lub wdrażające zapobieganie wstrzykiwaniu niezaufanych danych]. |

| | | |
|---|---|---|
| **SI-11** | **OBSŁUGA BŁĘDÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-11_ODP** | ***określono personel lub role, którym mają być ujawniane komunikaty o błędach;*** |

| | | |
|---|---|---|
| **SI-11** | **OBSŁUGA BŁĘDÓW** | |
| | **SI-11a.** | komunikaty o błędach, które dostarczają informacji niezbędnych do podjęcia działań naprawczych, są generowane bez ujawniania informacji, które mogłyby zostać wykorzystane w niewłaściwych celach; |
| | **SI-11b.** | komunikaty o błędach są ujawniane tylko ***<personelowi lub rolom SI-11_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-11-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące obsługi błędów systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja określająca strukturę i treść komunikatów o błędach; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-11-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za weryfikację danych wejściowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-11-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące obsługi błędów; automatyczne mechanizmy wspierające lub wdrażające obsługę błędów; automatyczne mechanizmy wspierające lub wdrażające obsługę komunikatów o błędach]. |

| | | |
|---|---|---|
| **SI-12** | **ZARZĄDZANIE I RETENCJA DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-12[01]** | zarządzanie danymi w systemie odbywa się zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, regulacjami, politykami, normami, wytycznymi i wymogami operacyjnymi; |
| | **SI-12[02]** | przechowywanie danych w systemie odbywa się zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, regulacjami, politykami, normami, wytycznymi i wymogami operacyjnymi; |
| | **SI-12[03]** | zarządzanie danymi wyjściowymi w systemie odbywa się zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, regulacjami, politykami, normami, wytycznymi i wymogami operacyjnymi; |
| | **SI-12[04]** | przechowywanie danych wyjściowych w systemie odbywa się zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, regulacjami, politykami, normami, wytycznymi i wymogami operacyjnymi. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-12** | **ZARZĄDZANIE I RETENCJA DANYCH** | |
| | **SI-12-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; polityka przechowywania i dysponowania dokumentacją; procedury przechowywania i dysponowania dokumentacją; krajowe przepisy prawne, rozporządzenia, dyrektywy, polityki, regulacje, standardy<br>i wymogi operacyjne mające zastosowanie do zarządzania informacjami i ich przechowywania; polityka ochrony mediów; procedury ochrony mediów; wyniki audytu; plan bezpieczeństwa systemu; plan ochrony prywatności; plan programu ochrony prywatności; wykaz danych identyfikacyjnych; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-12-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie, przechowywanie i usuwanie informacji i zapisów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy sieci]. |
| | **SI-12-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zarządzania, przechowywania i dysponowania informacjami; automatyczne mechanizmy wspierające lub wdrażające zarządzanie, przechowywanie i dysponowanie informacjami]. |

| | | |
|---|---|---|
| **SI-12(01)** | **ZARZĄDZANIE I RETENCJA DANYCH \|OGRANICZANIE ELEMENTÓW DANYCH OSOBOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-12(01)_ODP** | ***określono elementy danych identyfikacyjnych, które są przetwarzane w cyklu życia informacji;*** |

| | | |
|---|---|---|
| **SI-12(01)** | **ZARZĄDZANIE I RETENCJA DANYCH \|OGRANICZANIE ELEMENTÓW DANYCH OSOBOWYCH** | |
| | **SI-12(01)** | dane identyfikacyjne przetwarzane w cyklu życia informacji są ograniczone do ***<elementów danych identyfikacyjnych SI-12(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-12(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury przetwarzania danych identyfikacyjnych; polityka przechowywania i usuwania dokumentacji; procedury przechowywania i usuwania dokumentacji; krajowe przepisy, rozporządzenia, dyrektywy, polityki, regulacje, standardy i wymogi operacyjne dotyczące ograniczeń w zakresie wykorzystania danych identyfikacyjnych; wykaz danych identyfikacyjnych; zapisy z audytu systemu; wyniki audytu; plan bezpieczeństwa systemu; plan ochrony prywatności; plan programu ochrony prywatności; wpływ na prywatność ocena wpływu na prywatność;<br>dokumentacja oceny ryzyka dla prywatności; dokumentacja mapowania danych; inne istotne dokumenty lub zapisy]. |
| | **SI-12(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie, przechowywanie i usuwanie informacji i zapisów; personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność; administratorzy sieci]. |
| | **SI-12(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zarządzania informacjami i ich przechowywania (w tym ograniczenia w przetwarzaniu danych identyfikacyjnych); automatyczne mechanizmy wspierające lub wdrażające ograniczenia w przetwarzaniu danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **SI-12(02)** | **ZARZĄDZANIE I RETENCJA DANYCH \| MINIMALIZOWANIE WYKORZYSTYWANIA DANYCH OSOBOWYCH PODCZAS TESTÓW, SZKOLEŃ I BADAŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-12(02)_ODP[01]** | ***określono techniki stosowane w celu minimalizacji wykorzystania danych identyfikacyjnych do celów badań;*** |
| | **SI-12(02)_ODP[02]** | ***określono techniki stosowane w celu minimalizacji wykorzystania danych identyfikacyjnych do celów testów;*** |
| | **SI-12(02)_ODP[03]** | ***określono techniki stosowane w celu minimalizacji wykorzystania danych identyfikacyjnych do celów szkoleniowych;*** |
| | **SI-12(02)[01]** | w celu zminimalizowania wykorzystania danych identyfikacyjnych do celów badań stosuje się ***<techniki SI-12(02)_ODP[01]>***; |
| | **SI-12(02)[02]** | w celu zminimalizowania wykorzystania danych identyfikacyjnych do celów testów stosuje się ***<techniki SI-12(02)_ODP[02]>***; |
| | **SI-12(02)[03]** | w celu zminimalizowania wykorzystania danych identyfikacyjnych do celów szkoleniowych stosuje się ***<techniki SI-12(02)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-12(02)** | **ZARZĄDZANIE I RETENCJA DANYCH \| MINIMALIZOWANIE WYKORZYSTYWANIA DANYCH OSOBOWYCH PODCZAS TESTÓW, SZKOLEŃ I BADAŃ** | |
| | **SI-12(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury przetwarzania danych identyfikacyjnych; krajowe przepisy, rozporządzenia, dyrektywy, polityki, regulacje, standardy i wymogi operacyjne mające zastosowanie do minimalizacji wykorzystania danych identyfikacyjnych w testach, szkoleniach i badaniach; polityka minimalizacji wykorzystania danych identyfikacyjnych w testach, szkoleniach i badaniach; procedury minimalizacji wykorzystania danych identyfikacyjnych w testach, szkoleniach i badaniach; dokumentacja wspierająca wdrażanie polityki minimalizacji wykorzystania danych identyfikacyjnych (np. wzorce w zakresie ich wykorzystania do testowania, szkolenia i badań);<br><br>zbiory danych wykorzystywane do testowania, szkolenia i badań; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-12(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie, przechowywanie i usuwanie informacji i zapisów; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy sieci; programiści systemów; personel odpowiedzialny za stosowanie metody IRB]. |
| | **SI-12(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące minimalizacji wykorzystania danych identyfikacyjnych w testach, szkoleniach i badaniach; automatyczne mechanizmy wspierające lub wdrażające minimalizację wykorzystania danych identyfikacyjnych w testach, szkoleniach i badaniach]. |

| | | |
|---|---|---|
| **SI-12(03)** | **ZARZĄDZANIE I RETENCJA DANYCH \| USUWANIE INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-12(03)_ODP[01]** | ***określono techniki stosowane do usuwania sunięcia informacji po upływie okresu przechowywania;*** |
| | **SI-12(03)_ODP[02]** | ***określono techniki stosowane do niszczenia informacji po upływie okresu przechowywania;*** |
| | **SI-12(03)_ODP[03]** | ***określono techniki stosowane do kasowania informacji po upływie okresu przechowywania;*** |
| | **SI-12(03)[01]** | do usuwania informacji po upływie okresu przechowywania stosuje się ***<techniki SI-12(03)_ODP[01]>***; |
| | **SI-12(03)[02]** | do niszczenia informacji po upływie okresu przechowywania stosuje się ***<techniki SI-12(03)_ODP[02]>***; |
| | **SI-12(03)[03]** | do kasowania informacji po upływie okresu przechowywania stosuje się ***<techniki SI-12(03)_ODP[03]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-12(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury przetwarzania danych identyfikacyjnych; polityka przechowywania i dysponowania dokumentacją; procedury przechowywania i dysponowania dokumentacją; krajowe przepisy, rozporządzenia, dyrektywy, polityki, regulacje, standardy i wymogi operacyjne dotyczące usuwania informacji; polityka ochrony mediów; procedury ochrony mediów; zapisy z audytu systemu; wyniki audytu; zapisy dotyczące usuwania informacji; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-12(03)** | **ZARZĄDZANIE I RETENCJA DANYCH \| USUWANIE INFORMACJI** | |
| | **SI-12(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie i przechowywanie informacji i zapisów oraz ich usuwanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; administratorzy sieci]. |
| | **SI-12(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące dysponowania informacjami; automatyczne mechanizmy wspierające lub wdrażające dysponowanie informacjami]. |

| | | |
|---|---|---|
| **SI-13** | **PRZEWIDYWANIE AWARII** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-13_ODP[01]** | ***określono komponenty systemu, dla których należy zidentyfikować średni czas do wystąpienia awarii (MTTF);*** |
| | **SI-13_ODP[02]** | ***określono kryteria zastępowania komponentów po upływie średniego czasu do awarii (MTTF), które mają być stosowane do celów wymiany komponentów aktywnych i zastępczych;*** |
| | **SI-13a.** | określa się średni czas do awarii (MTTF) ***<komponentów systemu SI-13_ODP[01]>*** w określonych środowiskach pracy; |
| | **SI-13b.** | zapewnione są zastępcze komponenty systemu oraz sposób wymiany komponentów aktywnych i zastępczych zgodnie z ***<kryteriami wymiany komponentów po upływie średniego czasu do awarii (MTTF) SI-13_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-13** | **PRZEWIDYWANIE AWARII** | |
| | **SI-13-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące przewidywania awarii; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz kryteriów zastępowania komponentów po okresie MTTF; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-13-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za określenie kryteriów i działania w zakresie MTTF; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za planowanie awaryjne]. |
| | **SI-13-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie MTTF]. |

| | | |
|---|---|---|
| **SI-13(01)** | **PRZEWIDYWANIE AWARII \| PRZENIESIENIE ODPOWIEDZIALNOŚCI KOMPONENTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-13(01)_ODP** | ***określono wartość ułamkową lub procent średniego czasu do awarii, w którym można przenieść odpowiedzialność za realizację funkcji na zastępczy komponent systemu;*** |
| | **SI-13(01)** | komponenty systemu są wycofywane z eksploatacji poprzez przeniesienie odpowiedzialności za realizowane funkcje na komponenty zastępcze nie później niż po upływie***<wartość ułamkowa lub procentowa SI-13(01)_ODP>*** średniego czasu do awarii. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-13(01)** | **PRZEWIDYWANIE AWARII \| PRZENIESIENIE ODPOWIEDZIALNOŚCI KOMPONENTÓW** | |
| | **SI-13(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące przewidywania awarii; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-13(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za działania w zakresie MTTF; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za planowanie awaryjne]. |
| | **SI-13(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie MTTF; automatyczne mechanizmy wspierające lub wdrażające przenoszenie odpowiedzialności za realizowane funkcje na komponenty zastępcze]. |

| | | |
|---|---|---|
| **SI-13(02)** | **PRZEWIDYWANIE AWARII \| LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU** | |
| | [WYCOFANE: Włączone do SI-07(16)]. | |

| | | |
|---|---|---|
| **SI-13(03)** | **PRZEWIDYWANIE AWARII \| RĘCZNY TRANSFER MIĘDZY KOMPONENTAMI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-13(03)_ODP** | ***określono procent średniego czasu do awarii, przed którego upływem możliwe jest dokonanie ręcznego przeniesienia odpowiedzialności na komponent zastępczy;*** |

| | | |
|---|---|---|
| **SI-13(03)** | **PRZEWIDYWANIE AWARII \| RĘCZNY TRANSFER MIĘDZY KOMPONENTAMI** | |
| | **SI-13(03)** | przeniesienie odpowiedzialności z komponentu aktywnego na zastępczy jest inicjowane ręcznie po eksploatacji aktywnego komponentu przez ***<wartość procentowa SI-13(03)_ODP>*** średniego czasu do awarii. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-13(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące przewidywania awarii; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-13(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za działania w zakresie MTTF; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za planowanie awaryjne]. |
| | **SI-13(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie MTTF i ręcznego przeniesienia odpowiedzialności za realizowane funkcje z komponentu aktywnego na zastępczy]. |

| | | |
|---|---|---|
| **SI-13(04)** | **PRZEWIDYWANIE AWARII \| INSTALACJA KOMPONENTÓW Z LISTY REZERWOWEJ/POWIADOMIENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-13(04)_ODP[01]** | ***określono okres, w którym należy zainstalować dostępne komponenty zastępcze;*** |

| | | |
|---|---|---|
| **SI-13(04)** | **PRZEWIDYWANIE AWARII \| INSTALACJA KOMPONENTÓW Z LISTY REZERWOWEJ/POWIADOMIENIE** | |
| | **SI-13(04)_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW:***<br>***{aktywacja <alarmu SI-13(04)_ODP[03]>; automatyczne wyłączenie systemu;***<br>***<działanie SI-13(04)_ODP[04]>};*** |
| | **SI-13(04)_ODP[03]** | ***określono alarm uruchamiany w przypadku wykrycia awarii komponentów systemu (jeśli wybrano);*** |
| | **SI-13(04)_ODP[04]** | ***określono działania podejmowane przypadku wykrycia awarii komponentów systemu (jeśli wybrano);*** |
| | **SI-13(04)(a)** | w przypadku wykrycia awarii komponentów systemu komponenty zastępcze są instalowane pomyślnie i w sposób przejrzysty w ciągu ***<okresu SI-13(04)_ODP[01]>;*** |
| | **SI-13(04)(b)** | w przypadku wykrycia awarii komponentów systemu wykonywane są działania ***<WYBRANA WARTOŚĆ PARAMETRU SI-13(04)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-13(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące przewidywania awarii; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz działań podejmowanych po wykryciu awarii komponentu systemu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-13(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za działania w zakresie MTTF; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za planowanie awaryjne]. |

| | | |
|---|---|---|
| **SI-13(04)** | **PRZEWIDYWANIE AWARII \| INSTALACJA KOMPONENTÓW Z LISTY REZERWOWEJ/POWIADOMIENIE** | |
| | **SI-13(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne w zakresie MTTF; automatyczne mechanizmy wspierające lub wdrażające instalację komponentów zastępczych w przejrzysty sposób; automatyczne mechanizmy wspierające lub wdrażające alarmy bądź wyłączanie systemu w przypadku wykrycia awarii komponentów]. |

| | | |
|---|---|---|
| **SI-13(05)** | **PRZEWIDYWANIE AWARII \| PRZEŁĄCZANIE AWARYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-13(05)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {w czasie rzeczywistym; w czasie zbliżonym do rzeczywistego};*** |
| | **SI-13(05)_ODP[02]** | ***określono zdolność systemu do przełączania się w tryb awaryjny w razie wystąpienia awarii;*** |
| | **SI-13(05)** | dla systemu zapewniona jest zdolność ***<WYBRANA WARTOŚĆ PARAMETRU SI-13(05)_ODP[01]> <przełączania się w tryb awaryjny SI-13(05)_ODP[02]>*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-13(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące przewidywania awarii; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; dokumentacja opisująca zdolność systemu do przełączania się w tryb awaryjny; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-13(05)** | **PRZEWIDYWANIE AWARII \| PRZEŁĄCZANIE AWARYJNE** | |
| | **SI-13(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zdolność do pracy w trybie awaryjnym; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacyjny odpowiedzialny za planowanie awaryjne]. |
| | **SI-13(05)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zarządzania zdolnością do przełączania się w tryb awaryjny; automatyczne mechanizmy wspierające lub wdrażające zdolność do przełączania się w tryb awaryjny]. |

| | | |
|---|---|---|
| **SI-14** | **ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-14_ODP[01]** | ***określono nietrwałe komponenty systemu i usługi, które mają być wdrożone;*** |
| | **SI-14_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {po zakończeniu sesji użytkowania; <częstotliwość SI-14_ODP[03]>};*** |
| | **SI-14_ODP[03]** | ***określono częstotliwość, z jaką następuje kończenie działania nietrwałych komponentów i usług inicjowanych w bezpiecznym stanie (jeśli wybrano);*** |
| | **SI-14[01]** | wdrożono nietrwałe ***<komponenty i usługi systemowe SI-14_ODP[01]>***, które są inicjowane w bezpiecznym stanie; |
| | **SI-14[02]** | w przypadku nietrwałych ***<komponentów i usług systemowych SI-14_ODP[01]>*** następuje zakończenie działania ***<WYBRANA WARTOŚĆ PARAMETRU SI-14_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-14** | **ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT** | |
| | **SI-14-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące nietrwałości komponentów systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-14-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nietrwałość; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-14-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspierające lub wdrażające inicjowanie i zakończenie działania komponentów nietrwałych]. |

| | | |
|---|---|---|
| **SI-14(01)** | **ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT \| ODŚWIEŻANIE Z ZAUFANYCH ŹRÓDEŁ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-14(01)_ODP** | ***określono zaufane źródła pozyskiwania oprogramowania i danych do celów odświeżania komponentów systemu i usług;*** |
| | **SI-14(01)** | oprogramowanie i dane wykorzystywane podczas odświeżania komponentów systemu i usług są pozyskiwane z ***<zaufanych źródeł SI-14(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-14(01)** | **ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT \| ODŚWIEŻANIE Z ZAUFANYCH ŹRÓDEŁ** | |
| | **SI-14(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące nietrwałości komponentów systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-14(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za pozyskiwanie oprogramowania i danych z zaufanych źródeł do celów odświeżania komponentów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SI-14(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania i pozyskiwania oprogramowania i danych z zaufanych źródeł do celów odświeżania komponentów i usług; automatyczne mechanizmy wspierające lub wdrażające odświeżanie komponentów i usług]. |

| | | |
|---|---|---|
| **SI-14(02)** | **ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT \| NIETRWAŁOŚĆ INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-14(02)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {odświeżanie <informacje SI-14(02)_ODP[02]> <częstotliwość SI-14(02)_ODP[03]>; generowanie <informacji SI-14(02)_ODP[04]> na żądanie};*** |
| | **SI-14(02)_ODP[02]** | ***określono informacje, które mają być odświeżane (jeśli wybrano);*** |
| | **SI-14(02)_ODP[03]** | ***określono częstotliwość odświeżania informacji (jeśli wybrano);*** |

| | | |
|---|---|---|
| **SI-14(02)** | **ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT \| NIETRWAŁOŚĆ INFORMACJI** | |
| | **SI-14(02)_ODP[04]** | ***określono informacje, które mają być generowane (jeśli wybrano);*** |
| | **SI-14(02)(a)** | wykonuje się **<*WYBRANA WARTOŚĆ PARAMETRU SI-14(02)_ODP[01]*>**; |
| | **SI-14(02)(b)** | informacje są usuwane, gdy nie są już potrzebne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-14(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące nietrwałości komponentów systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-14(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zapewnienie bieżącej i przyszłej nietrwałości informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SI-14(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne zapewniające bieżącą i przyszłą nietrwałość informacji; automatyczne mechanizmy wspierające lub wdrażające odświeżanie komponentów i usług]. |

| | | |
|---|---|---|
| **SI-14(03)** | **ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT \| NIETRWAŁOŚĆ POŁĄCZEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-14(03)_ODP** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {wykonanie żądania; okres nieużywania};*** |
| | **SI-14(03)[01]** | połączenia do systemu są nawiązane na żądanie; |

| | | |
|---|---|---|
| **SI-14(03)** | **ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT \| NIETRWAŁOŚĆ POŁĄCZEŃ** | |
| | **SI-14(03)[02]** | połączenia z systemem są przerywane po ***<WYBRANA WARTOŚĆ PARAMETRU SI-14(03)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-14(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące nietrwałości komponentów systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-14(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ograniczanie stosowania trwałych połączeń; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji]. |
| | **SI-14(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne ograniczające nawiązywanie trwałych połączeń; automatyczne mechanizmy wspierające lub wdrażające stosowanie połączeń nietrwałych]. |

| | | |
|---|---|---|
| **SI-15** | **FILTROWANIE INFORMACJI WYJŚCIOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-15_ODP** | ***określono programy lub aplikacje, których dane wyjściowe wymagają zatwierdzenia;*** |
| | **SI-15** | dane wyjściowe ***<oprogramowania lub aplikacji SI-15_ODP>*** są zatwierdzane w celu zagwarantowania ich spójności z oczekiwaną zawartością. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-15** | **FILTROWANIE INFORMACJI WYJŚCIOWYCH** | |
| | **SI-15-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące filtrowania danych wyjściowych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-15-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zatwierdzanie danych wyjściowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-15-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zatwierdzania danych wyjściowych; automatyczne mechanizmy wspierające lub wdrażające zatwierdzanie danych wyjściowych]. |

| | | |
|---|---|---|
| **SI-16** | **OCHRONA PAMIĘCI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-16_ODP** | ***określono zabezpieczenia wdrażane w celu ochrony pamięci systemu przed nieautoryzowanym wykonaniem kodu;*** |
| | **SI-16** | wdrożono ***<zabezpieczenia SI-16_ODP>*** w celu ochrony pamięci systemu przed nieautoryzowanym wykonaniem kodu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-16** | **OCHRONA PAMIĘCI** | |
| | **SI-16-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; procedury dotyczące ochrony pamięci systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista zabezpieczeń chroniących pamięć systemu przed nieautoryzowanym wykonaniem kodu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-16-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za ochronę pamięci; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-16-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspierające lub wdrażające zabezpieczenia chroniące pamięć systemu przed nieautoryzowanym wykonaniem kodu]. |

| | | |
|---|---|---|
| **SI-17** | **PROCEDURY AWARYJNE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-17_ODP[01]** | ***określono procedury awaryjne stosowane w przypadku wystąpienia warunków stanu awaryjnego;*** |
| | **SI-17_ODP[02]** | ***określono wykaz warunków stanu awaryjnego, wymagających procedur awaryjnych;*** |
| | **SI-17** | ***<procedury awaryjne SI-17_ODP[01]>*** są wdrażane w przypadku wystąpienia warunków z ***<listy warunków awaryjnych SI-17_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-17** | **PROCEDURY AWARYJNE** | |
| | **SI-17-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; dokumentacja dotycząca procedur awaryjnych dla systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; lista zabezpieczeń chroniących pamięć systemu przed nieautoryzowanym wykonaniem kodu; zapisy z audytu systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SI-17-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za procedury awaryjne; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; programista systemu]. |
| | **SI-17-Test** | [WYBÓR SPOŚRÓD: Organizacyjne procedury awaryjne; automatyczne mechanizmy wspierające lub wdrażające procedury awaryjne]. |

| | | |
|---|---|---|
| **SI-18** | **OPERACJE SPRADZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-18_ODP[01]** | ***określono częstotliwość sprawdzania dokładności danych identyfikacyjnych w całym cyklu życia informacji;*** |
| | **SI-18_ODP[02]** | ***określono częstotliwość sprawdzania przydatności danych identyfikacyjnych w całym cyklu życia informacji;*** |
| | **SI-18_ODP[03]** | ***określono częstotliwość sprawdzania aktualności danych identyfikacyjnych w całym cyklu życia informacji;*** |
| | **SI-18_ODP[04]** | ***określono częstotliwość sprawdzania kompletności danych identyfikacyjnych w całym cyklu życia informacji;*** |

| | | |
|---|---|---|
| **SI-18** | **OPERACJE SPRADZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH** | |
| | **SI-18a.[01]** | dokładność danych identyfikacyjnych w całym cyklu życia informacji jest sprawdzana z ***<częstotliwością SI-18_ODP[01]>***; |
| | **SI-18a.[02]** | przydatność danych identyfikacyjnych w całym cyklu życia informacji jest sprawdzana z ***<częstotliwością SI-18_ODP[02]>***; |
| | **SI-18a.[03]** | aktualność danych identyfikacyjnych w całym cyklu życia informacji jest sprawdzana z ***<częstotliwością SI-18_ODP[03]>***; |
| | **SI-18a.[04]** | kompletność danych identyfikacyjnych w całym cyklu życia informacji jest sprawdzana z ***<częstotliwością SI-18_ODP[04]>***; |
| | **SI-18b.** | niepoprawne lub nieaktualne dane identyfikacyjne są poprawiane bądź usuwane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-18-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; dokumentacja dotycząca działań w zakresie kontroli jakości danych identyfikacyjnych; sprawozdania dotyczące jakości; dzienniki dotyczące konserwacji; zapisy z audytu systemu; wyniki audytu; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka w zakresie ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-18-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za przeprowadzanie kontroli jakości danych identyfikacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę prywatności]. |

| | | |
|---|---|---|
| **SI-18** | **OPERACJE SPRADZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH** | |
| | **SI-18-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące kontroli jakości danych identyfikacyjnych; automatyczne mechanizmy wspierające lub wdrażające działania w zakresie kontroli jakości danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **SI-18(01)** | **OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH \| AUTOMATYZACJA WSPARCIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-18(01)_ODP** | ***określono automatyczne mechanizmy stosowane do poprawiania lub usuwania danych identyfikacyjnych, które są niedokładne, nieaktualne, nieprawidłowo określone pod względem ich wpływu lub niepoprawnie zanonimizowane;*** |
| | **SI-18(01)** | stosuje się ***<automatyczne mechanizmy SI-18(01)_ODP>*** do poprawiania lub usuwania danych identyfikacyjnych, które są niedokładne, nieaktualne, nieprawidłowo określone pod względem ich wpływu lub niepoprawnie zanonimizowane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-18(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; dokumentacja dotycząca działań w zakresie kontroli jakości danych identyfikacyjnych; sprawozdania dotyczące jakości; dzienniki dotyczące konserwacji; zapisy z audytu systemu; wyniki audytu; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka w zakresie ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-18(01)** | **OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH \| AUTOMATYZACJA WSPARCIA** | |
| | **SI-18(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za kontrolę jakości danych identyfikacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-18(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące kontroli jakości danych identyfikacyjnych; automatyczne mechanizmy wspierające lub wdrażające działania w zakresie kontroli jakości danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **SI-18(02)** | **OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH \| ZNACZNIKI DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-18(02)** | stosuje się znaczniki danych w celu zautomatyzowania poprawiania lub usuwania danych identyfikacyjnych w całym cyklu życia informacji w systemach organizacyjnych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-18(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury dotyczące znakowania danych; wykaz danych identyfikacyjnych; zapisy z audytu systemu; wyniki audytu; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-18(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za znakowanie danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |

| | | |
|---|---|---|
| **SI-18(02)** | **OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH \| ZNACZNIKI DANYCH** | |
| | **SI-18(02)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy znakowania danych; automatyczne mechanizmy wspierające lub wdrażające znakowanie danych]. |

| | | |
|---|---|---|
| **SI-18(03)** | **OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH \|ZBIERANIE DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-18(03)** | dane identyfikacyjne są zbierane bezpośrednio od osoby. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-18(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; dokumentacja konfiguracji systemu; zapisy z audytu systemu; interfejs użytkownika wykorzystywany do gromadzenia danych identyfikacyjnych; plan bezpieczeństwa systemu; plan ochrony prywatności;<br>ocena wpływu na prywatność; dokumentacja oceny ryzyka dla prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-18(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za gromadzenie danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-18(03)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy gromadzenia danych; automatyczne mechanizmy wspierające lub zatwierdzające gromadzenie danych bezpośrednio od osoby fizycznej]. |

| | | |
|---|---|---|
| **SI-18(04)** | **OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH \| ZGŁOSZENIA USUNIĘCIA DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-18(04)** | dane identyfikacyjne są poprawiane lub usuwane na wniosek osób fizycznych lub ich wyznaczonych przedstawicieli. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-18(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; konfiguracja systemu; indywidualne wnioski o usunięcie danych; zapisy przeprowadzonych działań w celu korekty lub usunięcia danych; zapisy z audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-18(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za odpowiadanie na indywidualne wnioski o korektę lub usunięcie danych identyfikacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-18(04)-Test** | [WYBÓR SPOŚRÓD: Mechanizmy wnioskowania; automatyczne mechanizmy wspierające lub wdrażające indywidualne wnioski o korektę lub usunięcie danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **SI-19** | **DE-IDENTYFIKACJA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-19_ODP[01]** | ***określono elementy danych identyfikacyjnych, które mają zostać usunięte ze zbiorów danych;*** |

| | | |
|---|---|---|
| **SI-19** | **DE-IDENTYFIKACJA** | |
| | **SI-19_ODP[02]** | ***określono częstotliwość, z jaką należy dokonywać oceny skuteczności anonimizacji danych;*** |
| | **SI-19a.** | ***<elementy SI-19_ODP[01]>*** są usuwane ze zbiorów danych; |
| | **SI-19b.** | skuteczność anonimizacji oceniana jest z ***<częstotliwością SI-19_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-19-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych;<br>procedury anonimizacji; konfiguracja systemu; zanonimizowane zbiory danych; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-19-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za identyfikację zbędnych identyfikatorów; personel organizacyjny odpowiedzialny za usuwanie danych identyfikacyjnych ze zbiorów danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-19-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspierające lub wdrażające usuwanie elementów danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **SI-19(01)** | **DE-IDENTYFIKACJA \| ZBIERANIE DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-19(01)** | zbiór danych jest anonimizowany w momencie tworzenia jego zawartości poprzez unikanie gromadzenia danych identyfikacyjnych. |

| | | |
|---|---|---|
| **SI-19(01)** | **DE-IDENTYFIKACJA \| ZBIERANIE DANYCH** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-19(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury anonimizacji; procedury minimalizacji gromadzenia danych identyfikacyjnych; konfiguracja systemu; mechanizmy gromadzenia danych; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-19(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za anonimizację zbioru danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-19(01)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy zapobiegające gromadzeniu danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **SI-19(02)** | **DE-IDENTYFIKACJA \| ARCHIWIZACJA DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-19(02)** | zabrania się archiwizacji elementów danych identyfikacyjnych w przypadku gdy elementy te nie będą potrzebne po zarchiwizowaniu zbioru danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-19(02)** | **DE-IDENTYFIKACJA \| ARCHIWIZACJA DANYCH** | |
| | **SI-19(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury anonimizacji; dokumentacja konfiguracji systemu; mechanizmy archiwizacji danych; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-19(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za anonimizację zbioru danych; personel organizacyjny odpowiedzialny za archiwizację zbioru danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-19(02)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy zakazujące archiwizacji danych identyfikacyjnych]. |

| | | |
|---|---|---|
| **SI-19(03)** | **DE-IDENTYFIKACJA \| UJAWNIANIE DANYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-19(03)** | elementy danych identyfikacyjnych są usuwane ze zbioru danych przed jego udostępnieniem, jeżeli elementy te nie muszą być częścią udostępnianych danych. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-19(03)** | **DE-IDENTYFIKACJA \| UJAWNIANIE DANYCH** | |
| | **SI-19(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury anonimizacji; procedury minimalizacji udostępniania danych identyfikacyjnych; konfiguracja systemu; mechanizmy udostępniania danych; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-19(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za anonimizację zbioru danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-19(03)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspierające lub wdrażające usuwanie elementów informacji identyfikacyjnych ze zbioru danych]. |

| | | |
|---|---|---|
| **SI-19(04)** | **DE-IDENTYFIKACJA \| USUWANIE, MASKOWANIE, SZYFROWANIE, HASZOWANIE LUB WYMIANA IDENTYFIKATORÓW BEZPOŚREDNICH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-19(04)** | identyfikatory bezpośrednie zawarte w zbiorze danych są usuwane, maskowane, szyfrowane, haszowane lub zastępowane. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-19(04)** | **DE-IDENTYFIKACJA \| USUWANIE, MASKOWANIE, SZYFROWANIE, HASZOWANIE LUB WYMIANA IDENTYFIKATORÓW BEZPOŚREDNICH** | |
| | **SI-19(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania informacji umożliwiających identyfikację osób; procedury anonimizacji; konfiguracja systemu; dokumentacja zanonimizowanych zbiorów danych; narzędzia do usuwania, maskowania, szyfrowania, haszowania lub zastępowania identyfikatorów bezpośrednich; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-19(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za anonimizację zbioru danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-19(04)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspierające lub wdrażające usuwanie, maskowanie, szyfrowanie, haszowanie lub zastępowanie identyfikatorów bezpośrednich]. |

| | | |
|---|---|---|
| **SI-19(05)** | **DE-IDENTYFIKACJA \| ZABEZPIECZENIE UJAWNIANIA DANYCH STATYSTYCZNYCH** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-19(05)[01]** | danymi liczbowymi manipuluje się tak, aby wyniki analizy nie umożliwiały identyfikacji żadnej osoby lub organizacji; |
| | **SI-19(05)[02]** | tabelami dotyczącymi procedur awaryjnych manipuluje się tak, aby wyniki analizy nie umożliwiały identyfikacji żadnej osoby lub organizacji; |
| | **SI-19(05)[03]** | ustaleniami statystycznymi manipuluje się tak, aby wyniki analizy nie umożliwiały identyfikacji żadnej osoby lub organizacji. |

| | | |
|---|---|---|
| **SI-19(05)** | **DE-IDENTYFIKACJA \| ZABEZPIECZENIE UJAWNIANIA DANYCH STATYSTYCZNYCH** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-19(05)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury anonimizacji; konfiguracja systemu; zanonimizowane zbiory danych; raport z analizy statystycznej; narzędzia kontroli ujawniania danych statystycznych; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-19(05)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za anonimizację zbioru danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-19(05)-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wspomagające lub wdrażające kontrolę ujawniania danych statystycznych]. |

| | | |
|---|---|---|
| **SI-19(06)** | **DE-IDENTYFIKACJA \| PRYWATNOŚĆ RÓŻNICOWA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-19(06)** | zapobiega się ujawnieniu danych identyfikacyjnych poprzez dodanie niedeterministycznego szumu do wyników operacji matematycznych przed podaniem wyników. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-19(06)** | **DE-IDENTYFIKACJA \| PRYWATNOŚĆ RÓŻNICOWA** | |
| | **SI-19(06)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury anonimizacji; konfiguracja systemu; zanonimizowane zbiory danych; różnicowe narzędzia ochrony prywatności; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka związanego z prywatnością; inne istotne dokumenty lub zapisy]. |
| | **SI-19(06)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za anonimizację zbioru danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-19(06)-Test** | [WYBÓR SPOŚRÓD: Systemy zapytań online; automatyczne mechanizmy wspierające lub wdrażające prywatność różnicową]. |

| | | |
|---|---|---|
| **SI-19(07)** | **DE-IDENTYFIKACJA \| ZATWIERDZONE ALGORYTMY I OPROGRAMOWANIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-19(07)[01]** | anonimizacja danych odbywa się przy użyciu zatwierdzonych algorytmów; |
| | **SI-19(07)[02]** | anonimizacja danych odbywa się przy użyciu oprogramowania, które jest zatwierdzone do wdrażania algorytmów. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-19(07)** | **DE-IDENTYFIKACJA \| ZATWIERDZONE ALGORYTMY I OPROGRAMOWANIE** | |
| | **SI-19(07)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury anonimizacji; konfiguracja systemu; zanonimizowane zbiory danych; narzędzia weryfikacji algorytmów i oprogramowania; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-19(07)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za anonimizację zbioru danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-19(07)-Test** | [WYBÓR SPOŚRÓD: Zatwierdzone algorytmy i oprogramowanie]. |

| | | |
|---|---|---|
| **SI-19(08)** | **DE-IDENTYFIKACJA \| ZMOTYWOWANY INTRUZ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-19(08)** | zanonimizowane zbiory danych poddaje się testowi zmotywowanego intruza w celu ustalenia, czy nadal zawierają one dane identyfikacyjne bądź czy proces anonimizacji danych może zostać odwrócony. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-19(08)-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury anonimizacji; konfiguracja systemu; procedury przeprowadzania testów zmotywowanego intruza; zanonimizowane zbiory danych; plan bezpieczeństwa systemu; plan ochrony prywatności; ocena wpływu na prywatność; dokumentacja oceny ryzyka dla ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-19(08)** | **DE-IDENTYFIKACJA \| ZMOTYWOWANY INTRUZ** | |
| | **SI-19(08)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za anonimizację zbioru danych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-19(08)-Test** | [WYBÓR SPOŚRÓD: Test zmotywowanego intruza]. |

| | | |
|---|---|---|
| **SI-20** | **SKAŻENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-20_ODP** | ***określono systemy lub komponenty systemu, w które mają być wbudowane dane lub funkcje;*** |
| | **SI-20** | dane lub funkcje są wbudowane w ***<systemy lub komponenty systemu SI-20_ODP>***, umożliwiając określenie, czy nastąpiła eksfiltracja danych lub ich niewłaściwie usunięcie z organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-20-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury dotyczące integralności oprogramowania i informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; polityka i procedury dotyczące techniki inżynierii bezpieczeństwa polegającej na oszukaniu atakujących; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SI-20** | **SKAŻENIE** | |
| | **SI-20-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za wykrywanie skażonych danych; personel organizacyjny odpowiedzialny za inżynierię bezpieczeństwa systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności]. |
| | **SI-20-Test** | [WYBÓR SPOŚRÓD: Automatyczne mechanizmy wykrywania naruszeń po włamaniu; wabiki, pułapki, przynęty i metody zwodzenia atakujących; mechanizmy wykrywania i powiadamiania]. |

| | | |
|---|---|---|
| **SI-21** | **ODŚWIEŻENIE INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-21_ODP[01]** | ***określono informacje, które mają być odświeżane;*** |
| | **SI-21_ODP[02]** | ***określono częstotliwość odświeżania informacji;*** |
| | **SI-21** | ***<informacje SI-21_ODP[01]>*** są odświeżane z ***<częstotliwością SI-21_ODP[02]>*** lub są generowane na żądanie i usuwane, gdy nie są już potrzebne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-21-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury dotyczące integralności oprogramowania i informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; procedury odświeżania informacji; wykaz informacji podlegających odświeżaniu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |

| **SI-21** | **ODŚWIEŻENIE INFORMACJI** | |
|---|---|---|
| | **SI-21-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za odświeżanie informacji; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i prywatność; personel organizacyjny odpowiedzialny za inżynierię bezpieczeństwa systemów; programiści systemu]. |
| | **SI-21-Test** | [WYBÓR SPOŚRÓD: Mechanizmy odświeżania informacji; procesy organizacyjne dotyczące odświeżania informacji]. |

| **SI-22** | **RÓŻNICOWANIE INFORMACJI** | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-22_ODP[01]** | ***określono alternatywne źródła informacji wykorzystywanych w ramach podstawowych funkcji i usług;*** |
| | **SI-22_ODP[02]** | ***określono podstawowe funkcje i usługi, które wymagają alternatywnych źródeł informacji;*** |
| | **SI-22_ODP[03]** | ***określono systemy lub komponenty systemu, które wymagają alternatywnego źródła informacji na potrzeby podstawowych funkcji lub usług;*** |
| | **SI-22a.** | ***<wskazano alternatywne źródła informacji SI-22_ODP[01]>*** dla ***<podstawowych funkcji i usług SI-22_ODP[02]>***; |
| | **SI-22b.** | wykorzystuje się alternatywne źródło informacji do realizacji podstawowych funkcji lub usług w ***<systemach lub komponentach systemu SI-22_ODP[03]>***, jeżeli podstawowe źródło informacji jest uszkodzone lub niedostępne. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SI-22** | **RÓŻNICOWANIE INFORMACJI** | |
| | **SI-22-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; wykaz źródeł informacji; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-22-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; personel organizacyjny odpowiedzialny za inżynierię bezpieczeństwa systemów; programiści systemów]. |
| | **SI-22-Test** | [WYBÓR SPOŚRÓD: Automatyczne metody i mechanizmy konwersji informacji z nośnika analogowego na cyfrowy]. |

| | | |
|---|---|---|
| **SI-23** | **FRAGMENTACJA INFORMACJI** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SI-23_ODP[01]** | ***określono okoliczności, które wymagają stosowania fragmentacji informacji;*** |
| | **SI-23_ODP[02]** | ***określono informacje, które mają być poddawane fragmentacji;*** |
| | **SI-23_ODP[03]** | ***określono systemy lub komponenty systemu, pomiędzy które mają być dystrybuowane informacje poddane fragmentacji;*** |
| | **SI-23a.** | w ***<okolicznościach SI-23_ODP[01]>*** stosuje się fragmentację ***<informacji SI-23_ODP[02]>***; |
| | **SI-23b.** | w ***<okolicznościach SI-23_ODP[01]>*** informacje poddane fragmentacji są dystrybuowane pomiędzy ***<systemy lub komponenty systemu SI-23_ODP[03]>***. |

| | | |
|---|---|---|
| **SI-23** | **FRAGMENTACJA INFORMACJI** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SI-23-Badanie** | [WYBÓR SPOŚRÓD: Polityka integralności systemu i informacji; procedury integralności systemu i informacji; polityka przetwarzania danych identyfikacyjnych; procedury dotyczące integralności oprogramowania i informacji; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; procedury identyfikacji informacji do fragmentacji i dystrybucji pomiędzy systemami/komponentami systemu; wykaz informacji dystrybuowanych i fragmentowanych; wykaz okoliczności wymagających fragmentacji informacji; architektura korporacyjna; architektura bezpieczeństwa systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SI-23-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo i prywatność informacji; personel organizacyjny odpowiedzialny za inżynierię bezpieczeństwa systemów; programiści systemów; architekci bezpieczeństwa]. |
| | **SI-23-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne służące identyfikacji informacji do fragmentacji i dystrybucji w ramach komponentów systemu/systemu; automatyczne mechanizmy wspierające lub wdrażające fragmentację i dystrybucję informacji w ramach systemu/komponentów systemu]. |

## 4.20. KATEGORIA SR - ZARZĄDZANIE RYZYKIEM W ŁAŃCUCHU DOSTAW

| | | |
|---|---|---|
| **SR-01** | **POLITYKA I PROCEDURY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-01_ODP[01]** | ***określono personel lub role, wśród których ma być rozpowszechniana polityka zarządzania ryzykiem łańcucha dostaw;*** |
| | **SR-01_ODP[02]** | ***określono personel lub role, wśród których mają być rozpowszechniane procedury zarządzania ryzykiem łańcucha dostaw;*** |
| | **SR-01_ODP[03]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: (poziom organizacji; misja/poziom procesu biznesowego; poziom systemu);*** |
| | **SR-01_ODP[04]** | ***określono urzędnika odpowiedzialnego za zarządzanie opracowywaniem, dokumentowaniem i rozpowszechnianiem polityki i procedur w zakresie zarządzania ryzykiem łańcucha dostaw;*** |
| | **SR-01_ODP[05]** | ***określono częstotliwość przeglądu i aktualizacji obowiązującej polityki zarządzania ryzykiem łańcucha dostaw;*** |
| | **SR-01_ODP[06]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji obowiązującej polityki zarządzania ryzykiem łańcucha dostaw;*** |
| | **SR-01_ODP[07]** | ***określono częstotliwość, z jaką dokonuje się przeglądu i aktualizacji aktualnej procedury zarządzania ryzykiem łańcucha dostaw;*** |
| | **SR-01_ODP[08]** | ***określono zdarzenia, które wymagają przeglądu i aktualizacji procedur zarządzania ryzykiem łańcucha dostaw;*** |
| | **SR-01a.[01]** | opracowano i udokumentowano politykę zarządzania ryzykiem łańcucha dostaw; |
| | **SR-01a.[02]** | polityka zarządzania ryzykiem łańcucha dostaw jest rozpowszechniana wśród ***<personelu lub ról SR-01_ODP[01]>***; |

| | | |
|---|---|---|
| **SR-01** | **POLITYKA I PROCEDURY** | |
| | **SR-01a.[03]** | opracowano i udokumentowano procedury zarządzania ryzykiem łańcucha dostaw, ułatwiające wdrażanie polityki w tym obszarze oraz związane z nią zabezpieczenia; |
| | **SR-01a.[04]** | procedury zarządzania ryzykiem łańcucha dostaw są rozpowszechniane wśród ***<personelu lub ról SR-01_ODP[02]>***. |
| | **SR-01a.01(a)[01]** | polityka zarządzania ryzykiem łańcucha dostaw ***<WYBRANA WARTOŚĆ PARAMETRU SR-01_ODP[03]>*** odnosi się do celu; |
| | **SR-01a.01(a)[02]** | polityka zarządzania ryzykiem łańcucha dostaw ***<WYBRANA WARTOŚĆ PARAMETRU SR-01_ODP[03]>*** odnosi się do zakresu; |
| | **SR-01a.01(a)[03]** | polityka zarządzania ryzykiem łańcucha dostaw ***<WYBRANA WARTOŚĆ PARAMETRU SR-01_ODP[03]>*** odnosi się do ról; |
| | **SR-01a.01(a)[04]** | polityka zarządzania ryzykiem łańcucha dostaw ***<WYBRANA WARTOŚĆ PARAMETRU SR-01_ODP[03]>*** odnosi się do obowiązków; |
| | **SR-01a.01(a)[05]** | polityka zarządzania ryzykiem łańcucha dostaw ***<WYBRANA WARTOŚĆ PARAMETRU SR-01_ODP[03]>*** odnosi się do zaangażowania kierownictwa; |
| | **SR-01a.01(a)[06]** | polityka zarządzania ryzykiem łańcucha dostaw ***<WYBRANA WARTOŚĆ PARAMETRU SR-01_ODP[03]>*** odnosi się do koordynacji pomiędzy podmiotami organizacji; |
| | **SR-01a.01(a)[07]** | polityka zarządzania ryzykiem łańcucha dostaw ***<WYBRANA WARTOŚĆ PARAMETRU SR-01_ODP[03]>*** odnosi się do zgodności; |
| | **SR-01a.01(b)** | polityka zarządzania ryzykiem łańcucha dostaw ***<WYBRANA WARTOŚĆ PARAMETRU SR-01_ODP[03]>*** jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, politykami, normami i wytycznymi; |

| | | |
|---|---|---|
| **SR-01** | **POLITYKA I PROCEDURY** | |
| | **SR-01b.** | ***<urzędnik SR-01_ODP[04]>*** jest wyznaczony do zarządzania opracowywaniem, dokumentacją, i rozpowszechnianiem polityki i procedur zarządzania ryzykiem łańcucha dostaw; |
| | **SR-01c.01[01]** | aktualna polityka zarządzania ryzykiem łańcucha dostaw jest przeglądana i aktualizowana z ***<częstotliwością SR-01_ODP[05]>***; |
| | **SR-01c.01[02]** | aktualna polityka zarządzania ryzykiem łańcucha dostaw jest przeglądana i aktualizowana po ***<zdarzeniach SR-01_ODP[06]>***; |
| | **SR-01c.02[01]** | aktualne procedury zarządzania ryzykiem łańcucha dostaw są przeglądane i aktualizowane z ***<częstotliwością SR-01_ODP[07]>***; |
| | **SR-01c.02[02]** | aktualne procedury zarządzania ryzykiem łańcucha dostaw są przeglądane i aktualizowane po***<zdarzeniach SR-01_ODP[08]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-01-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania ryzykiem łańcucha dostaw; procedury zarządzania ryzykiem łańcucha dostaw; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SR-01-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem w organizacji]. |

| | | |
|---|---|---|
| **SR-02** | **PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-02_ODP[01]** | ***określono systemy, komponenty systemu lub usługi systemowe, dla których opracowano plan zarządzania ryzykiem łańcucha dostaw;*** |
| | **SR-02_ODP[02]** | ***określono częstotliwość przeglądu i aktualizacji planu zarządzania ryzykiem łańcucha dostaw;*** |
| | **SR-02a.[01]** | opracowano plan zarządzania ryzykiem łańcucha dostaw; |
| | **SR-02a.[02]** | plan zarządzania ryzykiem łańcucha dostaw uwzględnia ryzyko związane z pracami badawczo-rozwojowymi w zakresie ***<systemu, komponentów systemu lub usług systemowych SR-02_ODP[01]>***; |
| | **SR-02a.[03]** | plan zarządzania ryzykiem łańcucha dostaw uwzględnia ryzyko związane z projektowaniem ***<systemu, komponentów systemu lub usług systemowych SR-02_ODP[01]>***; |
| | **SR-02a.[04]** | plan zarządzania ryzykiem łańcucha dostaw uwzględnia ryzyko związane z produkcją ***<systemu, komponentów systemu lub usług systemowych SR-02_ODP[01]>***; |
| | **SR-02a.[05]** | plan zarządzania ryzykiem w łańcuchu dostaw uwzględnia ryzyko związane z nabywaniem ***<systemu, komponentów systemu lub usług systemowych SR-02_ODP[01]>***; |
| | **SR-02a.[06]** | plan zarządzania ryzykiem łańcucha dostaw uwzględnia ryzyko związane z dostawą ***<systemu, komponentów systemu lub usług systemowych SR-02_ODP[01]>***; |
| | **SR-02a.[07]** | plan zarządzania ryzykiem w łańcuchu dostaw uwzględnia ryzyko związane z integracją***<systemu, komponentów systemu lub usług systemowych SR-02_ODP[01]>***; |

| | | |
|---|---|---|
| **SR-02** | **PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW** | |
| | **SR-02a.[08]** | plan zarządzania ryzykiem łańcucha dostaw uwzględnia ryzyko związane z eksploatacją i utrzymaniem ***<systemu, komponentów systemu lub usług systemowych SR-02_ODP[01]>***; |
| | **SR-02a.[09]** | plan zarządzania ryzykiem łańcucha dostaw uwzględnia ryzyko związane z utylizacją***<systemu, komponentów systemu lub usług systemowych SR-02_ODP[01]>***; |
| | **SR-02b.** | plan zarządzania ryzykiem łańcucha dostaw jest poddawany przeglądowi i aktualizowany z ***<częstotliwością SR-02_ODP[02]>*** lub w miarę potrzeb w celu uwzględnienia zmian dotyczących zagrożeń, samej organizacji, lub jej środowiska; |
| | **SR-02c.[01]** | plan zarządzania ryzykiem łańcucha dostaw jest chroniony przed nieautoryzowanym ujawnieniem; |
| | **SR-02c.[02]** | plan zarządzania ryzykiem łańcucha dostaw jest chroniony przed nieautoryzowaną modyfikacją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SR-02** | **PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW** | |
| | **SR-02-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania ryzykiem łańcucha dostaw; procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; procedury nabywania systemów i usług; procedury dotyczące ochrony łańcucha dostaw;<br><br>procedury ochrony planu zarządzania ryzykiem łańcucha dostaw przed nieuprawnionym ujawnieniem i modyfikacją; procedury dotyczące cyklu życia systemu; procedury dotyczące integracji wymagań w zakresie bezpieczeństwa informacji i prywatności z procesem nabywania; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; lista zagrożeń dla łańcucha dostaw; lista zabezpieczeń wdrożonych w celu ochrony przed zagrożeniami łańcucha dostaw; dokumentacja cyklu życia systemu;<br><br>umowy i procedury międzyorganizacyjne; plan bezpieczeństwa systemu; plan ochrony prywatności; plan programu ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SR-02-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i prywatność; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-02-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania i dokumentowania cyklu życia systemu (SDLC); procesy organizacyjne dotyczące identyfikacji ról i obowiązków w zakresie SDLC; procesy organizacyjne dotyczące włączania zarządzania ryzykiem łańcucha dostaw do procesu SDLC; mechanizmy wspierające lub wdrażające proces SDLC]. |

| | | |
|---|---|---|
| **SR-02(01)** | **PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW \| POWOŁANIE ZESPOŁU ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-02(01)_ODP[01]** | ***określono personel, role i obowiązki zespołu ds. zarządzania ryzykiem łańcucha dostaw;*** |
| | **SR-02(01)_ODP[02]** | ***określono działania w zakresie zarządzania ryzykiem łańcucha dostaw;*** |
| | **SR-02(01)** | powołano zespół ds. zarządzania ryzykiem łańcucha dostaw obejmujący ***<personel, role i obowiązki SR-02(01)_ODP[01]>*** w celu realizowania i wspierania<br>***<działań w zakresie zarządzania ryzykiem łańcucha dostaw SR-02(01)_ODP[02]>.*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-02(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania ryzykiem łańcucha dostaw; procedury zarządzania ryzykiem łańcucha dostaw; statut zespołu ds. zarządzania ryzykiem łańcucha dostaw; strategia zarządzania ryzykiem łańcucha dostaw; plan wdrażania zarządzania ryzykiem łańcucha dostaw; procedury dotyczące ochrony łańcucha dostaw; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SR-02(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem w organizacji; radca prawny; personel organizacyjny odpowiedzialny za ciągłość działania]. |

| | | |
|---|---|---|
| **SR-03** | **ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-03_ODP[01]** | ***określono system lub komponent systemu wymagający zastosowania procesu lub procesów identyfikacji i usuwania słabych punktów lub braków;*** |
| | **SR-03_ODP[02]** | ***określono personel ds. łańcucha dostaw, z którym należy koordynować proces lub procesy mające na celu identyfikację i eliminację słabych punktów lub braków w elementach i procesach łańcucha dostaw;*** |
| | **SR-03_ODP[03]** | ***określono zabezpieczenia dla łańcucha dostaw stosowane w celu ochrony przed zagrożeniami dla systemu, komponentu systemu lub usługi systemowej, a także w celu ograniczenia szkód lub skutków zdarzeń związanych z łańcuchem dostaw;*** |
| | **SR-03_ODP[04]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {plany bezpieczeństwa i ochrony prywatności; plan zarządzania ryzykiem łańcucha dostaw; <dokument SR-03_ODP[05]>};*** |
| | **SR-03_ODP[05]** | ***określono dokument identyfikujący wybrane i wdrażane procesy oraz zabezpieczenia w łańcuchu dostaw (jeśli wybrano);*** |
| | **SR-03a.[01]** | ustanowiono proces lub procesy w celu identyfikacji i usunięcia słabych punktów lub braków w elementach i procesach łańcucha dostaw ***<systemu lub komponentu systemu SR-03_ODP[01]>***; |
| | **SR-03a.[02]** | proces lub procesy służące identyfikacji i usuwaniu słabych punktów lub braków w elementach i procesach łańcucha dostaw ***<systemu lub komponentu systemu SR-03_ODP[01]>*** jest koordynowany/są koordynowane z ***<personelem ds. łańcucha dostaw SR-03_ODP[02]>***; |

| | | |
|---|---|---|
| **SR-03** | **ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW** | |
| | **SR-03b.** | ***<zabezpieczenia łańcucha dostaw SR-03_ODP[03]>*** są stosowane w celu ochrony przed ryzykiem dla systemu, komponentu systemu lub usługi systemowej związanym z łańcuchem dostaw, a także w celu ograniczenia szkód lub konsekwencji wynikających ze zdarzeń związanych z łańcuchem dostaw; |
| | **SR-03c.** | wybrane i wdrażane procesy i zabezpieczenia dla łańcucha dostaw są udokumentowane w ***<WYBRANA WARTOŚĆ PARAMETRU SR-03_ODP[04]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-03-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania ryzykiem łańcucha dostaw; procedury zarządzania ryzykiem łańcucha dostaw; strategia zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; dokumentacja inwentaryzacyjna systemów i krytycznych komponentów systemu; polityka nabywania systemu i usług; procedury nabywania systemu i usług; procedury dotyczące integracji wymogów w zakresie bezpieczeństwa informacji i ochrony prywatności z procesem nabywania; dokumentacja przetargowa; dokumentacja nabywania (w tym zamówienia zakupu); umowy o poziomie usług; umowy nabycia systemu lub usług; dokumentacja dotycząca rejestru ryzyka; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SR-03-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i prywatność; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-03-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące identyfikacji i usuwania braków w zakresie elementów i procesów w łańcuchu dostaw]. |

| | | |
|---|---|---|
| **SR-03(01)** | **ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW \| ZRÓŻNICOWANA BAZA DOSTAW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-03(01)_ODP[01]** | ***określono komponenty systemu dostępne ze zróżnicowanych źródeł;*** |
| | **SR-03(01)_ODP[02]** | ***określono usługi systemowe dostępne ze zróżnicowanych źródeł;*** |
| | **SR-03(01)[01]** | dla ***<komponentów systemu SR-03(01)_ODP[01]>*** dostępny jest zróżnicowany zestaw źródeł; |
| | **SR-03(01)[02]** | dla ***<usług SR-03(01)_ODP[02]>*** dostępny jest zróżnicowany zestaw źródeł. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-03(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; polityka planowania; procedury ochrony łańcucha dostaw; fizyczna inwentaryzacja krytycznych systemów i komponentów systemu; wykaz krytycznych dostawców, usługodawców, programistów i umów; zapisy dotyczące inwentaryzacji krytycznych komponentów systemu;<br>wykaz zabezpieczeń zapewniających odpowiednią podaż krytycznych komponentów systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-03(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zakup systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę łańcucha dostaw]. |

| | | |
|---|---|---|
| **SR-03(01)** | **ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW \| ZRÓŻNICOWANA BAZA DOSTAW** | |
| | **SR-03(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne służące określeniu i stosowaniu zabezpieczeń zapewniających odpowiednią podaż krytycznych komponentów systemu; procesy służące identyfikacji krytycznych dostawców; mechanizmy wspierające lub wdrażające zabezpieczenia zapewniające odpowiednią podaż krytycznych komponentów systemu]. |

| | | |
|---|---|---|
| **SR-03(02)** | **ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW \| OGRANICZANIE SZKODY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-03(02)_ODP** | ***określono środki kontroli mające na celu ograniczenie szkód wyrządzanych przez potencjalnych atakujących w łańcuchu dostaw;*** |
| | **SR-03(02)** | stosuje się ***<zabezpieczenia SR-03(02)_ODP>*** w celu ograniczenia szkód wyrządzonych przez potencjalnych atakujących, podejmujących próby rozpoznania i zaatakowania łańcucha dostaw organizacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SR-03(02) | ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW \| OGRANICZANIE SZKODY | |
|---|---|---|
| | **SR-03(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; polityka zarządzania konfiguracją; procedury dotyczące ochrony łańcucha dostaw; procedury dotyczące integracji wymogów bezpieczeństwa informacji w procesie nabywania; procedury dotyczące konfiguracji bazowej systemu;<br>plan zarządzania konfiguracją; dokumentacja projektowa systemu; architektura systemu i związana z nią dokumentacja konfiguracyjna; dokumentacja przetargowa; dokumentacja nabycia; umowy nabycia systemu, komponentu systemu lub usługi systemowej; oceny zagrożeń; oceny podatności; wykaz zabezpieczeń, które należy podjąć w celu ochrony organizacyjnego łańcucha dostaw przed potencjalnymi zagrożeniami; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-03(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-03(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania i stosowania zabezpieczeń w celu ograniczenia szkód wywołanych przez atakujących w organizacyjnym łańcuchu dostaw; mechanizmy wspierające lub wdrażające definiowanie i stosowanie zabezpieczeń w celu ochrony organizacyjnego łańcucha dostaw]. |

| | | |
|---|---|---|
| **SR-03(03)** | **ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW \| PODWYKONAWCY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-03(03)** | zabezpieczenia zawarte w umowach z głównymi wykonawcami są również zawarte w umowach z podwykonawcami. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-03(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; procedury dotyczące ochrony łańcucha dostaw; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; umowy i procedury międzyorganizacyjne; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-03(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-03(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zawierania umów i ustanawiania procedur międzyorganizacyjnych z podmiotami łańcucha dostaw]. |

| | | |
|---|---|---|
| **SR-04** | **POCHODZENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-04_ODP** | ***określono systemy, komponenty systemu i powiązane dane, które wymagają potwierdzenia autentyczności pochodzenia;*** |

| | | |
|---|---|---|
| **SR-04** | **POCHODZENIE** | |
| | **SR-04[01]** | potwierdzenie autentyczności pochodzenia ***<systemów, komponentów systemu i powiązanych danych SR-04_ODP>*** jest udokumentowane; |
| | **SR-04[02]** | potwierdzenie autentyczności pochodzenia ***<systemów, komponentów systemu i powiązanych danych SR-04_ODP>*** jest monitorowane; |
| | **SR-04[03]** | potwierdzenie autentyczności pochodzenia ***<systemów, komponentów systemu i powiązanych danych SR-04_ODP>*** jest utrzymywane; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-04-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania ryzykiem łańcucha dostaw; procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; dokumentacja krytycznych systemów i komponentów systemu oraz związanych z nimi danych; dokumentacja przedstawiająca historię własności, nadzoru i lokalizacji krytycznych systemów lub komponentów systemu oraz zmian w nich zachodzących; architektura systemu; umowy i procedury międzyorganizacyjne; umowy; plan bezpieczeństwa systemu; plan ochrony prywatności; polityka przetwarzania danych identyfikacyjnych; inne istotne dokumenty lub zapisy]. |
| | **SR-04-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i prywatność; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-04-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące identyfikacji pochodzenia krytycznych systemów i komponentów systemu; mechanizmy stosowane do dokumentowania, monitorowania lub utrzymywania potwierdzenia autentyczności pochodzenia]. |

| | | |
|---|---|---|
| **SR-04(01)** | **POCHODZENIE \| TOŻSAMOŚĆ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-04(01)_ODP** | ***określono elementy łańcucha dostaw oraz procesy i personel związany z systemami i krytycznymi komponentami systemu, które wymagają unikalnej identyfikacji;*** |
| | **SR-04(01)[01]** | ustanowiono unikalną identyfikację dla ***<elementów, procesów i personelu łańcucha dostaw SR-04(01)_ODP>***; |
| | **SR-04(01)[02]** | utrzymuje się unikalną identyfikację dla ***<elementów, procesów i personelu łańcucha dostaw SR-04(01)_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-04(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; procedury dotyczące ochrony łańcucha dostaw; procedury dotyczące integracji wymogów bezpieczeństwa informacji z procesem nabywania; wykaz elementów, procesów i uczestników łańcucha dostaw (związanych z systemem, komponentem systemu lub usługą systemową) wymagających wdrażania procesów, procedur, narzędzi, mechanizmów, sprzętu, technik lub konfiguracji dotyczącej unikalnej identyfikacji; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-04(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę łańcucha dostaw; personel organizacyjny odpowiedzialny za ustanowienie i utrzymanie unikalnej identyfikacji elementów, procesów i uczestników łańcucha dostaw]. |

| | | |
|---|---|---|
| **SR-04(01)** | **POCHODZENIE \| TOŻSAMOŚĆ** | |
| | **SR-04(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania, ustanawiania i utrzymywania unikalnej identyfikacji dla elementów, procesów i uczestników łańcucha dostaw; mechanizmy wspierające lub wdrażające definiowanie, ustanawianie i utrzymywanie niepowtarzalnej identyfikacji dla elementów, procesów i uczestników łańcucha dostaw]. |

| | | |
|---|---|---|
| **SR-04(02)** | **POCHODZENIE \| ŚLEDZENIE PRZESYŁEK** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-04(02)_ODP** | ***określono systemy i krytyczne komponenty systemu, które wymagają unikalnej identyfikacji w celu śledzenia przesyłek w łańcuchu dostaw;*** |
| | **SR-04(02)[01]** | ustanowiono unikalną identyfikację dla ***<systemów i krytycznych komponentów systemu SR-04(02)_ODP> w*** celu śledzenia przesyłek w łańcuchu dostaw; |
| | **SR-04(02)[02]** | utrzymuje się unikalną identyfikację ***<systemów i krytycznych komponentów systemu SR-04(02)_ODP> w*** celu śledzenia przesyłek w łańcuchu dostaw. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| SR-04(02) | POCHODZENIE \| ŚLEDZENIE PRZESYŁEK | |
|---|---|---|
| | **SR-04(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; procedury dotyczące ochrony łańcucha dostaw; procedury dotyczące integracji wymogów bezpieczeństwa informacji z procesem nabywania; plan zarządzania ryzykiem łańcucha dostaw; wykaz elementów, procesów i uczestników łańcucha dostaw (związanych z systemem, komponentem systemu lub usługą systemową) wymagających wdrażania procesów, procedur, narzędzi, mechanizmów, sprzętu, technik lub konfiguracji dotyczącej unikalnej identyfikacji; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-04(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę łańcucha dostaw; personel organizacyjny odpowiedzialny za ustanowienie i utrzymanie unikalnej identyfikacji elementów, procesów i uczestników łańcucha dostaw]. |
| | **SR-04(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania, ustanawiania i utrzymywania unikalnej identyfikacji dla elementów, procesów i uczestników łańcucha dostaw; mechanizmy wspierające lub wdrażające definiowanie, ustanawianie i utrzymywanie niepowtarzalnej identyfikacji dla elementów, procesów i uczestników łańcucha dostaw]. |

| SR-04(03) | POCHODZENIE \|POTWIERDZANIE AUTENTYCZNOŚCI I NIEZMIENNOŚCI | |
|---|---|---|
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-04(03)_ODP[01]** | ***określono zabezpieczenia mające na celu weryfikację autentyczności otrzymanego systemu lub komponentu systemu;*** |

| | | |
|---|---|---|
| **SR-04(03)** | **POCHODZENIE \|POTWIERDZANIE AUTENTYCZNOŚCI I NIEZMIENNOŚCI** | |
| | **SR-04(03)_ODP[02]** | ***określono zabezpieczenia mające na celu weryfikację, że otrzymany system lub komponent systemu nie został zmodyfikowany;*** |
| | **SR-04(03)[01]** | stosuje się ***<zabezpieczenia SR-04(03)_ODP[01]>*** w celu potwierdzenia, że otrzymany system lub komponent systemu jest autentyczny; |
| | **SR-04(03)[02]** | stosuje się ***<zabezpieczenia SR-04(03)_ODP[02]>*** w celu potwierdzenia, że otrzymany system lub komponent systemu nie został zmodyfikowany; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-04(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; procedury ochrony łańcucha dostaw; procedury dotyczące zasady wykorzystywania zaufanych komponentów przy specyfikacji, projektowaniu, opracowywaniu, wdrażaniu i modyfikowaniu systemu; dokumentacja projektowa systemu; procedury dotyczące integracji wymogów bezpieczeństwa informacji z procesem nabywania; dokumentacja przetargowa; dokumentacja nabywania; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; dokumentacja dowodowa (w tym stosowne konfiguracje) wskazująca, że system lub komponent systemu jest autentyczny i nie został zmodyfikowany; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-04(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |

| | | |
|---|---|---|
| **SR-04(03)** | **POCHODZENIE \|POTWIERDZANIE AUTENTYCZNOŚCI I NIEZMIENNOŚCI** | |
| | **SR-04(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania i stosowania zabezpieczeń weryfikacyjnych; mechanizmy wspierające lub wdrażające definiowanie i stosowanie zabezpieczeń weryfikacyjnych; mechanizmy wspierające stosowanie zasady wykorzystywania zaufanych komponentów przy specyfikacji, projektowaniu, opracowywaniu, wdrażaniu i modyfikowaniu systemu]. |

| | | |
|---|---|---|
| **SR-04(04)** | **POCHODZENIE \| INTEGRALNOŚĆ ŁAŃCUCHA DOSTAW - POCHODZENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-04(04)_ODP[01]** | ***określono zabezpieczenia stosowane w celu zapewnienia integralności systemu i komponentu systemu;*** |
| | **SR-04(04)_ODP[02]** | ***określono metodę analizy przeprowadzanej w celu potwierdzenia wewnętrznego składu i pochodzenia krytycznych lub istotnych dla misji technologii, produktów i usług, aby zapewnić integralność systemu i komponentu systemu;*** |
| | **SR-04(04)[01]** | stosuje się ***<zabezpieczenia SR-04(04)_ODP[01]>*** w celu zapewnienia integralności systemu i komponentów systemu; |
| | **SR-04(04)[02]** | stosuje się ***<metodę analizy SR-04(04)_ODP[02]>*** w celu zapewnienia integralności systemu i komponentów systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SR-04(04)** | **POCHODZENIE \| INTEGRALNOŚĆ ŁAŃCUCHA DOSTAW - POCHODZENIE** | |
| | **SR-04(04)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; procedury dotyczące ochrony łańcucha dostaw; zestawienie materiałów dla krytycznych systemów lub komponentów systemu; dokumentacja nabywania; etykiety identyfikacyjne oprogramowania; deklaracje producenta dotyczące atrybutów platformy (np. numery seryjne,<br>wykaz komponentów sprzętowych) i pomiarów (np. hashów oprogramowania układowego), które są ściśle związane z samym sprzętem; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-04(04)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-04(04)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące identyfikacji pochodzenia; procesy organizacyjne dotyczące określania i weryfikacji integralności wewnętrznego składu krytycznych systemów i komponentów systemu; mechanizmy dotyczące określania i weryfikacji integralności wewnętrznego składu krytycznych systemów i komponentów systemu]. |

| | | |
|---|---|---|
| **SR-05** | **STRATEGIE, NARZĘDZIA I METODY NABYCIA** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-05_ODP** | ***określono strategie pozyskiwania, narzędzia umowne i metody nabywania w celu identyfikacji i łagodzenia ryzyka łańcucha dostaw, a także zabezpieczenia przed nim;*** |

| | | |
|---|---|---|
| **SR-05** | **STRATEGIE, NARZĘDZIA I METODY NABYCIA** | |
| | **SR-05[01]** | stosuje się ***<strategie, narzędzia i metody SR-05_ODP> w*** celu ochrony przed ryzykiem łańcucha dostaw; |
| | **SR-05[02]** | stosuje się ***<strategie, narzędzia i metody SR-05_ODP> w*** celu identyfikacji ryzyka łańcucha dostaw; |
| | **SR-05[03]** | stosuje się ***<strategie, narzędzia i metody SR-05_ODP> w*** celu łagodzenia ryzyka łańcucha dostaw. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-05-Badanie** | [WYBÓR SPOŚRÓD: Polityka zarządzania ryzykiem łańcucha dostaw; procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; procedury nabywania systemów i usług; procedury dotyczące ochrony łańcucha dostaw; procedury dotyczące integracji wymogów w zakresie bezpieczeństwa informacji i ochrony prywatności z procesem nabywania; dokumentacja przetargowa; dokumentacja nabywania (w tym zamówienia zakupu); umowy o poziomie usług; umowy nabycia systemów, komponentów systemów, lub usług;<br><br>dokumentacja programów szkoleniowych, edukacyjnych i uświadamiających personel w zakresie ryzyka łańcucha dostaw; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SR-05-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i prywatność; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-05-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące określania i wykorzystania dostosowanych strategii nabywania, narzędzi umownych i metod udzielania zamówień; mechanizmy wspierające lub wdrażające określanie i wykorzystanie dostosowanych strategii nabywania, narzędzi umownych i metod udzielania zamówień]. |

| | | |
|---|---|---|
| **SR-05(01)** | **STRATEGIE, NARZĘDZIA I METODY NABYCIA \| ODPOWIEDNIE ZAOPATRZENIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-05(01)_ODP[01]** | ***określono zabezpieczenia mające na celu zapewnienie odpowiedniej podaży krytycznych komponentów systemu;*** |
| | **SR-05(01)_ODP[02]** | ***określono krytyczne komponenty systemu, w przypadku których wymagane jest zapewnienie odpowiedniej podaży;*** |
| | **SR-05(01)** | stosuje się ***<zabezpieczenia SR-05(01)_ODP[01]> w*** celu zapewnienia odpowiedniej podaży<br>***<krytycznych elementów systemu SR-05(01)_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-05(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; strategia zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; dokumentacja dotycząca planowania awaryjnego; inwentaryzacja krytycznych systemów i komponentów systemów; określenie odpowiedniej podaży; polityka nabywania systemu i usług; procedury ochrony łańcucha dostaw; procedury dotyczące integracji wymogów bezpieczeństwa informacji z procesem nabywania; procedury dotyczące integracji strategii nabywania, narzędzi umownych i metod udzielania zamówień z procesem nabywania; dokumentacja przetargowa; dokumentacja nabywania; umowy o poziomie usług;<br>umowy nabycia systemów lub usług; zamówienia/zapotrzebowania na zakup systemu, komponentu systemu lub usługi systemowej od dostawców; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| **SR-05(01)** | **STRATEGIE, NARZĘDZIA I METODY NABYCIA \| ODPOWIEDNIE ZAOPATRZENIE** | |
| | **SR-05(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-05(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące określania i wykorzystania dostosowanych strategii nabywania, narzędzi umownych i metod udzielania zamówień; mechanizmy wspierające lub wdrażające określanie i wykorzystanie dostosowanych strategii nabywania, narzędzi umownych i metod udzielania zamówień]. |

| | | |
|---|---|---|
| **SR-05(02)** | **STRATEGIE, NARZĘDZIA I METODY NABYCIA \| OCENY PRZED WYBOREM, AKCEPTACJĄ, MODYFIKACJĄ LUB AKTUALIZACJĄ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-05(02)[01]** | system, komponent systemu lub usługa systemowa są oceniane przed ich wyborem; |
| | **SR-05(02)[02]** | system, komponent systemu lub usługa systemowa są oceniane przed ich akceptacją; |
| | **SR-05(02)[03]** | system, komponent systemu lub usługa systemowa są oceniane przed ich modyfikacją; |
| | **SR-05(02)[04]** | system, komponent systemu lub usługa systemowa są oceniane przed ich aktualizacją; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |

| | | |
|---|---|---|
| **SR-05(02)** | **STRATEGIE, NARZĘDZIA I METODY NABYCIA \| OCENY PRZED WYBOREM, AKCEPTACJĄ, MODYFIKACJĄ LUB AKTUALIZACJĄ** | |
| | **SR-05(02)-Badanie** | [WYBÓR SPOŚRÓD: Plan bezpieczeństwa systemu; polityka integralności systemu i informacji; procedury dotyczące ochrony łańcucha dostaw; procedury dotyczące integracji wymogów bezpieczeństwa informacji z procesem nabywania; wyniki testów i oceny bezpieczeństwa; wyniki oceny podatności; wyniki testów penetracyjnych; wyniki oceny ryzyka w organizacji; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-05(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zakup systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę łańcucha dostaw]. |
| | **SR-05(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przeprowadzania ocen przed wyborem, akceptacją lub aktualizacją systemu, komponentu lub usługi; mechanizmy wspierające lub wdrażające przeprowadzanie ocen przed wyborem, akceptacją lub aktualizacją systemu, komponentu lub usługi]. |

| | | |
|---|---|---|
| **SR-06** | **OCENY I RECENZJE DOSTAWCÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-06_ODP** | ***określono częstotliwość, z jaką należy dokonywać oceny i przeglądu ryzyka związanego z łańcuchem dostaw, dostawcami lub wykonawcami oraz dostarczanymi przez nich systemami, komponentami systemu lub usługami systemowymi;*** |

| | | |
|---|---|---|
| **SR-06** | **OCENY I RECENZJE DOSTAWCÓW** | |
| | **SR-06** | ryzyko związane z łańcuchem dostaw, dostawcami lub wykonawcami oraz dostarczanymi przez nich systemami, komponentami systemu lub usługami systemowymi jest oceniane i przeglądane z ***<częstotliwością SR-06_ODP>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-06-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; strategia zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemu i usług; procedury dotyczące ochrony łańcucha dostaw; procedury dotyczące integracji wymogów bezpieczeństwa informacji z procesem nabywania; zapisy z przeglądów due diligence u dostawców; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-06-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za zakup systemu i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę łańcucha dostaw]. |
| | **SR-06-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące przeprowadzania przeglądów dostawców; mechanizmy wspierające lub wdrażające przeglądy dostawców]. |

| | | |
|---|---|---|
| **SR-06(01)** | **OCENY I RECENZJE DOSTAWCÓW \| BADANIA I ANALIZY** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-06(01)_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {analiza organizacyjna; niezależna analiza zewnętrzna; testy organizacyjne; niezależne testy zewnętrzne};*** |

| | | |
|---|---|---|
| **SR-06(01)** | **OCENY I RECENZJE DOSTAWCÓW \| BADANIA I ANALIZY** | |
| | **SR-06(01)_ODP[02]** | ***określono elementy łańcucha dostaw, procesy i podmioty, które mają być analizowane i testowane;*** |
| | **SR-06(01)** | stosuje się ***<WYBRANA WARTOŚĆ PARAMETRU SR-06(01)_ODP[01]>*** w odniesieniu do ***<elementów, procesów i podmiotów łańcucha dostaw SR-06(01)_ODP[02]>*** związanych z systemem, komponentem systemu lub usługą systemową. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-06(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; procedury dotyczące ochrony łańcucha dostaw; dowody przeprowadzenia analizy organizacyjnej, niezależnej analizy realizowanej przez podmiot trzeci, organizacyjnych testów penetracyjnych lub niezależnych testów penetracyjnych realizowanych przez podmiot trzeci; wykaz elementów, procesów i uczestników łańcucha dostaw (związanych z systemem, komponentem systemu lub usługą systemową) podlegających analizie lub testom; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-06(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw; personel organizacyjny odpowiedzialny za analizę lub testowanie elementów, procesów i uczestników łańcucha dostaw]. |
| | **SR-06(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące określania i stosowania metod analizy/testowania elementów, procesów i uczestników łańcucha dostaw; mechanizmy wspierające lub wdrażające analizę/testowanie elementów, procesów i uczestników łańcucha dostaw]. |

| | | |
|---|---|---|
| **SR-07** | **BEZPIECZEŃSTWO OPERACYJNE W RAMACH ŁAŃCUCHA DOSTAW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-07_ODP** | ***określono zabezpieczenia systemu, komponentu systemu lub usługi systemowej zapewniające bezpieczeństwo operacyjne (OPSEC) w celu ochrony informacji związanych z łańcuchem dostaw;*** |
| | **SR-07** | stosuje się ***<zabezpieczenia OPSEC SR-07_ODP>*** w celu ochrony informacji związanych z łańcuchem dostaw dla systemu, komponentu systemu lub usługi systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-07-Badanie** | [WYBÓR SPOŚRÓD: Plan zarządzania ryzykiem łańcucha dostaw; procedury zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; procedury nabywania systemów i usług; procedury dotyczące ochrony łańcucha dostaw; wykaz stosowanych zabezpieczeń OPSEC;<br>dokumentacja przetargowa; dokumentacja nabycia; umowy nabycia systemu, komponentu systemu lub usługi systemowej; zapisy analiz obejmujących wszystkie źródła informacji; plan bezpieczeństwa systemu; plan ochrony prywatności; inne istotne dokumenty lub zapisy]. |
| | **SR-07-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za pozyskiwanie; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji i ochronę prywatności; personel organizacyjny odpowiedzialny za OPSEC; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-07-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące definiowania i stosowania zabezpieczeń OPSEC; mechanizmy wspierające lub wdrażające definiowanie i stosowanie zabezpieczeń OPSEC]. |

| | | |
|---|---|---|
| **SR-08** | **UMOWY DOTYCZĄCE POWIADOMIEŃ** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-08_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {zawiadomienie o naruszeniach bezpieczeństwa w łańcuchu dostaw; <wyniki oceny lub audytu SR-08_ODP[02]>};*** |
| | **SR-08_ODP[02]** | ***określono informacje, dla których mają zostać ustanowione umowy i procedury (jeśli wybrano);*** |
| | **SR-08** | zawarto umowy i ustanowiono procedury dla ***<WYBRANA WARTOŚĆ PARAMETRU SR-08_ODP[01]>*** z podmiotami uczestniczącymi w łańcuchu dostaw systemu, komponentów systemu lub usługi systemowej. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-08-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; procedury dotyczące ochrony łańcucha dostaw; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; umowy i procedury międzyorganizacyjne; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-08-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-08-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zawierania umów i ustanawiania procedur międzyorganizacyjnych z podmiotami łańcucha dostaw]. |

| | | |
|---|---|---|
| **SR-09** | **ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-09** | dla systemu, komponentu systemu lub usługi systemowej wdrożono program ochrony przed manipulacją. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-09-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; procedury dotyczące ochrony łańcucha dostaw; procedury dotyczące odporności na manipulacje i wykrywania sabotażu; dokumentacja programu ochrony przed manipulacją; dokumentacja narzędzi i technik ochrony przed manipulacją; dokumentacja narzędzi i technik wykrywania sabotażu i odporności na manipulacje; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-09-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za program ochrony przed manipulacją; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-09-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące wdrożenia programu ochrony przed manipulacją; mechanizmy wspierające lub wdrażające program ochrony przed manipulacją]. |

| | | |
|---|---|---|
| **SR-09(01)** | **ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU \| WIELOETAPOWY CYKL ŻYCIA SYSTEMU** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-09(01)** | technologie, narzędzia i techniki ochrony przed manipulacją są stosowane w całym cyklu życia systemu. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-09(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemu i usług; procedury dotyczące odporności na manipulację i wykrywania sabotażu; dokumentacja programu ochrony przed manipulacją; dokumentacja narzędzi i technik ochrony przed manipulacją; dokumentacja narzędzi (technologii) i technik ochrony przed manipulacją; dokumentacja cyklu życia rozwoju systemu; procedury dotyczące ochrony łańcucha dostaw; procedury cyklu życia systemu; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; umowy i procedury międzyorganizacyjne; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-09(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw; personel organizacyjny odpowiedzialny za proces SDLC]. |
| | **SR-09(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące stosowania technologii ochrony przed manipulacją; mechanizmy wspierające lub wdrażające technologie ochrony przed manipulacją]. |

| | | |
|---|---|---|
| **SR-10** | **KONTROLA SYSTEMÓW/KOMPONENTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-10_ODP[01]** | ***określono systemy lub komponenty systemu, które wymagają kontroli;*** |
| | **SR-10_ODP[02]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {losowo; z <częstotliwością SR-10_ODP[03]>; po wystąpieniu <wskazań do przeprowadzenia kontroli SR-10_ODP[04]>};*** |
| | **SR-10_ODP[03]** | ***określono częstotliwość kontroli systemów lub komponentów systemu (jeżeli wybrano);*** |
| | **SR-10_ODP[04]** | ***określono wskazania do przeprowadzenia kontroli systemów lub komponentów systemu (jeśli wybrano);*** |
| | **SR-10** | ***<systemy lub komponenty systemu SR-10_ODP[01]>*** są kontrolowane ***<WYBRANA WARTOŚĆ PARAMETRU SR-10_ODP[02]>*** w celu wykrywania manipulacji. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-10-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; zapisy dotyczące kontroli losowych; sprawozdania/wyniki z kontroli; sprawozdania/wyniki z oceny; dokumentacja dotycząca nabycia; umowy o poziomie usług; umowy nabycia systemu, komponentu systemu lub usługi systemowej; umowy i procedury międzyorganizacyjne; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-10-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |

| | | |
|---|---|---|
| **SR-10** | **KONTROLA SYSTEMÓW/KOMPONENTÓW** | |
| | **SR-10-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zawierania umów i ustanawiania procedur międzyorganizacyjnych z podmiotami łańcucha dostaw; procesy organizacyjne dotyczące kontroli pod kątem manipulacji]. |

| | | |
|---|---|---|
| **SR-11** | **AUTENTYCZNOŚĆ KOMPONENTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-11_ODP[01]** | ***wybrano co najmniej jedną z następujących WARTOŚCI PARAMETRÓW: {źródło podrobionego elementu; <zewnętrzne organizacje sprawozdawcze SR-11_ODP[02]>;***<br>***<personel lub role SR-11_ODP[03]>;*** |
| | **SR-11_ODP[02]** | ***określono zewnętrzne organizacje sprawozdawcze, do których należy zgłaszać podrobione komponenty systemu (jeśli wybrano);*** |
| | **SR-11_ODP[03]** | ***określono personel lub role, do których należy zgłaszać podrobione komponenty systemu (jeśli wybrano);*** |
| | **SR-11a.[01]** | opracowano i wdrożono politykę przeciwdziałania fałszerstwom; |
| | **SR-11a.[02]** | opracowano i wdrożono procedury przeciwdziałania fałszerstwom; |
| | **SR-11a.[03]** | procedury przeciwdziałania fałszerstwom obejmują środki do wykrywania podrobionych komponentów wprowadzanych do systemu; |
| | **SR-11a.[04]** | procedury przeciwdziałania fałszerstwom obejmują środki zapobiegające wprowadzaniu do systemu podrobionych komponentów; |
| | **SR-11b.** | Podrobione komponenty systemu są zgłaszane do ***<WYBRANA WARTOŚĆ PARAMETRU SR-11_ODP[01]>***. |

| | | |
|---|---|---|
| **SR-11** | **AUTENTYCZNOŚĆ KOMPONENTÓW** | |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-11-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; plan przeciwdziałania fałszerstwom; polityka i procedury przeciwdziałania fałszerstwom; polityka utylizacji nośników; polityka ochrony nośników; polityka reagowania na incydenty; raporty powiadamiające programistów, producentów, sprzedawców, wykonawców lub zewnętrzne organizacje sprawozdawcze o podrobionych komponentach systemu; dokumentacja nabywania; umowy o poziomie usług;<br><br>umowy nabycia systemu, komponentu systemu lub usługi systemowej; umowy i procedury międzyorganizacyjne; zapisy dotyczące zgłoszonych podrobionych komponentów systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-11-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw; personel organizacyjny odpowiedzialny za politykę, procedury i sprawozdawczość w zakresie przeciwdziałania fałszerstwom]. |
| | **SR-11-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zapobiegania, wykrywania i zgłaszania fałszerstw; mechanizmy wspierające lub wdrażające wykrywanie, zapobieganie i zgłaszanie fałszerstw]. |

| | | |
|---|---|---|
| **SR-11(01)** | **AUTENTYCZNOŚĆ KOMPONENTU \| SZKOLENIE Z ZAKRESU ZAPOBIEGANIA FAŁSZERSTWOM** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-11(01)_ODP** | ***określono personel lub role wymagające szkolenia w zakresie wykrywania podrobionych komponentów systemu (w tym sprzętu, oprogramowania i oprogramowania układowego);*** |
| | **SR-11(01)** | ***<personel lub role SR-11(01)_ODP>*** są przeszkolone w zakresie wykrywania podrobionych komponentów systemu (w tym sprzętu, oprogramowania i oprogramowania układowego). |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-11(01)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka nabywania systemów i usług; plan przeciwdziałania fałszerstwom; polityka i procedury przeciwdziałania fałszerstwom; polityka utylizacji nośników; polityka ochrony nośników; polityka reagowania na incydenty; materiały szkoleniowe dotyczące podrabianych komponentów systemu; dokumentacja szkoleniowa dotycząca wykrywania i zapobiegania wprowadzaniu podrabianych komponentów do systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-11(01)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem w łańcuchu dostaw; personel organizacyjny odpowiedzialny za politykę, procedury i sprawozdawczość w zakresie przeciwdziałania fałszerstwom]. |
| | **SR-11(01)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące szkoleń w zakresie przeciwdziałania fałszerstwom]. |

| | | |
|---|---|---|
| **SR-11(02)** | **AUTENTYCZNOŚĆ KOMPONENTU \| ZABEZPIECZENIE KONFIGURACJI SERWISOWANYCH I NAPRAWIANYCH KOMPONENTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-11(02)_ODP** | ***określono komponenty systemu wymagające zabezpieczenia konfiguracji;*** |
| | **SR-11(02)[01]** | zachowana jest kontrola nad konfiguracją ***<komponentów systemu SR-11(02)_ODP>*** oczekujących na serwis lub naprawę; |
| | **SR-11(02)[02]** | zachowana jest kontrola nad konfiguracją ***<komponentów systemu SR-11(02)_ODP>*** oczekujących na ponowne wdrożenie do eksploatacji; |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-11(02)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; procedury zabezpieczania konfiguracji; dokumentacja nabycia; umowy o poziomie usług; umowy nabycia komponentu systemu;<br>umowy i procedury międzyorganizacyjne; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-11(02)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw]. |
| | **SR-11(02)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące zawierania umów i ustanawiania procedur międzyorganizacyjnych z podmiotami łańcucha dostaw; procesy zabezpieczania konfiguracji w organizacji]. |

| | | |
|---|---|---|
| **SR-11(03)** | **AUTENTYCZNOŚĆ KOMPONENTU \| SKANOWANIE ANTYFAŁSZERSKIE** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-11(03)_ODP** | ***określono częstotliwość skanowania w poszukiwaniu podrobionych komponentów systemu;*** |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-11(03)-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; polityka i procedury przeciwdziałania fałszerstwom; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; narzędzia skanujące i związana z nimi dokumentacja; wyniki skanowania; procedury dotyczące ochrony łańcucha dostaw; dokumentacja dotycząca nabywania; umowy i procedury międzyorganizacyjne; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-11(03)-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za nabywanie systemów i usług; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za zarządzanie ryzykiem łańcucha dostaw; personel organizacyjny odpowiedzialny za politykę i procedury przeciwdziałania fałszerstwom; personel organizacyjny odpowiedzialny za skanowanie w celu wykrywania fałszerstw]. |
| | **SR-11(03)-Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące skanowania w poszukiwaniu fałszywych komponentów systemu; mechanizmy wspierające lub wdrażające skanowanie w celu wykrywania fałszerstw]. |

| | | |
|---|---|---|
| **SR-12** | **USUWANIE KOMPONENTÓW** | |
| | **CEL OCENY:**<br>*Ustalenie, czy:* | |
| | **SR-12_ODP[01]** | ***określono dane, dokumentację, narzędzia lub komponenty systemu, które mają być poddawane utylizacji;*** |
| | **SR-12_ODP[02]** | ***określono techniki i metody utylizacji danych, dokumentacji, narzędzi lub komponentów systemu;*** |
| | **SR-12** | ***<dane, dokumentacja, narzędzia lub komponenty systemu SR-12_ODP[01]>*** są usuwane przy użyciu ***<technik i metod SR-12_ODP[02]>***. |
| | **POTENCJALNE METODY I PRZEDMIOTY OCENY:** | |
| | **SR-12-Badanie** | [WYBÓR SPOŚRÓD: Polityka i procedury zarządzania ryzykiem łańcucha dostaw; plan zarządzania ryzykiem łańcucha dostaw; procedury utylizacji związane z ochroną łańcucha dostaw; polityka utylizacji nośników; polityka ochrony nośników; dokumentacja dotycząca utylizacji komponentów systemu; dokumentacja dotycząca komponentów systemu zidentyfikowanych do utylizacji; dokumentacja dotycząca technik i metod utylizacji stosowanych w odniesieniu do komponentów systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **SR-12-Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacyjny odpowiedzialny za usuwanie komponentów systemu; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; personel organizacyjny odpowiedzialny za ochronę łańcucha dostaw]. |
| | **SR-12-Test** | [WYBÓR SPOŚRÓD: Organizacyjne techniki i metody utylizacji komponentów systemu; mechanizmy wspomagające i/lub wdrażające utylizację komponentów systemu]. |