Ministerstwo Cyfryzacji

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

**Część 1**

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.

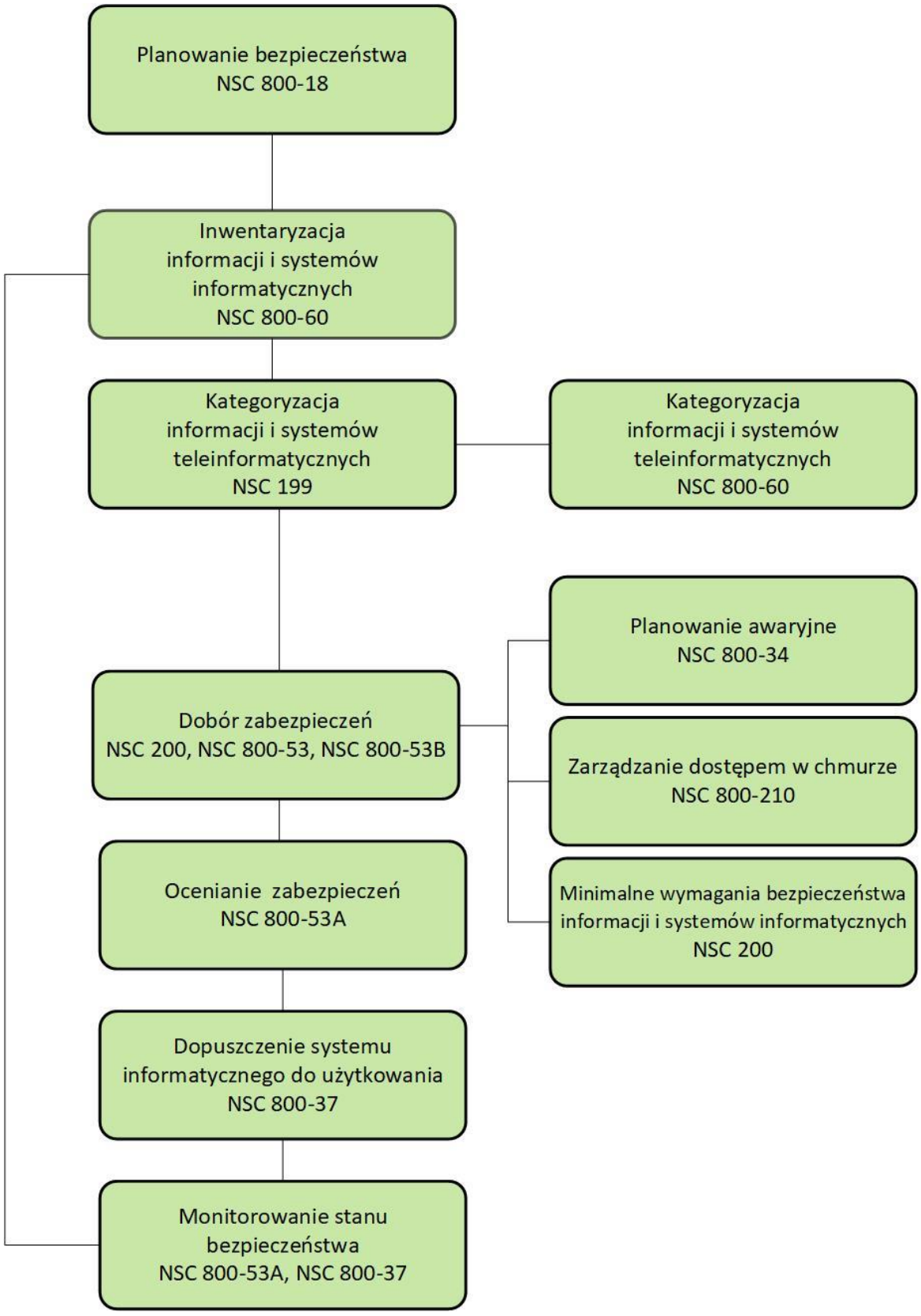
Zestaw publikacji specjalnych obejmuje następujące pozycje:

- 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.

## Abstrakt

Niniejsza publikacja zawiera metodologię i zestaw procedur do przeprowadzania oceny środków bezpieczeństwa i ochrony prywatności stosowanych w systemach i organizacjach w ramach skutecznego zarządzania ryzykiem. Procedury oceny, przeprowadzane na różnych etapach cyklu życia systemu, są zgodne ze środkami bezpieczeństwa i zabezpieczeniami prywatności zawartymi w publikacji NSC 800-53, wersja 2[2]. Rozwiązania te można łatwo dostosować do potrzeb organizacji, aby zapewnić jej niezbędną elastyczność w przeprowadzaniu ocen środków bezpieczeństwa i zabezpieczeń prywatności, które wspierają procesy zarządzania ryzykiem organizacyjnym i są zgodne z określoną tolerancją ryzyka organizacji. Podane zostały również informacje na temat tworzenia skutecznych planów oceny środków bezpieczeństwa i ochrony prywatności oraz wskazówki dotyczące analizy wyników oceny.

## Słowa kluczowe

Ocena (*ang. assessment*); plan oceny (*ang. assessment plan*); zapewnienie (*ang. assurance*); ocenianie zabezpieczeń (*ang. control assessment*); zabezpieczenia prywatności (*ang. privacy controls*); Open Security Controls Assessment Language (OSCAL); wymagania dotyczące prywatności (*ang. privacy requirements*); Ramy Zarządzania Ryzykiem (*ang. ; Risk Management Framework*); środki bezpieczeństwa/zabezpieczenia (*ang. security controls*); wymagania w zakresie bezpieczeństwa (*ang. security requirements*).

[2] Rekomendacje te zostały opracowana na podstawie publikacji specjalnej NIST SP 800-53 rev. 5.

## Konwencje stosowane w niniejszym dokumencie

Dla celów niniejszego dokumentu termin „bezpieczeństwo i prywatność" jest używany powszechnie, ponieważ wytyczne mają zastosowanie zarówno do oceny środków bezpieczeństwa, jak i zabezpieczeń prywatności. W przypadku niektórych systemów wytyczne mogą być jednak istotne tylko w odniesieniu do ***bezpieczeństwa lub prywatności***. Organizacje same decydują o tym, czy oceny środków bezpieczeństwa i zabezpieczeń prywatności powinny być przeprowadzane razem czy osobno.

Publikacja NSC 800-53A zawiera wskazówki dotyczące oceny zabezpieczeń ujętych w planach programów bezpieczeństwa informacji, planach programów ochrony prywatności, planach bezpieczeństwa systemów i planach ochrony prywatności. Tam, gdzie w wytycznych jest mowa o wszystkich wymienionych wyżej planach, używa się terminu „plany bezpieczeństwa i ochrony prywatności". Jeśli wytyczne odnoszą się do konkretnego rodzaju planu (np. planu bezpieczeństwa systemu), wówczas wyszczególniony jest dany rodzaj planu.

**FORMATOWANIE PROCEDURY OCENY**

Nowy format procedur oceny, wprowadzony w publikacji NSC 800-53A wer. 1[3] został udoskonalony w niniejszej publikacji (NSC 800-53A, wer. 2). Format nadal odzwierciedla dekompozycję celów oceny na bardziej *szczegółowe* oświadczenia stwierdzające, tam, gdzie jest to możliwe, zapewniając w ten sposób możliwość identyfikacji i oceny poszczególnych składowych środków bezpieczeństwa i ochrony prywatności.

Uaktualnienia dokumentu NSC 800-53A wer. 2 (w stosunku do NSC 800-53A wer. 1):

- W pierwszej kolejności i niezależnie od oświadczeń o dokonaniu ustaleń dla każdego elementu zabezpieczenia powinno nastąpić zidentyfikowanie oświadczenia o ustaleniu wartości parametrów zabezpieczeń zdefiniowanych przez organizację (*ang. organization-defined parameters - ODP*).
- Poprawa czytelności procedur oceny.
- Zapewnienie ustrukturyzowanego schematu dla zautomatyzowanych narzędzi, gdy informacje o ocenie są wprowadzane do takich narzędzi;
- Zapewnienie większej elastyczności w przeprowadzaniu ocen poprzez umożliwienie organizacjom skupienia się na określonych aspektach zabezpieczeń (podkreślenie poszczególnych wad i/lub braków w zabezpieczeniach).
- Poprawa skuteczności ocen środków bezpieczeństwa i ochrony prywatności.
- Wspieranie ciągłego monitorowania i programów bieżącej autoryzacji poprzez zapewnienie większej liczby części składowych środków bezpieczeństwa i ochrony prywatności, które mogą być poddawane ocenie z określoną przez organizację częstotliwością i stopniem rygorystyczności.

[3] Rekomendacje te zostały opracowana na podstawie publikacji specjalnej NIST SP 800-53A rev. 4.

Możliwość wykorzystania zasobów do oceny i monitorowania w sposób ukierunkowany i precyzyjny oraz jednoczesne maksymalne wykorzystanie technologii automatyzacji może skutkować tym, że procesy oceny będą przebiegały szybciej i bardziej ekonomicznie dla organizacji.

**Uwaga:** Standard NSC 800-53 zostanie odpowiednio zaktualizowany, aby zapewnić zgodność numeracji wszystkich środków bezpieczeństwa i ochrony prywatności z nowym formatem wprowadzonym w niniejszej publikacji.

## Streszczenie

Ocenianie środków bezpieczeństwa i zabezpieczeń prywatności nie sprowadza się do sporządzenia list kontrolnych, uzyskania prostego wyniku „zaliczenia/niezaliczenia" czy opracowania dokumentacji w celu przejścia inspekcji lub audytu. Ocenianie zabezpieczeń jest głównym narzędziem weryfikacji, czy wybrane środki bezpieczeństwa i zabezpieczenia prywatności zostały wdrożone oraz czy spełniają założone cele i zadania. Publikacja NSC 800-53A, ułatwia ocenianie środków bezpieczeństwa i zabezpieczeń prywatności przeprowadzane w ramach skutecznego zarządzania ryzykiem. Głównym celem projektowym NSC 800-53A jest zapewnienie ram oceny i wstępnego punktu wyjścia dla procedur oceny, które są wystarczająco elastyczne, aby sprostać potrzebom różnych organizacji, zapewniając jednocześnie spójność w przeprowadzaniu ocen zabezpieczeń. Wyniki oceny zabezpieczeń dostarczają osobom odpowiedzialnym za organizację:

- potwierdzenie skuteczności wdrożonych zabezpieczeń,
- informacje o jakości procesów zarządzania ryzykiem,
- informacje o mocnych i słabych stronach systemów wspierających misje organizacji i funkcje biznesowe w zakresie bezpieczeństwa i prywatności.

Ustalenia poczynione przez oceniających są wykorzystywane do określenia ogólnej skuteczności środków bezpieczeństwa i zabezpieczeń prywatności związanych z systemami i ich środowiskami pracy oraz do zapewnienia wiarygodnego i znaczącego wkładu w proces zarządzania ryzykiem w organizacji. Prawidłowo przeprowadzona ocena pomaga określić zasadność zabezpieczeń zawartych w planach bezpieczeństwa i ochrony prywatności organizacji, a następnie zastosowanych w systemach i środowiskach pracy organizacji. Oceny zabezpieczeń gwarantują ekonomiczne podejście do zarządzania ryzykiem poprzez identyfikację podatności lub braków w systemach, co pozwala organizacji w skoordynowany sposób określić odpowiednie reakcje na ryzyko, zgodne z jej misją i potrzebami biznesowymi.

NSC 800-53A jest rekomendacją uzupełniającą do standardu [NSC 800-53]. Każda z publikacji zawiera wytyczne dotyczące wdrażania poszczególnych kroków w ramach zarządzania ryzykiem (*ang. Risk Management Framework - RMF*) [4]. Rekomendacje NSC 800-53 oraz [NSC 800-53B][5] odnoszą się do etapu *Wyboru* w RMF i zawierają wytyczne dotyczące wyboru środków bezpieczeństwa i zabezpieczeń prywatności (tj. określenia zabezpieczeń niezbędnych do zarządzania ryzykiem dla operacji i aktywów organizacji, osób, innych organizacji i państwa). NSC 800-53A omawia etapy *Oceny* i *Monitorowania* w ramach zarządzania ryzykiem RMF i dostarcza wskazówek na temat procesów oceny środków bezpieczeństwa i zabezpieczeń prywatności. NSC 800-53A zawiera również wytyczne dotyczące tego, jak tworzyć efektywne plany oceny oraz jak analizować i zarządzać wynikami oceny.

NSC 800-53A określa proces, który pozwoli organizacjom na dostosowanie procedur oceny przedstawionych w niniejszych wytycznych. Dostosowywanie polega na indywidualizacji procedur oceny w celu lepszego dopasowania ich do charakterystyki systemu i środowiska eksploatacji. Proces dostosowywania opisany w niniejszych wytycznych daje organizacjom elastyczność potrzebną do uniknięcia zastosowania metod oceny, które są niepotrzebnie skomplikowane lub kosztowne, przy jednoczesnym spełnieniu wymagań dotyczących oceny i zasad zarządzania ryzykiem określonych w ramach zarządzania ryzykiem. Decyzje dotyczące dostosowywania podejmowane są według uznania danej organizacji, aby zmaksymalizować elastyczność w tworzeniu planów oceny - na podstawie wyników oceny ryzyka określa się zakres, rygor i poziom szczegółowości ocen potrzebnych do uzyskania wystarczającej wiarygodności co do stanu bezpieczeństwa i ochrony prywatności systemu.

[4] Publikacja [NSC 800-37], zawiera rekomendacje w zakresie zastosowania ram zarządzania ryzykiem do systemów i organizacji.

[5] Publikacja ta została opracowana na podstawie publikacji specjalnej NIST SP 800-53B.

# Spis treści

## Spis ilustracji



## Spis tabel

## ROZDZIAŁ PIERWSZY

# 1. WPROWADZENIE

### KONIECZNOŚĆ OCENY EFEKTYWNOŚCI ŚRODKÓW BEZPIECZEŃSTWA I ZABEZPIECZEŃ PRYWATNOŚCI

Współczesne systemy[6] to złożone zespoły rozwiązań technologicznych (tj. sprzętu, oprogramowania użytkowego i oprogramowania układowego), procesów i ludzi współpracujących ze sobą w celu zapewnienia organizacjom możliwości przetwarzania, przechowywania i przekazywania informacji w odpowiednim czasie, w celu wsparcia różnych misji i funkcji biznesowych. Stopień, w jakim organizacje uzależniły się od systemów przy wykonywaniu rutynowych, ważnych i krytycznych zadań i funkcji biznesowych oznacza, że ochrona podstawowych systemów i środowisk pracy ma pierwszoplanowe znaczenie dla powodzenia misji organizacji. Wybór odpowiednich środków bezpieczeństwa i zabezpieczeń prywatności dla danego systemu jest ważnym zadaniem, które może mieć istotny wpływ na działalność i majątek organizacji, a także na dobro osób fizycznych. Środki bezpieczeństwa to zabezpieczenia lub środki zaradcze stosowane w ramach systemu lub organizacji w celu ochrony poufności, integralności i dostępności systemu i jego informacji oraz w celu zarządzania ryzykiem bezpieczeństwa informacji. Zabezpieczenia prywatności to administracyjne, techniczne i fizyczne zabezpieczenia stosowane w systemie lub organizacji w celu zarządzania ryzykiem utraty prywatności i zapewnienia zgodności z obowiązującymi wymaganiami dotyczącymi ochrony prywatności.[7]

Po zastosowaniu w systemie, środki bezpieczeństwa i zabezpieczenia prywatności są oceniane w celu określenia ich ogólnej skuteczności (tzn. zakresu w jakim zabezpieczenia te zostały prawidłowo wdrożone, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w odniesieniu do spełnienia wymagań dotyczących

[6] Patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.*

[7] NSC 7298 zawiera definicje środków bezpieczeństwa i zabezpieczeń prywatności.

bezpieczeństwa i ochrony prywatności dla systemu i organizacji). Zrozumienie ogólnej skuteczności wdrożonych środków bezpieczeństwa i zabezpieczeń prywatności jest niezbędne do określenia ryzyka dla działań organizacji, jej aktywów, osób, innych organizacji i państwa, wynikającego z korzystania z systemu.

## 1.1. CEL I ZASTOSOWANIE

Niniejsza publikacja ma na celu przedstawienie rekomendacji pozwalających na tworzenie skutecznych planów oceny środków bezpieczeństwa i ochrony prywatności, a także kompleksowego zestawu procedur oceny skuteczności środków bezpieczeństwa i zabezpieczeń prywatności stosowanych w systemach i organizacjach. Wytyczne mają zastosowanie do środków bezpieczeństwa i zabezpieczeń prywatności określonych w standardzie [NSC 800-53] (z późniejszymi zmianami). Wytyczne zostały opracowane, aby ułatwić osiągnięcie większego bezpieczeństwa systemów poprzez:

- Umożliwienie przeprowadzania bardziej spójnych, skutecznych, porównywalnych i powtarzalnych ocen środków bezpieczeństwa i zabezpieczeń prywatności dających odtwarzalne wyniki.
- Promowanie lepszego zrozumienia zagrożeń dla działań organizacji, majątku organizacji, osób, innych organizacji i państwa, wynikających z pracy i użytkowania systemów.
- Ułatwianie przeprowadzania bardziej ekonomicznych ocen środków bezpieczeństwa i zabezpieczeń prywatności.
- Zapewnienie bardziej kompletnych, wiarygodnych i rzetelnych informacji dla pracowników organizacji w celu wsparcia podejmowania decyzji dotyczących zarządzania ryzykiem, wzajemności wyników oceny, wymiany informacji oraz zgodności z przepisami, rozporządzeniami wykonawczymi, dyrektywami, standardami i zasadami.

Niniejsza publikacja spełnia wymagania zawarte w uchwale A-130 [OMB A-130] Urzędu ds. Administracji i Budżetu (*ang.* Office of Management and Budget -

OMB) oraz w ustawie [FISMA][8]. Wytyczne dotyczące bezpieczeństwa i ochrony prywatności zawarte w niniejszej publikacji mają zastosowanie do systemów innych niż systemy określone jako systemy bezpieczeństwa narodowego, zgodnie z definicją zawartą w dziale 44 Kodeksu Stanów Zjednoczonych (U.S.C.), sekcja 3542[9]. Rekomendacje te zostały przygotowane jako uzupełnienie podobnych wytycznych dla systemów bezpieczeństwa narodowego pod kątem technicznym i mogą być stosowane w takich systemach za zgodą odpowiednich władz państwowych odpowiedzialnych za takie systemy. [10]

Organizacje powinny korzystać z niniejszej publikacji w połączeniu z zatwierdzonymi planami programów bezpieczeństwa informacji, planami programów ochrony prywatności, planami bezpieczeństwa systemu i planami ochrony prywatności przy opracowywaniu planów oceny służących do tworzenia i gromadzenia informacji niezbędnych do określenia skuteczności środków bezpieczeństwa i zabezpieczeń prywatności stosowanych w systemie i organizacji.

Rekomendacje zawarte w niniejszej publikacji zostały opracowane z myślą o umożliwieniu organizacjom dostosowania podstawowych procedur oceny do ich potrzeb. Procedury oceny są wykorzystywane jako punkt wyjścia dla planu oceny oraz jako jego uzupełnienie. Opracowując skuteczne plany oceny bezpieczeństwa i ochrony prywatności, organizacje powinny wziąć pod uwagę istniejące informacje o zabezpieczeniach, które mają zostać poddane ocenie (np.

[8] Przywołane dokumenty obowiązują w USA i nie znajdują bezpośredniego zastosowania w polskim ustawodawstwie. Podane zostały informacyjnie oraz w celu poszerzenia wiedzy.

[9] Tamże.

[10] Informacyjnie - zgodnie z postanowieniami [FISMA] i zasadami OMB, w każdym przypadku, gdy połączenie systemów federalnych z systemami obsługiwanymi przez rządy stanowe / lokalne / społecznościowe, wykonawców lub podmioty upoważnione, wiąże się z przetwarzaniem, przechowywaniem lub przekazywaniem informacji federalnych, zastosowanie mają standardy i wytyczne dotyczące bezpieczeństwa informacji opisane w niniejszej publikacji. Szczegółowe wymagania dotyczące bezpieczeństwa informacji oraz warunki połączeń między systemami są wyrażone w protokołach uzgodnień (*ang. Memorandum of Understanding - MOU*) i umowach o bezpiecznym połączeniu systemów (*ang. Interconnection Security Agreement - ISA*) sporządzanych przez organizacje uczestniczące. Dodatkowe wytyczne dotyczące zarządzania bezpieczeństwem wymiany informacji można znaleźć w dokumencie NIST [SP 800-47], wersja 1, *Managing the Security of Information Exchanges.*

wyniki oceny ryzyka; specyficzne dla danej platformy zależności w sprzęcie, oprogramowaniu użytkowym lub sprzętowym; oraz wszelkie procedury oceny wynikające z zastosowania zabezpieczeń specyficznych dla danej organizacji, które nie zostały uwzględnione w [NSC 800-53]).[11]

Wybór odpowiednich procedur oceny oraz rygorystyczność, intensywność i zakres oceny zależą od następujących czynników:

- Kategoryzacji systemu pod względem bezpieczeństwa. [12]
- Oceny ryzyka utraty prywatności dla danego systemu.
- Środków bezpieczeństwa i zabezpieczeń prywatności wymienionych w [NSC 800-53], zgodnie z zatwierdzonymi planami programu bezpieczeństwa informacji, planami programu ochrony prywatności, planami bezpieczeństwa i ochrony prywatności.[13]
- Wymagań dotyczących wiarygodności, które organizacja zamierza spełnić przy określaniu ogólnej skuteczności środków bezpieczeństwa i ochrony prywatności.

Proces oceny jest działaniem polegającym na zbieraniu informacji o aktualnym stanie systemu lub zabezpieczeniach wspólnych, a nie działaniem związanym z zapewnieniem bezpieczeństwa lub ochrony prywatności. Organizacje określają najbardziej opłacalny sposób wdrożenia procesu oceny poprzez zastosowanie

[11] Na przykład, aby odpowiednio ocenić określone cechy danego środka bezpieczeństwa lub zabezpieczenia prywatności, konieczne może być opracowanie szczegółowych skryptów testowych dla konkretnego systemu operacyjnego, komponentu sieciowego, oprogramowania pośredniczącego lub aplikacji zastosowanej w systemie. Takie skrypty testowe charakteryzują się niższym poziomem szczegółowości niż procedury oceny zawarte w niniejszych wytycznych i dlatego wykraczają poza zakres niniejszej publikacji.

[12] W przypadku systemów bezpieczeństwa narodowego kategoryzacja jest dokonywana zgodnie z wytycznymi odpowiednich organów . W przypadku systemów innych niż systemy bezpieczeństwa narodowego, kategoryzacja jest przeprowadzana zgodnie z rekomendacjami [NSC 199], [NSC 800-37], [NSC 800-60 część 1 i 2] oraz Rejestrem Nadzorowanych Informacji Jawnych (*ang. Controlled Unclassified Information Registry - CUI*) [NARA CUI] prowadzonym przez Krajową Administrację Archiwów i Rejestrów (*ang. National Archives and Records Administration*).

[13] Środki bezpieczeństwa i zabezpieczeń prywatności dla systemu i organizacji zostają udokumentowane w planach bezpieczeństwa systemu i planach ochrony prywatności, po wstępnym wyborze i dostosowaniu zabezpieczeń zgodnie z [NSC 800-53]. Zabezpieczenia zarządzania programem są udokumentowane w planach programów bezpieczeństwa informacji i planach programów ochrony prywatności, zgodnie z opisem zawartym w NSC 800-53.

wyników oceny ryzyka, uwzględnienie dojrzałości i poziomu jakości procesów zarządzania ryzykiem w organizacji oraz skorzystanie z elastyczności koncepcji opisanych w niniejszej publikacji. Wykorzystanie NSC 800-53A jako punktu wyjścia w procesie definiowania procedur oceny środków bezpieczeństwa i zabezpieczeń prywatności w systemach i organizacjach promuje spójne stosowanie środków bezpieczeństwa i zabezpieczeń prywatności oraz zapewnia niezbędną elastyczność w dostosowywaniu oceny w oparciu o zasady i wymagania organizacyjne, znane informacje o zagrożeniach i podatnościach, względy operacyjne, zależności między systemami i platformami oraz tolerancję na ryzyko.[14] Informacje uzyskane podczas oceny zabezpieczeń mogą być wykorzystane przez organizację do:

- Określenia potencjalnych problemów lub niedociągnięć związanych z wdrażaniem przez organizację ram zarządzania ryzykiem.
- Określenia wad i braków związanych z bezpieczeństwem i ochroną prywatności w systemie i w środowisku, w którym system funkcjonuje.
- Ustalenia priorytetów decyzji dotyczących reakcji na ryzyko i związanych z nimi działań[15].
- Potwierdzenia, że zidentyfikowane wady i braki związane z bezpieczeństwem i ochroną prywatności w systemie i w środowisku eksploatacji zostały usunięte.
- Wspierania działań monitorujących oraz świadomości sytuacyjnej w zakresie bezpieczeństwa informacji i ochrony prywatności.
- Ułatwienia podejmowania wszelkiego rodzaju decyzji związanych z autoryzacją systemu.[16] oraz
- Informowania o decyzjach budżetowych i procesie inwestycji kapitałowych.

[14] W niniejszej publikacji termin „ryzyko" odnosi się do zagrożeń dla działalności organizacji (tj. misji, funkcji, wizerunku i reputacji), majątku organizacji, osób, innych organizacji oraz państwa.

[15] [NSC 800-39] zawiera dodatkowe informacje na temat rodzajów reakcji na ryzyko.

[16] Rodzaje decyzji autoryzacyjnych zostały opisane w dokumencie [NSC 800-37], załącznik F.

Nie oczekuje się, że organizacje będą stosować wszystkie metody oceny i obiekty oceny zawarte w procedurach oceny określonych w niniejszej publikacji w odniesieniu do powiązanych środków bezpieczeństwa i zabezpieczeń prywatności wdrożonych w systemach organizacyjnych lub dostępnych do dziedziczenia przez te systemy. Zamiast tego, organizacje mają swobodę w ustalaniu wymaganego poziomu wysiłku i wiarygodności dla danej oceny (np. jakie metody oceny i cele oceny są najbardziej przydatne do uzyskania pożądanych wyników). Poziom wysiłku i wymagana wiarygodność są określane na podstawie czynników niezbędnych do osiągnięcia celów oceny w najbardziej opłacalny sposób i przy zachowaniu wystarczającej pewności, która pozwoli na późniejsze określenie ryzyka związanego z misją lub działalnością (tj. zarządzanie ryzykiem). Organizacje muszą zachować równowagę między zasobami przeznaczonymi na wdrażanie środków bezpieczeństwa i zabezpieczeń prywatności (tj. zabezpieczeń i środków zaradczych wdrożonych w celu ochrony bezpieczeństwa i prywatności) a zasobami przeznaczonymi na określenie ogólnej skuteczności zabezpieczeń, zarówno na etapie początkowym, jak i na bieżąco poprzez realizację programów ciągłego monitorowania.

## 1.2. DOCELOWI ODBIORCY

Niniejsza publikacja ma na celu służyć zróżnicowanej grupie specjalistów ds. bezpieczeństwa systemów i informacji oraz ochrony prywatności. Między innymi są to:

- Osoby odpowiedzialne za rozwój systemów (np. menadżerowie programów, projektanci i programiści systemów, integratorzy systemów, inżynierowie bezpieczeństwa informacji oraz inżynierowie ochrony prywatności).
- Osoby odpowiedzialne za ocenę i monitorowanie bezpieczeństwa i ochrony prywatności informacji (np. osoby oceniające system, osoby oceniające zabezpieczenia, niezależni weryfikatorzy, walidatorzy, analitycy, właściciele systemów, dostawcy zabezpieczeń wspólnych).
- Osoby odpowiedzialne za system, bezpieczeństwo informacji, ochronę prywatności lub zarządzanie ryzykiem i nadzór (np. osoby autoryzujące, CIO,

SISO,[17] SAOP/CPO, menadżerowie systemu, kierownicy bezpieczeństwa informacji i ochrony prywatności) [18].

- Osoby odpowiedzialne za bezpieczeństwo i ochronę prywatności informacji oraz działania operacyjne (np. właściciele systemów, dostawcy zabezpieczeń wspólnych, właściciele lub władający informacją, właściciele misji lub firm, administratorzy systemów, SSO, SPO).[19]

## 1.3. POWIĄZANE PUBLIKACJE I PROCESY OCENY

NSC 800-53A ma na celu wsparcie dokumentu [NSC 800-37], *Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu.* Procedury oceny zawarte w niniejszej publikacji oraz wytyczne dotyczące tworzenia planów oceny bezpieczeństwa i ochrony prywatności systemów organizacyjnych bezpośrednio wspierają działania związane z oceną i monitorowaniem, które są integralną częścią procesu zarządzania ryzykiem. Działania integralne obejmują dostarczanie pracownikom organizacji w czasie zbliżonym do rzeczywistego informacji związanych z bezpieczeństwem i ochroną prywatności, dotyczących aktualnego stanu bezpieczeństwa i ochrony prywatności w ich systemach i organizacjach.

Zaleca się organizacjom korzystanie z wyników oceny zabezpieczeń i związanej z nią dokumentacji, artefaktów i dowodów dostępnych dla komponentów systemu z wcześniej przeprowadzonych ocen, w tym z niezależnych testów, oceny i walidacji przeprowadzonych przez strony trzecie.[20] Testowanie, ocena i walidacja

[17] Na poziomie *podmiotu* funkcję tę pełni Senior Agency Information Security Officer (SAISO). Organizacje mogą również określać tę rolę jako *Senior Information Security Officer* lub *Chief Information Security Officer*.

[18] Definicje ról: patrz NSC 800-18; NSC 800-37, NSC 7298.

[19] Tamże.

[20] Wyniki oceny mogą pochodzić z wielu działań, wykonywanych rutynowo podczas cyklu życia systemu. Na przykład wyniki oceny są opracowywane podczas testowania i oceny nowych elementów systemu w trakcie modernizacji systemu lub działań związanych z jego integracją. Organizacje mogą w miarę możliwości korzystać z wyników wcześniejszych ocen, aby obniżyć ogólny koszt związany z przeprowadzeniem ocen i zwiększyć efektywność procesu oceny.

produktu mogą być przeprowadzane z wykorzystaniem standardów krajowych i międzynarodowych na modułach kryptograficznych i produktach informatycznych ogólnego przeznaczenia, takich jak systemy operacyjne, systemy baz danych, zapory ogniowe, systemy wykrywania włamań, przeglądarki internetowe, aplikacje internetowe, karty inteligentne, urządzenia biometryczne, urządzenia do weryfikacji tożsamości osobistej, urządzenia sieciowe i platformy sprzętowe. Jeżeli produkt będący składnikiem systemu jest określony w [NSC 800-53] jako zapewniający wsparcie dla wdrożenia konkretnego zabezpieczenia, to dowody uzyskane w trakcie testowania, oceny i walidacji produktu (np. specyfikacje bezpieczeństwa lub prywatności, analizy i wyniki testów, raporty walidacyjne i certyfikaty walidacyjne)[21] wykorzystywane są w zakresie, w jakim mają zastosowanie. Odpowiednie dowody uzyskane w wyniku testowania produktu można połączyć z dowodami związanymi z oceną uzyskanymi w wyniku zastosowania procedur oceny zawartych w niniejszej publikacji, aby w sposób ekonomiczny uzyskać informacje niezbędne do stwierdzenia, czy środki bezpieczeństwa i zabezpieczenia prywatności są skuteczne w swoim zastosowaniu.

## 1.4. ORGANIZACJA PUBLIKACJI

Pozostała część tej publikacji jest zorganizowana w następujący sposób:

- W rozdziale drugim opisano podstawowe pojęcia związane z oceną środków bezpieczeństwa i zabezpieczeń prywatności, w tym włączenie oceny do cyklu życia systemu, znaczenie strategii przeprowadzania ocen środków bezpieczeństwa i zabezpieczeń prywatności w całej organizacji, opracowanie skutecznych przypadków wiarygodności w celu zwiększenia zaufania

[21] Organizacje dokonują przeglądu dostępnych informacji o komponentach produktów informatycznych w celu ustalenia, jakie środki bezpieczeństwa i zabezpieczenia prywatności są zaimplementowane w produkcie, czy zabezpieczenia te są zgodne z zamierzonymi wymaganiami ocenianego systemu, czy konfiguracja produktu i środowisko, w którym produkt ten funkcjonuje, są zgodne z konfiguracją środowiska i produktu podaną przez sprzedawcę i/lub twórcę oraz czy wymagania wiarygodności podane w specyfikacji twórcy/sprzedawcy spełniają wymagania wiarygodności w zakresie oceny tych zabezpieczeń. Spełnienie powyższych kryteriów stanowi solidne uzasadnienie, że produkt nadaje się do zastosowania i spełnia zamierzone wymagania w zakresie środków bezpieczeństwa i zabezpieczeń prywatności dla ocenianego systemu.

do skuteczności ocenianych środków bezpieczeństwa i zabezpieczeń prywatności, a także format i treść procedur oceny.

- **W rozdziale trzecim** opisano proces oceny środków bezpieczeństwa i zabezpieczeń prywatności w systemach organizacyjnych i ich środowiskach pracy, w tym działania prowadzone przez organizacje i oceniających w celu przygotowania się do oceny środków bezpieczeństwa i zabezpieczeń prywatności, opracowanie planów oceny bezpieczeństwa, przeprowadzenie oceny środków bezpieczeństwa i zabezpieczeń prywatności, analizę, dokumentację i raportowanie wyników oceny oraz analizę raportu po przeprowadzeniu oceny i dalsze działania prowadzone przez organizacje.
- **W rozdziale czwartym** znajduje się katalog procedur oceny bezpieczeństwa i ochrony prywatności, które mogą być wykorzystane do opracowania planów oceny środków bezpieczeństwa.
- W załącznikach znajdują się szczegółowe informacje dotyczące oceny, w tym podstawowe referencje, definicje i terminy, akronimy, opis metod przeprowadzania oceny, wytyczne dotyczące testów penetracyjnych, zawartość raportów z oceny bezpieczeństwa i prywatności oraz informacje na temat automatyzacji przeprowadzanych ocen.

ROZDZIAŁ DRUGI

# 2. PODSTAWY

PODSTAWOWE POJĘCIA ZWIĄZANE Z OCENĄ ŚRODKÓW BEZPIECZEŃSTWA I ZABEZPIECZEŃ PRYWATNOŚCI

W niniejszym rozdziale przedstawiono podstawowe koncepcje związane z oceną środków bezpieczeństwa i zabezpieczeń prywatności w systemach organizacyjnych i środowiskach, w których te systemy działają, w tym włączenie oceny do cyklu życia systemu, znaczenie strategii przeprowadzania ocen w całej organizacji, opracowanie skutecznych przypadków wiarygodności w celu zwiększenia zaufania do skuteczności środków bezpieczeństwa i zabezpieczeń prywatności, a także format i treść procedur oceny. Podstawowym celem dokumentu NSC 800-53A jest zapewnienie elastycznych ram oceny i punktu wyjścia dla procedur oceny, które mogą być wykorzystywane przez różne organizacje i systemy, przy jednoczesnym zapewnieniu powtarzalnego podejścia ułatwiającego zachowanie spójności w przeprowadzaniu oceny zabezpieczeń.

## 2.1. OCENY W RAMACH CYKLU ŻYCIA SYSTEMU

Oceny bezpieczeństwa i ochrony prywatności można przeprowadzać na wszystkich etapach cyklu życia systemu[22] w celu zwiększenia pewności, że środki bezpieczeństwa i zabezpieczenia prywatności zastosowane w systemie lub przez niego dziedziczone są skuteczne w swoim zastosowaniu. Wytyczne zawarte w niniejszej publikacji stanowią kompleksowy zestaw procedur oceny, które wspierają działania związane z oceną bezpieczeństwa i ochrony prywatności w całym cyklu życia systemu. Przykładowo, oceny bezpieczeństwa i ochrony prywatności przeprowadza się rutynowo w fazach rozwoju/pozyskiwania i wdrażania podczas całego cyklu życia. Przeprowadzanie ocen w fazie

[22] W ogólnym cyklu życia systemu wyróżnia się zazwyczaj pięć faz: (I) inicjacja, (II) rozwój/pozyskanie, (III) wdrożenie, (IV) eksploatacja i utrzymywanie oraz (V) utylizacja (usuwanie).

rozwoju/pozyskiwania i wdrażania pomaga zagwarantować, że wymagane zabezpieczenia systemu zostaną zaprojektowane i opracowane zgodnie z celami zarządzania ryzykiem, że zostaną prawidłowo wdrożone oraz że będą zgodne z ustaloną organizacyjną architekturą bezpieczeństwa informacji i ochrony prywatności, zanim system wejdzie w fazę eksploatacji i utrzymywania. Oceny bezpieczeństwa i ochrony prywatności przeprowadzane w fazach cyklu życia przedoperacyjnego systemu obejmują przeglądy projektu i kodu, skanowanie aplikacji, testy regresji oraz zapewnienie, że przestrzegane są obowiązujące przepisy i zasady dotyczące ochrony prywatności, oraz że ochrona prywatności została uwzględniona w projekcie systemu.

Wady i braki związane z bezpieczeństwem i ochroną prywatności wykryte na wczesnym etapie cyklu życia systemu mogą być usunięte szybciej i w bardziej ekonomiczny sposób niż braki wykryte w kolejnych fazach cyklu życia. Wczesna identyfikacja wad i braków związanych z bezpieczeństwem i ochroną prywatności w wybranych środkach bezpieczeństwa i zabezpieczeniach prywatności ułatwia określenie i wdrożenie odpowiednich reakcji na ryzyko oraz umożliwia sprawdzenie skuteczności wdrożonych zabezpieczeń podczas projektowania i testowania systemu.

Oceny bezpieczeństwa i ochrony prywatności przeprowadza się również w fazie eksploatacji i utrzymywania cyklu życia, aby zapewnić, że zabezpieczenia są nadal skuteczne w środowisku pracy i chronią przed stale zmieniającymi się zagrożeniami. Podczas wstępnej autoryzacji systemu organizacje oceniają wszystkie środki bezpieczeństwa i zabezpieczenia prywatności stosowane w systemie i przez niego dziedziczone. Po wstępnej autoryzacji, organizacja na bieżąco ocenia wszystkie wdrożone środki bezpieczeństwa i zabezpieczenia prywatności zgodnie ze swoją Strategią ciągłego monitorowania bezpieczeństwa informacji (*ang. Information Security Continuous Monitoring - ISCM*)[23] i strategią ciągłego monitorowania ochrony

[23] Patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.*

prywatności[24]. W bieżącej ocenie i monitorowaniu zabezpieczeń stosuje się procedury oceny określone w niniejszej publikacji. Częstotliwość przeprowadzania takich ocen i monitorowania jest określana przez organizację, właściciela systemu i/lub dostawcę zabezpieczeń wspólnych i jest zatwierdzana przez osobę autoryzującą. Na koniec cyklu życia systemu przeprowadza się ocenę bezpieczeństwa i ochrony prywatności, aby upewnić się, że ważne informacje organizacyjne, w tym informacje umożliwiające identyfikację osób, zostały usunięte z systemu przed jego utylizacją oraz że przestrzegane są harmonogramy przechowywania danych.

## 2.2. STRUKTURA I ORGANIZACJA ZABEZPIECZEŃ

Zachęca się organizacje do opracowania szeroko zakrojonej strategii przeprowadzania ocen bezpieczeństwa i ochrony prywatności w całej organizacji, w celu osiągnięcia bardziej ekonomicznych i spójnych ocen we wszystkich systemach. Maksymalizacja liczby zabezpieczeń wspólnych stosowanych w organizacji znacznie obniża koszty opracowania, wdrożenia i oceny środków bezpieczeństwa i zabezpieczeń prywatności. Pozwala to organizacjom scentralizować i zautomatyzować oceny zabezpieczeń oraz zamortyzować koszty tych ocen we wszystkich systemach w organizacji, a także zwiększa spójność wdrażania środków bezpieczeństwa i zabezpieczeń prywatności.

[24] [NIST SP 800-137] zawiera wytyczne dotyczące ciągłego monitorowania środków bezpieczeństwa w ramach programu ISCM. Ciągłe monitorowanie może być skutecznie wykorzystane do zabezpieczeń prywatności zgodnie z koncepcjami, technikami i zasadami opisanymi w SP 800-137. SAOP (Senior Agency Officials for Privacy)/CPO (Chief Privacy Officers) zapewniają wytyczne dotyczące bieżącego monitorowania zabezpieczeń prywatności. Międzyagencyjny raport NIST 8011 [NISTIR 8011], *Automation Support for Security Control Assessments*, zawiera wytyczne dotyczące metod automatyzacji procesu oceny.

**KORZYŚCI WYNIKAJĄCE Z WDROŻENIA I OCENY ZABEZPIECZEŃ WSPÓLNYCH ORAZ Z DZIELENIA SIĘ WYNIKAMI OCENY**

Ogólnoorganizacyjne podejście do identyfikacji zabezpieczeń wspólnych na wczesnym etapie stosowania RMF umożliwia przyjęcie bardziej globalnej strategii oceny tych zabezpieczeń i udostępnienie wyników oceny właścicielom systemów oraz osobom autoryzującym. Dzielenie się wynikami oceny przez kluczowych pracowników organizacji, niezależnie od granic systemu, przynosi wiele istotnych korzyści, m.in:

- Zapewnienie możliwości przeglądu wyników oceny dla wszystkich systemów oraz podejmowania decyzji związanych z misją i działalnością w zakresie działań ograniczających ryzyko zgodnie z priorytetami organizacyjnymi, kategoryzacją systemów pod względem bezpieczeństwa oraz wynikami oceny ryzyka.
- Zapewnienie bardziej globalnego spojrzenia na wady i braki występujące w systemach w całej organizacji oraz możliwość opracowania ogólnoorganizacyjnych rozwiązań problemów związanych z bezpieczeństwem informacji i ochroną prywatności. Oraz
- Zwiększenie bazy wiedzy organizacji na temat zagrożeń, podatności (słabych punktów), ryzyka związanego z ochroną prywatności oraz strategii bardziej efektywnych kosztowo rozwiązań typowych problemów związanych z bezpieczeństwem informacji i ochroną prywatności.

Organizacje mogą również promować bardziej ukierunkowany i ekonomiczny proces oceny poprzez opracowywanie konkretnych procedur oceny, które są dostosowane do ich specyficznych środowisk pracy i wymagań (zamiast powierzania zadań związanych z opracowywaniem procedur oceny poszczególnym oceniającym zabezpieczenie lub zespołom oceniającym) oraz poprzez dostarczanie

ogólnoorganizacyjnych narzędzi, szablonów i technik pozwalających na przeprowadzanie bardziej spójnych ocen w całej organizacji.[25]

W skład osób odpowiedzialnych za przeprowadzanie ocen zabezpieczeń mogą wchodzić właściciele systemów, dostawcy zabezpieczeń wspólnych, osoby odpowiedzialne za bezpieczeństwo i prywatność systemów, niezależni oceniający, audytorzy i inspektorzy generalni, a nadzór nad nimi sprawuje osoba(y) autoryzująca(e)[26]. W proces oceny zaangażowane są również inne osoby działające w organizacji, dla których wynik oceny ma istotne znaczenie. Inne zainteresowane osoby to właściciele misji i przedsiębiorstw oraz właściciele informacji/władający informacją (jeśli te role pełni ktoś inny niż właściciel systemu). Konieczne jest, aby właściciele systemów i dostawcy zabezpieczeń wspólnych zidentyfikowali i skoordynowali działania z innymi stronami zainteresowanymi oceną zabezpieczeń, co zapewni, że główne misje i funkcje biznesowe organizacji zostaną odpowiednio uwzględnione w ocenie środków bezpieczeństwa i ochrony prywatności.

**UWAGA**

Podczas oceny środków bezpieczeństwa i zabezpieczeń prywatności w systemach *operacyjnych* organizacje powinny dokładnie rozważyć potencjalne skutki zastosowania procedur oceny określonych w niniejszej publikacji. Niektóre procedury oceny - zwłaszcza te, które bezpośrednio wpływają na pracę lub funkcje sprzętu, oprogramowania użytkowego lub oprogramowania układowego systemu - mogą niezamierzenie wpływać na rutynowe przetwarzanie, przesyłanie

[25] Organizacje mogą również dostarczać plany oceny środków bezpieczeństwa i zabezpieczeń prywatności, w tym dostosowane procedury oceny, zewnętrznym usługodawcom, którzy obsługują systemy w imieniu tych organizacji. Ponadto dostosowane do potrzeb plany oceny zabezpieczeń i ochrony prywatności mogą rekomendować pomocnicze szablony, narzędzia i techniki, a także być dostosowane do warunków umowy zawartej z dostawcą usług, dzięki czemu oceny stają się bardziej spójne, a artefakty związane z oceną są wykorzystywane ponownie w maksymalnym stopniu. Powtórne wykorzystanie artefaktów może poprawić bezpieczeństwo i ochronę prywatności dzięki zachowaniu jednolitości, a także może zmniejszyć lub wyeliminować niejednoznaczność umów, co prowadzi do zmniejszenia kosztów i ryzyka ponoszonego przez organizację.

[26] Zgodnie z [OMB A-130] przeprowadzanie niezależnej oceny programu i praktyk ochrony prywatności nie jest wymagane. Organizacja może jednak zdecydować się na przeprowadzenie niezależnych ocen ochrony prywatności według własnego uznania.

lub przechowywanie informacji, które wspierają misje organizacji lub funkcje biznesowe. Na przykład, krytyczny element systemu może zostać odłączony od sieci w celu przeprowadzenia oceny lub też element ten może ulec awarii lub usterce podczas procesu oceny. Organizacje podejmują niezbędne środki ostrożności, aby zapewnić, że ich misje i funkcje biznesowe są stale wspierane przez systemy oraz, że wszelkie potencjalne wpływy na efektywność operacyjną wynikające z działań związanych z oceną są brane pod uwagę z odpowiednim wyprzedzeniem.

## 2.3. OPRACOWYWANIE SKUTECZNEGO PRZYPADKU WIARYGODNOŚCI

Opracowywanie skutecznego przypadku wiarygodności[27] w zakresie skuteczności środków bezpieczeństwa i zabezpieczeń prywatności jest procesem obejmującym gromadzenie dowodów pochodzących z różnych działań prowadzonych w trakcie cyklu życia systemu, potwierdzających, że zabezpieczenia zastosowane w systemie są wdrożone prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądane efekty w odniesieniu do spełnienia wymagań systemu i organizacji dotyczące bezpieczeństwa i ochrony prywatności. Istotne jest przedstawianie tych dowodów w sposób, który osoby podejmujące decyzje są w stanie skutecznie wykorzystać przy podejmowaniu opartych na ryzyku decyzji dotyczących pracy lub użytkowania systemu (tj. w celu zarządzania ryzykiem). Wspomniane powyżej dowody wynikają z wdrożenia i dziedziczenia przez system środków bezpieczeństwa i zabezpieczeń prywatności (tj. zabezpieczeń wspólnych) oraz z ocen tego wdrożenia. W idealnej sytuacji oceniający bazuje na wcześniej opracowanych materiałach, które powstały na początku procesu określania potrzeb organizacji w zakresie bezpieczeństwa i ochrony prywatności informacji, a następnie były rozwijane podczas projektowania, tworzenia i wdrażania systemu. Materiały opracowane podczas

[27] Przypadek wiarygodności to zbiór dowodów ujętych w formie argumentu wskazującego na to, że pewne stwierdzenie dotyczące systemu jest prawdziwe (tzn. zostało osiągnięte). Przypadek wiarygodności jest konieczny, gdy ważne jest wykazanie, że system charakteryzuje się pewną złożoną właściwością, taką jak bezpieczeństwo, ochrona, prywatność lub niezawodność.

wdrażania bezpieczeństwa i ochrony prywatności w całym cyklu życia systemu stanowią wstępny materiał dowodowy dla przypadku wiarygodności.

W trakcie procesu oceny, osoba oceniająca uzyskują dowody niezbędne do umożliwienia właściwym pracownikom organizacji dokonania obiektywnych ustaleń dotyczących skuteczności środków bezpieczeństwa i zabezpieczeń prywatności oraz ogólnego stanu bezpieczeństwa i prywatności systemu. Dowody oceny potrzebne do dokonania takich ustaleń można uzyskać z różnych źródeł, w tym z ocen produktów i systemów informatycznych oraz - w przypadku oceny ochrony prywatności - z dokumentacji, takiej jak oceny wpływu na prywatność i system dokumentacji zgodny z ustawą o ochronie danych osobowych. Oceny produktu (znane także jako testowanie, ocena i walidacja produktu) są zwykle przeprowadzane przez niezależne, zewnętrzne organizacje testujące. W ramach oceny sprawdzane są funkcje produktów związane z bezpieczeństwem i ochroną prywatności oraz ustalone ustawienia konfiguracyjne.

Oceny można przeprowadzać w celu wykazania zgodności z branżowymi, krajowymi lub międzynarodowymi standardami dotyczącymi bezpieczeństwa informacji i ochrony prywatności, a także z oświadczeniami producentów/sprzedawców. Ponieważ wiele produktów informatycznych jest ocenianych przez komercyjne organizacje testujące, a następnie wdrażanych w milionach systemów, oceny produktów mogą być przeprowadzane na wyższym poziomie szczegółowości i zapewniać głębszy wgląd w możliwości poszczególnych produktów w zakresie bezpieczeństwa i ochrony prywatności.

Oceny systemów i zabezpieczeń wspólnych są zazwyczaj przeprowadzane przez twórców systemów, integratorów systemów, właścicieli systemów, dostawców zabezpieczeń wspólnych, oceniających, audytorów, inspektorów oraz pracowników zajmujących się bezpieczeństwem informacji i ochroną prywatności w organizacjach. Oceniający lub zespoły oceniające zbierają dostępne informacje o systemie lub zabezpieczeniu wspólnym, pochodzące np. z ocen poszczególnych produktów składowych, informacji zawartych w planach bezpieczeństwa i ochrony

prywatności systemu, innej dokumentacji systemu lub zabezpieczenia wspólnego, wyników poprzednich ocen, a następnie przeprowadzają dodatkowe oceny systemu lub zabezpieczeń wspólnych, stosując różne metody i techniki. Oceny systemów i zabezpieczeń wspólnych są wykorzystywane do gromadzenia i oceny dowodów potrzebnych pracownikom organizacji do określenia, jak skutecznie środki bezpieczeństwa i zabezpieczenia prywatności stosowane w ich systemach ograniczają ryzyko dla działań i aktywów organizacji, osób, innych organizacji i państwa. Wyniki ocen przeprowadzonych z wykorzystaniem procedur oceny specyficznych dla danego systemu i organizacji, zaczerpniętych z wytycznych zawartych w niniejszej publikacji, przyczyniają się do zebrania dowodów niezbędnych do określenia skuteczności środków bezpieczeństwa i zabezpieczeń prywatności zgodnie z wymaganiami dotyczącymi wiarygodności, udokumentowanymi w planach bezpieczeństwa i ochrony prywatności.

***Dowody wiarygodności wynikające z działań rozwojowych i operacyjnych***

Organizacje osiągają wiarygodność w zakresie bezpieczeństwa i ochrony prywatności dzięki działaniom podejmowanym przez twórców systemów, osoby wdrażające, operatorów, personel odpowiedzialny za utrzymywanie zabezpieczeń oraz osoby oceniające. Działania osób i/lub grup w trakcie rozwoju/funkcjonowania systemów są źródłem dowodów dotyczących bezpieczeństwa i ochrony prywatności, które przyczyniają się do uzyskania wiarygodności lub miary zaufania do funkcjonalności w zakresie bezpieczeństwa i ochrony prywatności niezbędnej do osiągnięcia odpowiedniej zdolności do ochrony i do zapewnienia prywatności. Szczegółowość i zakres stosowania tych działań (opisanych w załączniku C) również wpływa na skuteczność dowodów i środków zaufania. Dowody uzyskane przez programistów, osoby wdrażające, operatorów, oceniających i osoby odpowiedzialne za utrzymanie systemu podczas jego cyklu życia (np. artefakty projektowe/rozwojowe i wyniki oceny) przyczyniają się do zrozumienia skuteczności środków bezpieczeństwa i zabezpieczeń prywatności wdrożonych przez organizacje.

Poziom bezpieczeństwa i prywatności[28] odgrywa ważną rolę w osiąganiu pożądanych zdolności, a następnie w spełnianiu przez organizacje wymagań dotyczących bezpieczeństwa i ochrony prywatności. Twórcy systemów mogą zwiększyć poziom bezpieczeństwa i ochrony prywatności, stosując w procesie rozwoju systemu dobrze zdefiniowane zasady i procedury bezpieczeństwa i ochrony prywatności, ustrukturyzowane i rygorystyczne techniki projektowania i rozwoju oraz skuteczne techniki inżynierii systemów, bezpieczeństwa i ochrony prywatności. Artefakty powstałe w wyniku działań rozwojowych (np. specyfikacje funkcjonalne, dokumentacja projektowa systemu, wyniki testów i analizy kodu) mogą stanowić ważny dowód na to, że systemy i ich komponenty są niezawodne i wiarygodne. Dowody dotyczące bezpieczeństwa i ochrony prywatności mogą również pochodzić z testów przeprowadzanych przez niezależne, zewnętrzne organizacje zajmujące się oceną oraz z innych działań oceniających prowadzonych przez organizacje sektora rządowego i prywatnego.[29]

Oprócz dowodów uzyskanych w środowisku rozwojowym, organizacje mogą uzyskać dowody ze środowiska pracy, przyczyniające się do zapewnienia funkcjonalności oraz zdolności w zakresie bezpieczeństwa i ochrony prywatności. Dowody operacyjne obejmują zapisy działań naprawczych, dane dotyczące raportowania o zdarzeniach naruszających bezpieczeństwo (w tym o naruszeniach obejmujących informacje umożliwiające identyfikację osób) oraz wyniki ciągłego monitorowania organizacji. Dowody te pomagają w określeniu skuteczności wdrożonych środków bezpieczeństwa i zabezpieczeń prywatności, zmian

[28] Poziom (siła) bezpieczeństwa lub ochrony prywatności komponentu systemu (tj. sprzętu, oprogramowania użytkowego lub oprogramowania układowego) jest określany na podstawie tego, w jakim stopniu funkcjonalności w zakresie bezpieczeństwa lub ochrony prywatności zaimplementowane w tym komponencie są poprawne, kompletne, odporne na bezpośrednie ataki (siła mechanizmu) oraz odporne na obejście lub manipulację.

[29] Na przykład, zewnętrzne organizacje oceniające poddają ocenie usługi w chmurze i dostawców usług w ramach Federalnego Programu Zarządzania Ryzykiem i Autoryzacją (*ang. Federal Risk and Authorization Management Program*) [FedRAMP]. Laboratoria testujące kryteria wspólne przeprowadzają testy i ocenę produktów technologii informacyjnej zgodnie z normą [ISO 15408] Laboratoria testujące kryptografię/bezpieczeństwo przeprowadzają testy modułów kryptograficznych zgodnie z normą [FIPS 140-3].

w systemach i środowiskach pracy oraz zgodności z przepisami, zasadami, dyrektywami, regulacjami i standardami. Dowody w zakresie bezpieczeństwa i ochrony prywatności - uzyskane zarówno w trakcie prac rozwojowych, jak i działań operacyjnych - pomagają organizacjom określić, w jakim stopniu ich systemy są prawidłowo wdrażane, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w zakresie spełniania określonych wymagań dotyczących bezpieczeństwa i ochrony prywatności, zapewniając tym samym większą wiarygodność możliwości systemu w zakresie bezpieczeństwa i ochrony prywatności.

Szczegółowość i zakres stosowania dowodów dotyczących bezpieczeństwa i ochrony prywatności może wpłynąć na poziom wiarygodności wdrożonej funkcjonalności. Szczegółowość i zakres stosowania są atrybutami związanymi z metodami oceny i generowaniem dowodów dotyczących bezpieczeństwa i ochrony prywatności.[30] Metody oceny mogą być stosowane do wspierania wiarygodności rozwojowej i operacyjnej. W przypadku wiarygodności rozwojowej, szczegółowość wiąże się z rygorem, poziomem szczegółowości i formalnością artefaktów powstałych podczas projektowania i rozwoju systemu. Poziom szczegółowości artefaktów rozwojowych może mieć wpływ na rodzaj testów, oceny i analizy przeprowadzanych podczas cyklu życia systemu (np. testy podstawowe, kompleksowe i ukierunkowane, analiza statyczna/dynamiczna). Dla zapewnienia wiarygodności operacyjnej atrybut *szczegółowość* odnosi się do rygoru i poziomu wnikliwości oceny. Z kolei atrybut zakres stosowania jest związany z metodami oceny wykorzystywanymi podczas rozwoju i eksploatacji, odnoszącymi się do zakresu i skali uwzględnianych obiektów oceny (np. liczba i typy testów przeprowadzanych na kodzie źródłowym).

[30] Dodatkowe informacje na temat szczegółowości i zakresu stosowania – patrz: rozdział 2.4 i załącznik C.

## 2.4. PROCEDURY OCENY: OBIEKTY, METODY I CELE OCENY

***Procedura*** oceny składa się z zestawu *celów* oceny, z których każdy ma przypisany zestaw potencjalnych *metod* i *obiektów* oceny. Cel oceny obejmuje jedno lub więcej *oświadczeń stwierdzających*, odnoszących się do badanego zabezpieczenia [NSC 800-53]. Oświadczenia stwierdzające są powiązane z treścią zabezpieczenia (tj. funkcjonalnością środków bezpieczeństwa i zabezpieczeń prywatności), aby zapewnić identyfikowalność wyników oceny z podstawowymi wymogami dotyczącymi zabezpieczenia. Zastosowanie procedury oceny wobec zabezpieczenia skutkuje uzyskaniem wyników oceny[31]. Wyniki oceny odzwierciedlają lub są następnie wykorzystywane do określenia ogólnej skuteczności zabezpieczenia i pomagają osobie autoryzującej podjąć świadomą, uwzględniającą ryzyko decyzję, czy wdrożyć system, lub czy kontynuować jego działanie.

### *2.4.1. OBIEKTY OCENY*

***Obiekty*** oceny określają konkretne pozycje podlegające ocenie w ramach danego zabezpieczenia i obejmują *specyfikacje*, *mechanizmy*, *działania* i *osoby*. Specyfikacje to artefakty oparte na dokumentach (np. zasady, procedury, plany, wymagania dotyczące bezpieczeństwa i ochrony prywatności systemu, specyfikacje funkcjonalne, projekty architektury) związane z systemem lub zabezpieczeniem wspólnym.

*Mechanizmy* to określone zabezpieczenia i środki zaradcze w postaci sprzętu, oprogramowania użytkowego lub oprogramowania układowego, stosowane w ramach systemu lub zabezpieczenia wspólnego.[32] *Działania* to konkretne czynności związane z ochroną, wspierające system lub zabezpieczenie wspólne, w które zaangażowani są ludzie (np. wykonywanie kopii zapasowych systemu,

[31] Więcej informacji na temat wyników oceny zabezpieczeń można znaleźć w rozdziale 3.3.

[32] Mechanizmy obejmują również urządzenia ochrony fizycznej związane z systemem lub zabezpieczeniami wspólnymi (np. zamki, klawiatury, kamery bezpieczeństwa, urządzenia przeciwpożarowe, sejfy ognioodporne itp.).

monitorowanie ruchu sieciowego, realizacja planu awaryjnego). *Osoby lub grupy osób* to ludzie stosujący opisane powyżej specyfikacje, mechanizmy lub działania.

### *2.4.2. METODY OCENY*

**Metody** oceny określają charakter działań oceniającego i obejmują sprawdzanie, wywiad i test.

- *Sprawdzanie* polega na przeglądaniu, kontroli, obserwowaniu, studiowaniu lub analizowaniu jednego lub więcej obiektów oceny (tj. specyfikacji, mechanizmów lub działań) w celu ułatwienia oceniającemu zrozumienia, doprecyzowania lub uzyskania dowodów.
- *Wywiad* polega na prowadzeniu rozmów z osobami lub grupami osób w organizacji w celu lepszego zrozumienia zagadnienia przez oceniającego, uzyskania wyjaśnień lub uzyskania dowodów.
- *Test* polega na sprawdzeniu jednego lub więcej obiektów oceny (np. działań lub mechanizmów) w określonych warunkach w celu porównania rzeczywistego stanu obiektu z jego pożądanym stanem lub oczekiwanym zachowaniem.

We wszystkich trzech metodach oceny, wyniki wykorzystywane są do dokonywania określonych ustaleń, o których mowa w oświadczeniach stwierdzających, a tym samym do osiągnięcia celów procedury oceny. Pełny opis metod i obiektów oceny znajduje się w załączniku C.

Metody oceny posiadają zestaw powiązanych atrybutów - *szczegółowość i zakres* stosowania - które pomagają określić poziom wysiłku włożonego w ocenę. Atrybuty mają charakter hierarchiczny, co umożliwia określenie rygoru i zakresu oceny w celu uzyskania większej wiarygodności, która może być wymagana w przypadku niektórych systemów.

- Atrybut *szczegółowość* dotyczy rygoru i poziomu szczegółowości badań, wywiadów i testów. Wartości dla atrybutu szczegółowość to: *podstawowa*, *ukierunkowana* i *kompleksowa*.
- Atrybut *zakres stosowania* dotyczy zakresu lub rozległości badań, wywiadów i testów, w tym liczby i typów specyfikacji, mechanizmów i działań, które

podlegają badaniu lub testowaniu, oraz osób, z którymi należy przeprowadzić rozmowy. Podobnie jak w przypadku atrybutu szczegółowości, wartości dla atrybutu zakresu stosowania to: *podstawowy*, *ukierunkowany* i *kompleksowy*.

Odpowiednie wartości atrybutów szczegółowości i zakresu stosowania dla danej metody oceny opierają się na wymaganiach dotyczących wiarygodności określonych przez organizację i są ważnym elementem ochrony informacji współmiernej do ryzyka (tj. zarządzania ryzykiem). Wraz ze wzrostem wymagań dotyczących wiarygodności w odniesieniu do opracowania, wdrożenia i funkcjonowania zabezpieczeń w systemie lub przez niego dziedziczonych, wzrasta również rygor i zakres działań związanych z oceną (co znajduje odzwierciedlenie w wyborze metod i obiektów oceny oraz przypisaniu wartości atrybutów szczegółowości i zakresu stosowania)[33].

Załącznik C zawiera szczegółowy opis atrybutów metod oceny oraz ich wartości.

### *2.4.3. CELE OCENY*

**Cele** oceny są kolejno ponumerowane, najpierw zgodnie ze schematem numeracji zawartym w [NSC 800-53], a następnie, w miarę potrzeby, w celu dalszej granulacji wymagań dotyczących środków bezpieczeństwa lub zabezpieczeń prywatności, tak aby ułatwić przeprowadzenie oceny. Numery porządkowe umieszczone w nawiasach kwadratowych, w odróżnieniu od nawiasów zwykłych, są używane w celu podkreślenia, że zabezpieczenie zawarte w NSC 800-53 zostało bardziej uszczegółowione (np. AC-17a.[01], AC-17a.[02], AC-17a.[03]).

Rysunek 1 przedstawia przykładową procedurę oceny opracowaną w celu oceny skuteczności zabezpieczenia AC-17. Cel oceny dla AC-17 wynika z podstawowego oświadczenia dotyczącego zabezpieczenia opisanego w [NSC 800-53]. AC-17a.[01] jest przykładem oświadczenia określającego dla elementu zabezpieczenia, które zostało bardziej uszczegółowione w stosunku do NSC 800-53. AC-17b. to przykład

[33] Poziom wysiłku włożonego w ocenę, w tym jej szczegółowość i zakres zastosowania, zależy przede wszystkim od oceny ryzyka utraty prywatności lub kategoryzacji bezpieczeństwa ocenianego systemu lub zabezpieczenia wspólnego.

oświadczenia określającego dla elementu zabezpieczenia, które odpowiada bezpośrednio zabezpieczeniu opisanemu w NSC 800-53. Do każdej procedury oceny dodawane są potencjalne metody i obiekty oceny. Nie wszystkie procedury oceny obejmują wszystkie trzy potencjalne metody oceny (tj. badanie, wywiad, test).
To organizacja określa metody oceny potrzebne do zapewnienia wymaganego przez nią poziomu wiarygodności.

| | | |
|---|---|---|
| **AC-17** | **ZDALNY DOSTĘP** | |
| | **CEL OCENY:**<br>*Określić, czy:* | |
| | **AC-17a.[01]**<br>(Zabezpieczenie uszczegółowione w stosunku do NSC 800-53) | dla każdego rodzaju dozwolonego zdalnego dostępu zostały ustalone i udokumentowane ograniczenia użytkowania; |
| | **AC-17a.[02]**<br>(Odpowiada bezpośrednio zabezpieczeniu opisanemu w NSC 800-53) | dla każdego rodzaju dozwolonego zdalnego dostępu zostały ustalone i udokumentowane wymagania dotyczące konfigurowania/połączenia; |
| | **AC-17a.[03]** | dla każdego rodzaju dozwolonego zdalnego dostępu zostały ustalone i udokumentowane wytyczne dotyczące wdrożenia; |
| | **AC-17b.** | każdy rodzaj zdalnego dostępu do systemu jest autoryzowany przed zezwoleniem na takie połączenie. |
| | **POTENCJALNE METODY I OBIEKTY OCENY:** | |
| | **AC-17**<br>**Badanie** | [WYBÓR SPOŚRÓD: Zasady kontroli dostępu; procedury dotyczące wdrażania i użytkowania zdalnego dostępu (w tym ograniczenia); plan zarządzania konfiguracją; ustawienia konfiguracji systemu i związana z tym dokumentacja; uprawnienia do zdalnego dostępu; rejestry audytu systemu; plan bezpieczeństwa systemu; inne odpowiednie dokumenty lub rejestry]. |
| | **AC-17**<br>**Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacji odpowiedzialny za zarządzanie połączeniami zdalnego dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. |
| | **AC-17**<br>**Test** | [WYBÓR SPOŚRÓD: Możliwość zarządzania zdalnym dostępem do systemu]. |

**Rysunek 1. Procedura oceny zabezpieczenia.**

Innym przykładem uszczegółowienia wspomagającego ocenę zabezpieczeń jest przypadek, w którym wymaganie dotyczące zabezpieczenia prywatności nie ma zastosowania do danego systemu (np. system nie przetwarza informacji umożliwiających identyfikację osób); oceniający mogą nie brać pod uwagę takich nie mających zastosowania wymagań i uznać, że zabezpieczenie jest spełnione. Rysunek 2 przedstawia przykład zabezpieczenia CM-04[34], które zostało jeszcze bardziej uszczegółowione w celu uwzględnienia wpływu na bezpieczeństwo w CM-04[01] i wpływu na prywatność w CM-04[02].

[34] Należy zauważyć, że identyfikatory zabezpieczeń (np. CM-4), opublikowane w [NSC 800-53], nie zawierają zera wiodącego. W przyszłych wersjach NSC 800-53 identyfikatory zabezpieczenia będą zawierać zero (np. CM-04).

| | | |
|---|---|---|
| **CM-04** | **ANALIZY WPŁYWU** | |
| | **CEL OCENY:**<br>*Określić, czy:* | |
| | **CM-04[01]** | zmiany w systemie są analizowane w celu określenia potencjalnego wpływu na bezpieczeństwo przed ich wprowadzeniem; |
| | **CM-04[02]** | zmiany w systemie są analizowane w celu określenia potencjalnego wpływu na prywatność przed ich wprowadzeniem.<br>(Uszczegółowienie w celu odniesienia się do wpływu na ochronę prywatności oddzielnie od wpływu na bezpieczeństwo). |
| | **POTENCJALNE METODY I OBIEKTY OCENY:** | |
| | **CM-04 Badanie** | [WYBÓR SPOŚRÓD: Zasady zarządzania konfiguracją; procedury dotyczące analiz wpływu na bezpieczeństwo w odniesieniu do zmian w systemie; procedury dotyczące analiz wpływu na prywatność w odniesieniu do planu zarządzania konfiguracją; dokumentacja dotycząca analizy wpływu na bezpieczeństwo; dokumentacja dotycząca analizy wpływu na prywatność; ocena wpływu na prywatność; dokumentacja dotycząca oceny ryzyka utraty prywatności, dokumentacja projektowa systemu; narzędzia analizy i związane z nimi dane wyjściowe; dokumentacja dotycząca kontroli zmian; dokumentacja dotycząca audytu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; inne odpowiednie dokumenty lub zapisy]. |
| | **CM-04 Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacji odpowiedzialny za przeprowadzanie analiz wpływu na bezpieczeństwo; personel organizacji odpowiedzialny za przeprowadzanie analiz wpływu na prywatność; personel organizacji odpowiedzialny za bezpieczeństwo i ochronę prywatności informacji; twórcy systemu; administratorzy systemu/sieci; członkowie rady ds. kontroli zmian lub podobni]. |
| | **CM-04 Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące analiz wpływu na bezpieczeństwo; procesy organizacyjne dotyczące analiz wpływu na prywatność]. |

**Rysunek 2. Procedura oceny zabezpieczenia uszczegółowionego w celu ułatwienia oceny.**

Ponadto oświadczenia dotyczące parametrów zdefiniowanych przez organizację (*ang. organization-defined parameters - ODPs*) są wymieniane jako pierwsze i niezależnie od oświadczeń określających dla każdego elementu w ramach zabezpieczenia lub zabezpieczenia rozszerzonego, aby umożliwić oceniającemu szybkie ustalenie, czy organizacja zdefiniowała lub wybrała ODP. ODP pojawiają się jako pierwsze w stwierdzeniach określających, a każdy z nich zawiera unikalny identyfikator związany z zabezpieczeniem, co pozwala na przeprowadzenie skuteczniejszej i sprawniejszej oceny.

ODP obejmują:

- **Operacje przydzielania**, w których organizacja określa wartość (np. częstotliwość, okoliczności, personel lub role).
- **Operacje wyboru**, w których organizacja wybiera jedną lub więcej opcji przewidzianych w ODP.

Konwencja numeracji ODP wygląda następująco: „**XX-nn_ODP**”, gdzie „**XX**” jest dwuznakowym skrótem oznaczającym kategorię zabezpieczenia, a „**nn**” jest numerem zabezpieczenia (w przypadku cyfr pojedynczych, na początku występuje zero), po którym następuje „**_ODP**”. Jeśli istnieje więcej niż jeden ODP dla danej procedury oceny, po „**_ODP**” umieszcza się kolejne numery w nawiasach kwadratowych, zaczynając od „**01**”. Wartość ODP jest przywoływana w kolejnych stwierdzeniach określających przy użyciu unikalnego identyfikatora ODP i krótkiego wyrażenia opisującego ODP zapisanego pomiędzy znakami **< >**. Podobnie jak w przypadku deklarowania zmiennej w programowaniu komputerowym, ODP służy jako nazwa umowna odnosząca się do przechowywanej wartości. W tym scenariuszu, unikalny identyfikator ODP służy jako nazwa symboliczna, a wartość przypisana lub wybrana przez organizację jest wartością składową.

Rysunek 3 przedstawia przykład procedury oceny dla zabezpieczenia CM-02, która obejmuje dwie operacje przydzielania: CM-02_ODP[01] i CM-02_ODP[02].

| | | |
|---|---|---|
| **CM-02** | **CEL OCENY KONFIGURACJI BAZOWEJ:** | |
| | **CEL OCENY:**<br>*Określić, czy:* | |
| | **CM-02_ODP[01]** | **zdefiniowano częstotliwość przeprowadzania przeglądu i aktualizacji konfiguracji bazowej;** |
| | **CM-02_ODP[02]**<br>(ODP - identyfikator parametru definiowanego przez organizację) | **zdefiniowano okoliczności powodujące konieczność przeprowadzenia przeglądu i aktualizacji konfiguracji bazowej;**<br>(Operacje przydzielania) |
| | **CM-02a.[01]** | opracowano i udokumentowano aktualną konfigurację bazową systemu; |
| | **CM-02a.[02]** | aktualna konfiguracja bazowa systemu jest utrzymywana w ramach kontroli konfiguracji; |
| | **CM-02b.01** | konfiguracja bazowa systemu jest poddawana przeglądowi i jest aktualizowana; |
| | **CM-02b.02** | konfiguracja bazowa systemu jest poddawana przeglądowi i jest aktualizowana w razie potrzeby wynikającej z <CM-02_ODP[02] okoliczności>;<br>(Odniesienie do ODP w oświadczeniu stwierdzającym zgodność) |
| | **CM-02b.03** | konfiguracja bazowa systemu jest poddawana przeglądowi i aktualizowana po zainstalowaniu lub uaktualnieniu składników systemu. |
| | **POTENCJALNE METODY I OBIEKTY OCENY:** | |
| | **CM-02**<br>**Badanie** | [WYBÓR SPOŚRÓD: Zasady zarządzania konfiguracją; procedury dotyczące bazowej konfiguracji systemu; plan zarządzania konfiguracją; dokumentacja architektury korporacyjnej; dokumentacja projektu systemu; plan bezpieczeństwa systemu; plan ochrony prywatności; dokumentacja architektury i konfiguracji systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; inwentaryzacja komponentów systemu; rejestry dotyczące kontroli zmian; inne stosowne dokumenty lub zapisy]. |

| | | |
|---|---|---|
| | **CM-02**<br>**Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacji odpowiedzialny za zarządzanie konfiguracją; personel organizacji odpowiedzialny za bezpieczeństwo i ochronę prywatności informacji; administratorzy systemów/sieci]. |
| | **CM-02**<br>**Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne do zarządzania konfiguracjami bazowymi; zautomatyzowane mechanizmy wspomagające kontrolę konfiguracji bazowej]. |

**Rysunek 3. Procedura oceny zabezpieczenia o parametrze zdefiniowanym przez organizację: operacje przydzielania.**

Rysunek 4 przedstawia przykład procedury oceny dla zabezpieczenia MP-07, która obejmuje operacje dostosowywania i wyboru. Operacje wyboru obejmują listę potencjalnych wartości parametrów, spośród których organizacja może wybierać, oraz instrukcje wyboru jednego lub więcej parametrów. Lista wartości parametrów jest określana za pomocą nawiasów klamrowych { }, a każda potencjalna wartość parametru jest oddzielona średnikiem. Gdy ODP dla operacji wyboru jest przywoływany w kolejnym oświadczeniu stwierdzającym, unikatowy identyfikator ODP i wyrażenie „WYBRANA WARTOŚĆ PARAMETRU (WYBRANE WARTOŚCI PARAMETRÓW)" są otoczone znakiem < >.

| MP-07 | **UŻYWANIE NOŚNIKÓW DANYCH** | |
|---|---|---|
| | **CEL OCENY:**<br>*Określić, czy:* | |
| | **MP-07_ODP[01]** | **określono rodzaje nośników danych systemowych, których stosowanie w systemach lub komponentach jest ograniczone lub zabronione;** |
| | **MP-07_ODP[02]**<br>(ODP - identyfikator parametru definiowanego przez organizację) | **wybrano jedną z poniższych WARTOŚCI PARAMETRU, która ma być stosowana na określonych typach nośników danych systemowych: {ograniczyć; zakazać};**<br>(Deklaracja wyboru) |
| | **MP-07_ODP[03]** | **systemy lub komponenty systemu, w których zdefiniowano użycie określonych typów nośników danych systemowych, które mają być ograniczone lub zabronione;** |
| | **MP-07_ODP[04]** | **zdefiniowano zabezpieczenia ograniczające lub zakazujące stosowania określonych typów nośników systemowych w systemach lub komponentach systemu;** |
| | **MP-07a.** | zastosowanie <**MP-07_ODP[01] typy nośników systemowych**> jest <**MP-07_ODP[02] WARTOŚĆ PARAMETRU WYBRANEGO**> w <**MP-07_ODP[03] systemach lub komponentach systemu**><br>z zastosowaniem zabezpieczenia <**MP-07_ODP[04]**>;<br>(Odniesienie do ODP w oświadczeniu stwierdzającym zgodność) |
| | **MP-07b.** | korzystanie z przenośnych urządzeń pamięci masowej w systemach organizacyjnych jest zabronione, jeżeli urządzenia te nie mają identyfikowalnego właściciela. |
| | **POTENCJALNE METODY I OBIEKTY OCENY:** | |
| | **MP-07**<br>**Badanie** | WYBÓR SPOŚRÓD: Zasady ochrony nośników systemowych; zasady użytkowania systemu; procedury dotyczące ograniczeń w korzystaniu z nośników; zasady postępowania; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytów; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |

| MP-07 | UŻYWANIE NOŚNIKÓW DANYCH | |
|---|---|---|
| | **MP-07**<br>**Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacji odpowiedzialny za korzystanie z nośników systemowych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. |
| | **MP-07**<br>**Test** | [WYBÓR SPOŚRÓD: Procesy organizacyjne dotyczące korzystania z nośników danych; zautomatyzowane mechanizmy ograniczające lub zakazujące korzystania z nośników danych systemowych w systemach lub komponentach systemu]. |

**Rysunek 4. Procedura oceny zabezpieczenia o parametrze zdefiniowanym przez organizację: operacje wyboru.**

Rysunek 5 przedstawia przykład procedury oceny dla zabezpieczenia CA-03, które obejmuje ODP składający się z operacji wyboru z osadzoną operacją przydzielania. Operacja wyboru, CA-03(01)_ODP[01], określa listę parametrów do wyboru, w tym inny ODP. Operacja przydzielania dla CA-03(01)_ODP[02] jest zdefiniowana tylko wtedy, gdy organizacja wybierze ODP z listy parametrów. Gdy ODP dla operacji wyboru jest przywoływany w kolejnym oświadczeniu stwierdzającym, unikatowy identyfikator ODP i wyrażenie „WYBRANA WARTOŚĆ PARAMETRU (WYBRANE WARTOŚCI PARAMETRÓW)" są otoczone znakiem < >. W tym scenariuszu, jeśli zostanie wybrana osadzona operacja przydzielania, staje się ona „WYBRANĄ WARTOŚCIĄ PARAMETRU(WYBRANYMI WARTOŚCIAMI PARAMETRÓW)".

| **CA-03** | **WYMIANA INFORMACJI** | |
|---|---|---|
| | **CEL OCENY:**<br>*Określić, czy:* | |
| | **CA-03_ODP[01]**<br>(ODP - identyfikator parametru definiowanego przez organizację) | **Wybrano jedną lub więcej spośród następujących WARTOŚCI PARAMETRÓW: {umowy o bezpieczeństwie połączenia; umowy o bezpieczeństwie wymiany informacji; porozumienia o współpracy lub protokoły uzgodnień; umowy o poziomie usług; umowy z użytkownikami; umowy o nieujawnianiu informacji; <CA-03_ODP[02] typ umowy>};**<br>(Identyfikator parametru definiowanego przez organizację (ODP). |
| | **CA-03_ODP[02]** | **określono rodzaj umowy stosowanej do zatwierdzania wymiany informacji i zarządzania nią (jeśli została wybrana);**<br>(Osadzone oświadczenie o przydzieleniu, definiowane tylko po jego wybraniu). |
| | **CA-03_ODP[03]** | **określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji umów;** |
| | **CA-03a.** | wymiana informacji pomiędzy tym systemem a innymi systemami została zatwierdzona i jest zarządzana przy użyciu <**CA-03_ODP[01] WYBRANA WARTOŚĆ PARAMETRU**>;<br>(Odniesienie do ODP z wybraną wartością parametru w oświadczeniu). |
| | **CA-03b.[01]** | właściwości interfejsu są udokumentowane w ramach każdej umowy wymiany; |
| | **CA-03b.[02]** | wymagania bezpieczeństwa są dokumentowane jako element każdej umowy o wymianie; |
| | **CA-03b.[03]** | wymagania dotyczące ochrony prywatności są dokumentowane jako element każdej umowy o wymianie; |
| | **CA-03b.[04]** | zabezpieczenia są dokumentowane jako element każdej umowy o wymianie; |

| | | |
|---|---|---|
| | **CA-03b.[05]** | odpowiedzialność za każdy system jest udokumentowana jako element każdej umowy o wymianie; |
| | **CA-03b.[06]** | poziom wpływu przekazywanych informacji jest dokumentowany jako element każdej umowy o wymianie; |
| | **CA-03c.** | umowy są poddawane przeglądowi i aktualizowane <**CA-03_ODP[03] frequency**>. |
| | **POTENCJALNE METODY I OBIEKTY OCENY:** | |
| | **CA-03**<br>**Badanie** | [WYBÓR SPOŚRÓD: Zasady kontroli dostępu; procedury dotyczące połączeń systemowych; zasady ochrony systemu i komunikacji; umowy dotyczące bezpieczeństwa połączeń systemowych; umowy dotyczące bezpieczeństwa wymiany informacji; porozumienia o współpracy lub protokoły uzgodnień; umowy o poziomie świadczonych usług; umowy o zachowaniu poufności; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; plan bezpieczeństwa systemu; plan ochrony prywatności; inne stosowne dokumenty lub zapisy]. |
| | **CA-03**<br>**Wywiad** | [WYBÓR SPOŚRÓD: Personel organizacji odpowiedzialny za opracowywanie, wdrażanie lub zatwierdzanie umów o połączeniu systemów; personel organizacji odpowiedzialny za bezpieczeństwo i ochronę prywatności informacji; personel zarządzający systemem (systemami), do którego (których) ma zastosowanie umowa o zabezpieczeniu połączeń systemów]. |

**Rysunek 5. Procedura oceny zabezpieczenia o parametrach zdefiniowanych przez organizację: operacja wyboru z osadzoną operacją przydzielania.**

Chociaż nie jest to wyraźnie zaznaczone, przy każdej metodzie oceny w procedurze oceny wartości atrybutów szczegółowości i zakresu stosowania[35] są przypisywane przez organizację i określane w planie oceny (np. poziom rygoru przeglądu dokumentacji, liczba podobnych obiektów oceny do przetestowania).

[35] Wartości atrybutów szczegółowości i zakresu stosowania opisano w załączniku C.

Oceniający/zespół ds. oceny stosuje atrybuty szczegółowości i zakresu stosowania w trakcie realizacji metody oceny w odniesieniu do obiektu oceny w celu zapewnienia poziomu wiarygodności wymaganego przez organizację.

Jeśli zabezpieczenie obejmuje zabezpieczenia rozszerzone oznaczone przy pomocy numerów w nawiasach (Na przykład, AC-17(01) dla pierwszego rozszerzenia AC-17), cele oceny są opracowywane dla każdego rozszerzenia przy użyciu tego samego procesu, który został zastosowany dla zabezpieczenia podstawowego. Wynikające z tego cele oceny są numerowane kolejno w taki sam sposób, jak procedura oceny dla zabezpieczenia podstawowego - najpierw zgodnie ze schematem numeracji zawartej w [NSC 800-53], a następnie przy użyciu numerów sekwencyjnych w celu dalszego podziału wymagań dotyczących zabezpieczenia rozszerzonego, co ułatwia przeprowadzenie oceny (np. AC-17(01), AC-17(02), AC-17(03)).

Rysunek 6 przedstawia przykładową procedurę oceny opracowaną w celu oceny skuteczności pierwszego rozszerzenia środka bezpieczeństwa AC-17, AC-17(01).

| | | |
|---|---|---|
| **AC-17(01)** | **ZDALNY DOSTĘP \| ZAUTOMATYZOWANE MONITOROWANIE / KONTROLA** | |
| | **CEL OCENY:**<br>*Określić, czy:* | |
| | **AC-17(01)[01]** | do monitorowania metod zdalnego dostępu stosuje się mechanizmy automatyczne; |
| | **AC-17(01)[02]** | do kontroli metod zdalnego dostępu stosuje się mechanizmy automatyczne. |
| | **POTENCJALNE METODY I OBIEKTY OCENY:** | |
| | **AC-17(01)**<br>**Badanie** | [WYBÓR SPOŚRÓD: Zasady kontroli dostępu; procedury dotyczące zdalnego dostępu do systemu; dokumentacja projektowa systemu; ustawienia konfiguracyjne systemu i związana z nimi dokumentacja; zapisy z audytu systemu; rejestry monitorowania systemu; plan bezpieczeństwa systemu; inne istotne dokumenty lub zapisy]. |
| | **AC-17(01)**<br>**Wywiad** | [WYBÓR SPOŚRÓD: Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; twórcy systemów]. |
| | **AC-17(01)**<br>**Test** | [WYBÓR SPOŚRÓD: Zautomatyzowane mechanizmy monitorujące i kontrolujące metody zdalnego dostępu]. |

**Rysunek 6. Procedura oceny zabezpieczenia rozszerzonego.**

ROZDZIAŁ TRZECI

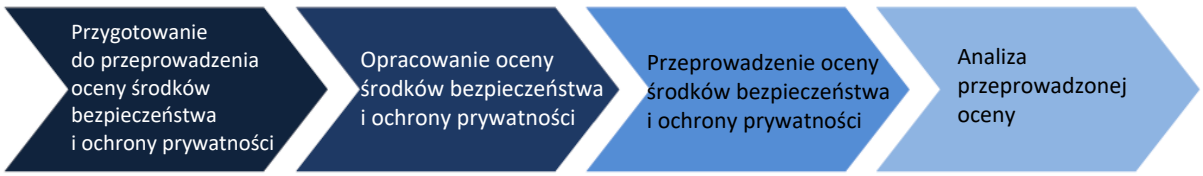
# 3. PROCES

PRZEPROWADZANIE SKUTECZNYCH OCEN ŚRODKÓW BEZPIECZEŃSTWA I ZABEZPIECZEŃ PRYWATNOŚCI

W niniejszym rozdziale opisano proces oceny środków bezpieczeństwa i zabezpieczeń prywatności w systemach organizacyjnych i środowiskach pracy. Proces oceny zabezpieczeń obejmuje:

- działania prowadzone przez organizacje i osoby oceniające w celu przygotowania się do oceny środków bezpieczeństwa i zabezpieczeń prywatności;
- opracowanie planów oceny środków bezpieczeństwa i ochrony prywatności; przeprowadzenie oceny zabezpieczeń i analiza wyników, przygotowanie dokumentacji i raportów z wynikami oceny; oraz
- analiza raportu z przeprowadzonej oceny i działania następcze.

Ponadto, w niniejszym rozdziale opisano ocenę *zdolności* do zapewnienia bezpieczeństwa i prywatności.[36]




**Rysunek 7. Proces przeprowadzania skutecznej oceny środków bezpieczeństwa i zabezpieczeń prywatności.**

[36] *Zdolność* do zapewnienia bezpieczeństwa i prywatności to połączenie wzajemnie uzupełniających się środków bezpieczeństwa i zabezpieczeń prywatności (tj. zabezpieczeń i środków zaradczych) wdrażanych za pomocą środków technicznych (tj. funkcjonalności sprzętu, oprogramowania użytkowego i oprogramowania układowego), środków fizycznych (tj. urządzeń fizycznych, działania zapobiegawcze) oraz środków proceduralnych (tj. procedury wykonywane przez osoby fizyczne).

## 3.1. PRZYGOTOWANIA DO PRZEPROWADZENIA OCENY ŚRODKÓW BEZPIECZEŃSTWA I ZABEZPIECZEŃ PRYWATNOŚCI

Tabela 1 zawiera opis celu, ról i oczekiwanych rezultatów dla etapu: *Przygotowania do oceny środków bezpieczeństwa i zabezpieczeń prywatności*.

| **Cel** | **Kwestie dotyczące kosztów, harmonogramu, zakresu oceny i przeprowadzenia oceny zabezpieczeń.** |
|---|---|
| **Role podstawowe** | Osoba autoryzująca, wyznaczony przedstawiciel osoby autoryzującej, właściciel systemu, dostawca zabezpieczeń wspólnych, oceniający zabezpieczenia. |
| **Role pomocnicze** | Osoba odpowiedzialna za zapewnienie utrzymania odpowiedniego poziomu bezpieczeństwa systemu, osoba odpowiedzialna za prywatność i ochronę danych osobowych w systemie. |
| **Rezultaty** | • Określenie celu, zakresu i ram czasowych oceny zabezpieczeń.<br>• Poinformowanie kluczowych interesariuszy i przydzielenie niezbędnych środków.<br>• Zebranie i przekazanie artefaktów oceniającym/zespołom ds. oceny.<br>• Opracowanie mechanizmu minimalizowania niejasności i nieporozumień odnośnie przeprowadzanej oceny, identyfikacja wad zabezpieczeń i braków w nich.<br>• Zapoznanie się przez oceniających/ zespoły ds. oceny z działalnością organizacji, jej strukturą, celem, zakresem i ramami czasowymi oceny zabezpieczeń. |

**Tabela 1. Podsumowanie etapu przygotowania do przeprowadzenia oceny środków bezpieczeństwa i zabezpieczeń prywatności.**

Przeprowadzanie oceny środków bezpieczeństwa i zabezpieczeń prywatności może być trudne i może wymagać dużej ilości zasobów. Ocena środków bezpieczeństwa

i zabezpieczeń prywatności może być przeprowadzana przez różne jednostki organizacyjne, posiadające odrębne obowiązki nadzorcze. W celu osiągnięcia sukcesu konieczna jest współpraca wszystkich stron zainteresowanych bezpieczeństwem i ochroną prywatności w organizacji, w tym osób dokonujących oceny, specjalistów ds. bezpieczeństwa i ochrony prywatności, właścicieli systemów, dostawców zabezpieczeń wspólnych, jednostek zatwierdzających, osób odpowiedzialnych za technologie informacyjne, jednostek ds. bezpieczeństwa informacji, jednostek ds. ochrony prywatności, pracowników ds. bezpieczeństwa i ochrony prywatności, inspektorów generalnych oraz biura zarządzania i budżetu. Ustalenie odpowiedniego zestawu oczekiwań przed, w trakcie i po dokonaniu oceny ma zasadnicze znaczenie dla osiągnięcia zadowalającego wyniku (tj. dostarczenie informacji niezbędnych do podjęcia przez jednostkę zatwierdzającą decyzji, opartej na analizie ryzyka, odnośnie tego czy wdrożyć dany system/kontynuować jego działanie).

Odpowiednie przygotowanie się organizacji i osób przeprowadzających ocenę jest ważnym aspektem przeprowadzenia skutecznej oceny środków bezpieczeństwa i zabezpieczeń prywatności. Działania przygotowawcze dotyczą szeregu kwestii związanych z kosztem, harmonogramem i samego przeprowadzenia oceny. Z perspektywy organizacji, przygotowanie się do oceny środków bezpieczeństwa i zabezpieczeń prywatności obejmuje następujące kluczowe działania:

- Zapewnienie, że odpowiednie zasady dotyczące oceny środków bezpieczeństwa i zabezpieczeń prywatności zostały wdrożone i zrozumiałe dla wszystkich zainteresowanych jednostek organizacyjnych.
- Upewnienie się, że wszystkie etapy odnośnie Ram Zarządzania Ryzykiem (RMF), poprzedzające etap oceny środków bezpieczeństwa lub zabezpieczeń prywatności, zostały pomyślnie zakończone i zaakceptowane przez kierownictwo[37].

[37] Przeprowadzanie oceny środków bezpieczeństwa i zabezpieczeń prywatności równolegle do etapu rozwoju/nabywania i wdrażania cyklu życia pozwala na wczesną identyfikację wad i braków i stanowi najbardziej opłacalną metodę inicjowania działań naprawczych. Problemy wykryte podczas

- Określenie celu i zakresu oceny (tj. cel oceny, co podlega ocenie).
- Zapewnienie, że opracowanie i przeprowadzenie oceny środków bezpieczeństwa i zabezpieczeń prywatności, rozumianych jako zabezpieczenia wspólne (oraz wspólna część zabezpieczeń hybrydowych) zostały przydzielone odpowiednim jednostkom organizacyjnym (tj. dostawcom zabezpieczeń wspólnych).[38]
- Informowanie kluczowych jednostek organizacyjnych o zbliżającej się ocenie i przydzielenie zasobów niezbędnych do przeprowadzenia oceny.
- Ustanowienie odpowiednich kanałów komunikacji między jednostkami organizacyjnymi zainteresowanymi oceną.
- Ustalenie ram czasowych oceny i kluczowych punktów decyzyjnych wymaganych przez organizację.
- Wybór odpowiednich oceniających/zespołów ds. oceny odpowiedzialnych za przeprowadzenie oceny i rozważenie kwestii niezależności oceniającego.
- Dostarczanie artefaktów oceniającym/zespołom ds. oceny (np. zasad, procedur, planów, specyfikacji, projektów, zapisów, instrukcji obsługi, dokumentacji systemowej, umów o wymianie informacji, wyników poprzednich ocen, wymogów prawnych).
- Wdrożenie odpowiedniego mechanizmu pomiędzy organizacją a oceniającymi/ zespołami ds. oceny w celu zminimalizowania niejasności lub nieporozumień dotyczących wdrażania środków bezpieczeństwa i zabezpieczeń prywatności oraz związanych z nimi wad i braków zidentyfikowanych podczas przeprowadzania ocen.

dokonywania oceny mogą być przekazane jednostkom zatwierdzającym w celu ich szybkiego rozwiązania, stosownie do potrzeb. Wyniki ocen systemu bezpieczeństwa i zabezpieczeń prywatności przeprowadzonych podczas opracowywania i wdrażania systemu mogą być również wykorzystane (zgodnie z kryteriami ponownego wykorzystania) w procesie autoryzacji w celu uniknięcia opóźnień w uruchomieniu systemu lub kosztów związanych z ponawianiem ocen.

[38] Za przeprowadzenie oceny zabezpieczeń wspólnych/wspólnej części zabezpieczeń hybrydowych odpowiedzialni są dostawcy zabezpieczeń wspólnych, a nie właściciel systemu dziedziczący zabezpieczenia.

Odnośnie oceniających/zespołów ds. oceny zabezpieczeń, przygotowanie się do przeprowadzenia oceny obejmuje:

- Zrozumienie, na czym polega działalność organizacji (w tym misja, funkcje i procesy biznesowe) oraz tego, w jaki sposób system lub zabezpieczenie wspólne będące przedmiotem danej oceny, wspiera działania organizacyjne w danej firmie.
- Zrozumienie struktury systemu (tj. architektury systemu) oraz środków bezpieczeństwa i zabezpieczeń prywatności (w tym zabezpieczeń specyficznych systemu, hybrydowych i wspólnych) będących przedmiotem danej oceny.
- Identyfikacja jednostek organizacyjnych odpowiedzialnych za opracowanie i wdrożenie zabezpieczeń wspólnych (lub części wspólnej zabezpieczeń hybrydowych) wspierających system.
- Dyskusja z odpowiednimi przedstawicielami organizacji, aby określić cele i zakres oceny.
- Uzyskanie danych potrzebnych do przeprowadzenia oceny (np. wytycznych, procedur, planów, specyfikacji, projektów, zapisów, instrukcji obsługi, dokumentacji systemowej, umów o wymianie informacji, wyników poprzedniej oceny).
- Wyznaczenie osób kontaktowych odnośnie przeprowadzanej oceny.
- Zapoznanie się z wynikami wcześniejszych ocen, które mogą być odpowiednio wykorzystane w bieżącej ocenie (np. raporty inspektora generalnego, audyty, skany podatności, inspekcje bezpieczeństwa fizycznego, testy i oceny rozwojowe, działania naprawcze dotyczące wad dostawcy, normy [ISO 15408]).

W ramach przygotowań do oceny środków bezpieczeństwa i zabezpieczeń prywatności gromadzone są niezbędne informacje ogólne i udostępniane oceniającym/zespołom ds. oceny.[39] W zakresie niezbędnym do przeprowadzenia konkretnej oceny i w zależności od tego czy oceniane są środki bezpieczeństwa

[39] Właściciele systemów (lub programów) oraz jednostki w organizacji odpowiedzialne za opracowanie, wdrożenie i/lub zarządzanie zabezpieczeniami wspólnymi (tj. dostawcy zabezpieczeń wspólnych) są odpowiedzialni za dostarczanie potrzebnych informacji oceniającym/zespołom ds. oceny

lub zabezpieczenia prywatności, organizacja określa i zapewnia dostęp do jednostek odpowiedzialnych za przygotowywanie, dokumentowanie, dystrybucję, przegląd i aktualizację:

- Wszelkich zasad i związanych z nimi procedur wdrażania zabezpieczeń zgodnych z zasadami.
- Zasad dla systemu i wszelkich powiązanych procedur wykonawczych, osób lub zespołów odpowiedzialnych za rozwój, wdrożenie, funkcjonowanie i utrzymywanie zabezpieczeń;[40]
- Wszelkich danych lub materiałów (np. plany bezpieczeństwa lub ochrony prywatności. rejestry, harmonogramy, sprawozdania z oceny, sprawozdania po zakończeniu działań, umowy, pakiety autoryzacyjne) związanych z wdrażaniem i działaniem ocenianych zabezpieczeń.
- Poszczególnych obiektów podlegających ocenie.[31]

Dostępność niezbędnej dokumentacji, jak również dostęp do kluczowego personelu organizacyjnego i ocenianego systemu lub zabezpieczenia wspólnego mają zasadnicze znaczenie dla pomyślnego przeprowadzenia oceny.

Podczas doboru osób oceniających środki bezpieczeństwa i zabezpieczenia prywatności, organizacje biorą pod uwagę zarówno wiedzę techniczną, jak i poziom niezależności.[41] Organizacje zapewniają, że oceniający posiadają wymagane umiejętności i wiedzę techniczną, aby z powodzeniem przeprowadzać ocenę zabezpieczeń specyficznych systemu, hybrydowych i wspólnych.[42] Umiejętności

[40] W sytuacji, gdy w organizacji przeprowadzanych/planowanych jest wiele ocen środków bezpieczeństwa i ochrony prywatności, organizacja zarządza dostępem do jednostek organizacyjnych, osób i danych w taki sposób, aby zapewnić efektywne wykorzystanie czasu i zasobów pod względem ponoszonych kosztów.

[41] Zgodnie z [OMB A-130], nie jest wymagana niezależna ocena programu i praktyki ochrony prywatności. Organizacja może jednak zdecydować się na zastosowanie niezależnej oceny ochrony prywatności według własnego uznania.

[42] NIST [SP 800-181] określa *Workforce Framework for Cybersecurity (National Initiative for Cybersecurity Education [NICE] Framework)* - punkt odniesienia odnośnie opisywania i dzielenia się informacjami na temat cyberbezpieczeństwa poprzez oświadczenia dotyczące zadań oraz oświadczenia dotyczące wiedzy i umiejętności. Ramy NICE stanowią źródło odniesienia, na podstawie którego organizacje lub sektory mogą opracowywać dodatkowe publikacje lub narzędzia spełniające ich potrzeby w zakresie

i wiedza specjalistyczna obejmują wiedzę i doświadczenie w zakresie konkretnego sprzętu, oprogramowania użytkowego i oprogramowania układowego stosowanych w danej organizacji. Niezależny oceniający to każda osoba zdolna do przeprowadzenia bezstronnej oceny środków bezpieczeństwa i zabezpieczeń prywatności stosowanych w danym systemie lub przez ten system dziedziczonych. Bezstronność oznacza, że oceniający środki bezpieczeństwa i zabezpieczenia prywatności są wolni od wszelkich domniemanych lub rzeczywistych konfliktów interesów w odniesieniu do opracowania, obsługi i/lub zarządzania systemem lub określania skuteczności środków bezpieczeństwa i zabezpieczeń prywatności.[43] Jednostka zatwierdzająca lub wyznaczony przedstawiciel określa wymagany poziom niezależności oceniających/zespołów ds. oceny na podstawie wyników procesu kategoryzacji bezpieczeństwa systemu (w przypadku oceny środków bezpieczeństwa) oraz ryzyka dla działań i aktywów organizacji, osób fizycznych, innych organizacji, państwa. Jednostka zatwierdzająca określa, czy poziom niezależności oceniającego jest wystarczający, aby zapewnić, że uzyskane wyniki oceny są rzetelne i mogą być wykorzystane do podjęcia opartej na analizie ryzyka decyzji o wdrożeniu/kontynuacji użytkowania systemu lub zabezpieczenia wspólnego.

Niezależne usługi dotyczące oceny środków bezpieczeństwa i zabezpieczeń prywatności mogą być świadczone przez jednostki w danej organizacji lub podmiot sektora publicznego czy prywatnego spoza organizacji. W szczególnych sytuacjach (np. gdy organizacja, która jest właścicielem systemu lub zabezpieczenia wspólnego jest mała lub jej struktura organizacyjna wymaga, aby ocena środków bezpieczeństwa czy zabezpieczeń prywatności została przeprowadzona przez osoby, które są częścią łańcucha rozwojowego, operacyjnego i/lub zarządu

definiowania lub zapewniania wytycznych dotyczących różnych aspektów kształcenia, szkolenia i rozwoju siły roboczej w zakresie cyberbezpieczeństwa.

[43] Zakontraktowane usługi oceny uznaje się za niezależne, jeśli właściciel systemu (lub programu) nie jest bezpośrednio zaangażowany w proces kontraktowania lub nie może w niewłaściwy sposób wpływać na niezależność oceniających przeprowadzających ocenę środków bezpieczeństwa lub zabezpieczeń prywatności.

właściciela systemu), niezależność w procesie oceny może być osiągnięta przez zapewnienie, że wyniki oceny są starannie sprawdzane i analizowane przez niezależny zespół ekspertów w celu potwierdzenia ich kompletności, spójności i prawdziwości.[44]

## 3.2. OPRACOWANIE PLANÓW OCENY ŚRODKÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Tabela 2 zawiera opis celu, ról i oczekiwanych rezultatów dla etapu: *Opracowanie planów bezpieczeństwa i ochrony prywatności.*

| **Cel** | **Cele oceny środków bezpieczeństwa i zabezpieczeń prywatności oraz szczegółowy plan dokonania takiej oceny w oparciu o plan(y) bezpieczeństwa i ochrony prywatności.** |
|---|---|
| **Role podstawowe** | Osoba oceniająca zabezpieczenia. |
| **Role pomocnicze** | Osoby odpowiedzialne za utrzymanie odpowiedniego poziomu bezpieczeństwa operacyjnego systemu informatycznego, osoby odpowiedzialne za ochronę prywatności i danych osobowych, właściciele systemu. |
| **Rezultaty** | • Określanie zabezpieczeń i zabezpieczeń rozszerzonych, które mają być uwzględnione podczas dokonywania ocen.<br>• Wybieranie i dostosowywanie procedur oceny; opracowywane są dodatkowe procedury odnośnie wymagań dotyczących bezpieczeństwa i ochrony prywatności lub środków bezpieczeństwa i zabezpieczeń prywatności nieuwzględnionych w [NSC 800-53]. |

[44] Jednostka zatwierdzająca uzgadnia z SISO, SAOP/CPO, CIO (definicja ról – patrz NSC 800-18; NSC 800-37; NSC 7298) konsekwencje wszelkich decyzji dotyczących niezależności oceniającego w szczególnych okolicznościach opisanych powyżej.

| **Cel** | **Cele oceny środków bezpieczeństwa i zabezpieczeń prywatności oraz szczegółowy plan dokonania takiej oceny w oparciu o plan(y) bezpieczeństwa i ochrony prywatności.** |
|---|---|
| | • Optymalizowanie procedur oceny w celu ograniczenia wykonywania tych samych czynności.<br>• Zakończenie prac nad przygotowaniem planu oceny i akceptacja. |

**Tabela 2. Podsumowanie etapu opracowania planów bezpieczeństwa i ochrony prywatności.**

*Plan oceny środków bezpieczeństwa* i *plan oceny ochrony prywatności* stanowią podstawę do określenia celów oceny środków bezpieczeństwa i zabezpieczeń prywatności, a także szczegółowego planu dokonania takiej oceny. Plany oceny mogą być opracowane jako jeden zintegrowany plan lub jako odrębne plany, w zależności od potrzeb organizacji. Podczas opracowywania planów oceny środków bezpieczeństwa i zabezpieczeń prywatności w systemach organizacyjnych lub zabezpieczeń wspólnych do dziedziczenia, oceniający powinni rozważyć następujące kroki:

- Określenie, które środki bezpieczeństwa i zabezpieczenia prywatności/zabezpieczenia rozszerzone należy uwzględnić przy dokonywaniu oceny, na podstawie planu bezpieczeństwa i planu ochrony prywatności (lub równoważnego dokumentu, jeżeli zabezpieczenia, które mają być ocenione, są zabezpieczeniami wspólnymi nieopartymi na systemie)[45], określenie celu i zakresu oceny.
- Wybór odpowiednich procedur oceny, które będą stosowane podczas dokonywania oceny środków bezpieczeństwa lub ochrony prywatności

[45] Opracowywanie planów oceny/ przeprowadzania oceny zabezpieczeń ma zastosowanie także do planów programów bezpieczeństwa informacji i planów programów ochrony prywatności.

oraz usprawnień środków bezpieczeństwa lub zabezpieczeń prywatności, które mają być poddane ocenie.

- Dostosowanie wybranych procedur oceny (np. wybór odpowiednich metod oceny, obiektów oraz przypisanie odpowiednich wartości).
- Opracowanie dodatkowych procedur oceny w celu uwzględnienia wszelkich wymagań środków bezpieczeństwa lub zabezpieczeń, które nie są uwzględnione w [NSC 800-53].
- Optymalizacja procedur oceny w celu ograniczenia wykonywania tych samych czynności (np. sekwencjonowanie i konsolidacja procedur oceny) i zapewnienie efektywnych kosztowo rozwiązań w zakresie oceny.
- Finalizowanie planów oceny i uzyskanie niezbędnych zgód na ich realizację.

### *3.2.1. OKREŚLENIE, KTÓRE ŚRODKI BEZPIECZEŃSTWA I ZABEZPIECZENIA PRYWATNOŚCI MAJĄ BYĆ PODDANE OCENIE*

Plan bezpieczeństwa i plan ochrony prywatności stanowią przegląd wymagań dotyczących bezpieczeństwa i ochrony prywatności dla systemu i organizacji oraz opisują sposoby przeprowadzania oceny środków bezpieczeństwa i zabezpieczeń prywatności stosowane w celu spełnienia tych wymagań.
Do dokonania oceny zabezpieczeń wspólnych, które nie są wdrożone przez system, można wykorzystać dokument równoważny planowi bezpieczeństwa lub planowi ochrony prywatności. Oceniający zaczyna od przeprowadzenia oceny środków bezpieczeństwa lub zabezpieczeń prywatności na podstawie planu bezpieczeństwa lub planu ochrony prywatności, biorąc pod uwagę cel oceny. Ocena środków bezpieczeństwa lub zabezpieczeń prywatności może być pełną oceną wszystkich zabezpieczeń w systemie (np. podczas procesu wstępnej autoryzacji systemu), częściową oceną (np. podczas rozwoju systemu w ramach ukierunkowanej oceny wynikającej ze zmian mających wpływ na określone zabezpieczenia lub gdy zabezpieczenia zostały wcześniej ocenione, a wyniki zaakceptowano w procesie wzajemności) lub oceną zabezpieczeń wspólnych.

W przypadku ocen częściowych właściciele systemów i dostawcy zabezpieczeń wspólnych współpracują z jednostkami w organizacji zainteresowanymi oceną (np. jednostkami ds. bezpieczeństwa informacji, jednostkami ds. prywatności/głównymi jednostkami ds. prywatności, osobami odpowiedzialnymi za misję/informacje, inspektorami generalnymi i jednostkami upoważniającymi) w celu określenia ocenianych zabezpieczeń. Określenie zabezpieczeń zależy od celu oceny.
Na przykład, w początkowych fazach cyklu życia systemu do oceny mogą zostać wybrane określone zabezpieczenia, aby promować wczesne wykrywanie wad i braków oraz bardziej efektywne kosztowo podejście do określania ryzyka.
Po uzyskaniu wstępnego zezwolenia na eksploatację konieczne może być przeprowadzenie ukierunkowanych ocen w przypadku wprowadzania zmian w systemie, określonych środkach bezpieczeństwa lub zabezpieczeniach prywatności, zabezpieczeniach wspólnych lub w środowisku eksploatacji. W takich przypadkach ocenia się zabezpieczenia, na które dana zmiana mogła mieć wpływ.

### *3.2.2. WYBÓR PROCEDUR OCENY ŚRODKÓW BEZPIECZEŃSTWA I ZABEZPIECZEŃ PRYWATNOŚCI*

NSC 800-53A zawiera procedury oceny dla każdego środka bezpieczeństwa i zabezpieczenia prywatności oraz zabezpieczenia rozszerzonego zawartego w [NSC 800-53]. Dla każdego zabezpieczenia w planie bezpieczeństwa i planie ochrony prywatności, które ma być objęte oceną, oceniający wybierają odpowiednią procedurę oceny z rozdziału 4. Wybrane procedury oceny mogą się różnić w zależności od planów bezpieczeństwa i planów ochrony prywatności oraz celu oceny (np. pełna ocena, częściowa ocena, ocena zabezpieczeń wspólnych).

### *3.2.3. DOSTOSOWYWANIE PROCEDUR OCENY*

W sposób podobny do tego, w jaki zabezpieczenia zawarte w [NSC 800-53] są dostosowywane do misji organizacji, jej funkcji biznesowych, charakterystyki systemu i środowiska operacyjnego, organizacje dostosowują procedury oceny zawarte w rozdziale 4 do specyficznych potrzeb organizacyjnych. Organizacje mogą przeprowadzać proces optymalizacji procedury oceny w sposób elastyczny,

na poziomie organizacji dla wszystkich systemów lub dla zabezpieczeń wspólnych, na poziomie poszczególnych systemów lub stosując kombinację podejść na poziomie organizacji i specyficznych dla danego systemu. Przed rozpoczęciem procesu optymalizacji oceniający zabezpieczenia ustalają, czy dana organizacja zapewnia dodatkowe wytyczne dotyczące optymalizacji.

Procedury oceny są dostosowywane poprzez:

- Wybór odpowiednich metod oceny i przedmiotów potrzebnych do osiągnięcia założonych celów oceny.
- Wybór odpowiednich wartości cech w celu określenia dokładności i zakresu oceny.
- Określenie zabezpieczeń wspólnych i dziedziczonych części zabezpieczeń hybrydowych, które zostały ocenione na podstawie odrębnego udokumentowanego planu oceny bezpieczeństwa lub planu oceny prywatności i nie wymagają powtórnego wykonania procedury oceny[46] .
- Opracowywanie procedur oceny specyficznych dla systemu/platformy i organizacji (które mogą być adaptacją procedur zawartych w rozdziale 4).
- Uwzględnianie wyników poprzednich ocen, w stosownym przypadku.
- Wprowadzanie odpowiednich zmian w procedurach oceny w celu uzyskania wymaganych dowodów oceny od zewnętrznych dostawców.

#### *3.2.3.1. KWESTIE ZWIĄZANE Z METODAMI I OBIEKTAMI OCENY*

Organizacje mogą w różny sposób określać, dokumentować i konfigurować swoje systemy, a zawartość i możliwość zastosowania istniejących dowodów oceny jest zróżnicowana. To zróżnicowanie może powodować konieczność stosowania różnych metod oceny w odniesieniu do obiektów oceny, w celu wygenerowania dowodów

[46] Zabezpieczenia wspólne nie są oceniane w ramach oceny zabezpieczeń systemu, chyba że zabezpieczenia wspólne są częścią systemu, który zapewnia zabezpieczenia wspólne dziedziczone przez inne systemy. Oceniający jedynie weryfikuje, czy oceniany system faktycznie dziedziczy zabezpieczenie wspólne (tzn. czy dane dziedziczone zabezpieczenie wspólne jest wykorzystywane przez oceniany system do zapewnienia ochrony) oraz czy zabezpieczenie to nie jest zaimplementowane na poziomie ocenianego systemu.

oceny niezbędnych do stwierdzenia czy środki bezpieczeństwa i zabezpieczenia prywatności są skuteczne w ich stosowaniu. Ponadto, jak opisano w rozdziale 2.3 i rozdziale 2.4, liczba i rodzaj metod oceny oraz obiektów oceny potrzebnych do uzyskania wymaganej wiarygodności różni się w zależności od szczegółowości i zakresu stosowania oceny.

Dlatego metody i przedmioty oceny dołączone do każdej procedury oceny są określane jako *potencjalne*, aby odzwierciedlić potrzebę wyboru konkretnych metod i przedmiotów najbardziej odpowiednich dla danej oceny. Wybrane metody i obiekty oceny to metody i obiekty uznane za niezbędne do uzyskania dowodów potrzebnych do dokonania określeń opisanych w stwierdzeniach określających, wspierających wymogi wiarygodności i związane z nimi zarządzanie ryzykiem. Wymienione w procedurze oceny potencjalne metody i obiekty służą jako źródło informacji pomocne w wyborze odpowiednich metod i obiektów, a nie jako narzędzie ograniczające wybór. Organizacje powinny kierować się własnym osądem przy wyborze metod oceny i związanych z nimi obiektów oceny. Organizacje wybierają te metody i obiekty, które pozwalają na najbardziej ekonomiczne zarządzanie ryzykiem i przyczyniają się do podejmowania decyzji związanych z celem oceny.[47]

Jakość wyników oceny opiera się na racjonalności uzasadnienia wyboru metod i obiektów, a nie na konkretnym zestawie zastosowanych metod i obiektów. W większości przypadków nie jest konieczne stosowanie każdej metody oceny do każdego obiektu oceny, aby uzyskać pożądaną wiarygodność.

#### *3.2.3.2. KWESTIE DOTYCZĄCE SZCZEGÓŁOWOŚCI I ZAKRESU STOSOWANIA*

Oprócz wyboru odpowiednich metod i obiektów oceny, każdej metodzie oceny (tj. badaniu, wywiadowi i testowi) przypisane są atrybuty szczegółowości i zakresu stosowania opisane w załączniku C.

[47] Wybór metod i obiektów oceny (w tym liczby i rodzaju obiektów oceny, tj. zakresu stosowania) może być istotnym czynnikiem w ekonomicznym zarządzaniu ryzykiem przy jednoczesnej realizacji celów oceny.

Wartości atrybutów określają rygor (szczegółowość) i zakres (zakres stosowania) procedur oceny przeprowadzanych przez oceniającego. Wartości wybrane przez organizację opierają się na charakterystyce ocenianego systemu (w tym na wymaganiach dotyczących wiarygodności) oraz na konkretnych ustaleniach, jakie mają być dokonane.

Wartości atrybutów szczegółowość i zakres stosowania są związane z wymaganiami wiarygodności określonymi przez organizację (tzn. rygor i zakres oceny wzrasta w bezpośrednim związku z wymaganiami dotyczącymi wiarygodności, które z kolei wzrastają w bezpośrednim związku z negatywnymi skutkami straty).

#### *3.2.3.3. KWESTIE DOTYCZĄCE ZABEZPIECZEŃ WSPÓLNYCH*

Oceniający odnotowują, które środki bezpieczeństwa i zabezpieczenia prywatności (lub części takich zabezpieczeń) w planach bezpieczeństwa lub ochrony prywatności są oznaczone jako *zabezpieczenia wspólne*.[48] Z uwagi na to, że ocena zabezpieczeń wspólnych jest obowiązkiem jednostki organizacyjnej, która opracowała i wdrożyła te zabezpieczenia (tj. dostawcy zabezpieczeń wspólnych), procedury oceny zawarte w rozdziale 4 są również wykorzystywane do oceny zabezpieczeń wspólnych. Wyniki oceny zabezpieczeń wspólnych są udostępniane systemom organizacyjnym i właścicielom systemów, którzy decydują się na dziedziczenie zabezpieczeń wspólnych.[49]

[48] Zabezpieczenia wspólne obsługują wiele systemów w organizacji, a środki ochrony zapewniane przez nie są dziedziczone przez poszczególne systemy. Dlatego też organizacja określa odpowiedni zestaw zabezpieczeń wspólnych, aby zapewnić, że zarówno siła zabezpieczeń (tj. zdolność do ochrony prywatności i ochrony), jak i poziom rygoru oraz intensywność ocen zabezpieczeń są współmierne do oceny ryzyka utraty prywatności i kategoryzacji poszczególnych systemów dziedziczących te zabezpieczenia. Wady lub braki w zabezpieczeniach wspólnych mogą potencjalnie negatywnie wpłynąć na dużą część organizacji i dlatego wymagają szczególnej uwagi.

[49] Jeśli wyniki oceny nie są obecnie dostępne dla zabezpieczeń wspólnych, należy odpowiednio odnotować plany oceny dla ocenianych systemów, które zależą od tych zabezpieczeń. Oceny nie można uznać za kompletną, dopóki wyniki oceny zabezpieczeń wspólnych nie zostaną udostępnione właścicielom systemu.

Innym czynnikiem branym pod uwagę przy ocenie zabezpieczeń wspólnych jest znajomość specyficznych dla danego systemu aspektów zabezpieczeń, które nie są objęte zakresem działania jednostek organizacyjnych odpowiedzialnych za wspólne aspekty zabezpieczeń. Takie zabezpieczenia są określane mianem *zabezpieczeń hybrydowych*. Na przykład, CP-02, plan ciągłości działania, może być uważany przez organizację za zabezpieczenie hybrydowe, o ile organizacja posiada plan awaryjny opracowany dla wszystkich systemów organizacyjnych. Od właścicieli systemów oczekuje się, że dostosują opracowany przez organizację plan awaryjny, jeśli istnieją specyficzne aspekty planu, które muszą być zdefiniowane dla konkretnego systemu, w którym zastosowano zabezpieczenie. Dla każdego zabezpieczenia hybrydowego oceniający włączają do planów oceny bezpieczeństwa lub planów oceny ochrony prywatności te części procedur oceny z rozdziału 4 , które odnoszą się do tych części zabezpieczenia, które są specyficzne dla danego systemu, aby zapewnić, że wraz z wynikami ocen zabezpieczeń wspólnych, oceniane są wszystkie ich aspekty.

### OCENA ZABEZPIECZEŃ WSPÓLNYCH I CZĘŚCI ZABEZPIECZEŃ HYBRYDOWYCH DZIEDZICZONYCH OD DOSTAWCY ZABEZPIECZEŃ WSPÓLNYCH

W planach bezpieczeństwa i ochrony prywatności systemu zabezpieczenia wspólne lub części zabezpieczeń hybrydowych wdrożonych i utrzymywanych przez dostawcę zabezpieczeń wspólnych są określane jako „dziedziczone” z odniesieniem do dostawcy zabezpieczeń wspólnych. Właściciel systemu nie jest odpowiedzialny za ocenę zabezpieczeń wspólnych ani dziedziczonej części zabezpieczeń hybrydowych. Zabezpieczenia wspólne są oceniane oddzielnie i nie są ponownie oceniane na poziomie systemu przez każdy system, który je dziedziczy. Oceniający sprawdza jednak, czy system rzeczywiście dziedziczy i wykorzystuje zabezpieczenie wspólne, jak wskazano w planach bezpieczeństwa i ochrony prywatności systemu. Ocena zabezpieczeń wspólnych (dla dostawcy zabezpieczeń wspólnych) jest przeprowadzana przy użyciu tego samego procesu, co w przypadku oceny zabezpieczeń systemu.

#### *3.2.3.4. KWESTIE ZWIĄZANE Z SYSTEMEM/PLATFORMĄ I ORGANIZACJĄ*

Procedury oceny zawarte w NSC 800-53A mogą być dostosowane do zależności specyficznych dla systemu, platformy lub organizacji. Na przykład, ocena wdrożenia zabezpieczenia IA-02 w systemie Linux w zakresie identyfikacji i uwierzytelniania użytkowników może obejmować wyraźne zbadanie możliwości logowania bez hasła i potencjalnego ryzyka wynikającego z braków w zarządzaniu kluczami, zarządzaniu kontami, ochronie systemu i granic systemu, ochronie fizycznej i środowiskowej oraz innych zabezpieczeniach uniemożliwiających ominięcie identyfikacji i uwierzytelniania przez nieuprawnionych użytkowników lub procesy działające w imieniu użytkowników.

#### *3.2.3.5. KWESTIE ZWIĄZANE Z PONOWNYM WYKORZYSTANIEM DOWODÓW OCENY*

Ponowne wykorzystanie wyników oceny z wcześniej zaakceptowanych lub zatwierdzonych ocen jest uwzględniane w materiale dowodowym służącym do określenia ogólnej skuteczności środków bezpieczeństwa i zabezpieczeń prywatności.

Wcześniej zaakceptowane lub zatwierdzone oceny obejmują oceny dziedziczonych zabezpieczeń wspólnych, które są zarządzane przez organizację i wspierają wiele systemów, oceny środków bezpieczeństwa lub zabezpieczeń prywatności, które są poddawane przeglądowi jako część wdrożenia zabezpieczenia (np. CP-02 wymaga przeglądu planu awaryjnego), lub informacje związane z bezpieczeństwem generowane przez program strategii ciągłego monitorowania bezpieczeństwa informacji w organizacji (*ang. Information Security Continuous Monitoring – ISCM*). Dopuszczalność ponownego wykorzystania wyników oceny w ramach oceny środków bezpieczeństwa lub zabezpieczeń prywatności jest uzgadniana z osobami korzystającymi z wyników oceny i przez nie zatwierdzana. Istotne jest, aby właściciele systemów i dostawcy zabezpieczeń wspólnych współpracowali z osobami autoryzującymi i innymi właściwymi pracownikami organizacji w celu określenia dopuszczalności wykorzystania wyników poprzedniej oceny. Rozważając

ponowne wykorzystanie wyników oceny oraz ich znaczenie dla bieżącej oceny, oceniający określają wiarygodność dowodów z oceny, adekwatność wcześniejszej analizy oraz możliwość zastosowania dowodów z oceny do bieżących warunków pracy systemu. Jeśli wyniki poprzedniej oceny są ponownie wykorzystywane, data i rodzaj pierwotnej oceny muszą zostać udokumentowane w planie oceny i raporcie z oceny.

W niektórych sytuacjach może być konieczne uzupełnienie wcześniejszych wyników oceny, których ponowne wykorzystanie jest rozważane, o dodatkowe działania oceniające, aby w pełni uwzględnić bieżące cele oceny. Na przykład, jeśli w niezależnej ocenie produktu informatycznego nie przetestowano określonego ustawienia konfiguracji, które jest stosowane przez organizację w systemie, wówczas oceniający może być zmuszony do uzupełnienia pierwotnych wyników testów o dodatkowe testy obejmujące to ustawienie konfiguracji w bieżącym środowisku systemowym. Decyzja o ponownym wykorzystaniu wyników oceny powinna zostać udokumentowana w planie oceny bezpieczeństwa lub planie oceny ochrony prywatności oraz w końcowym raporcie z oceny bezpieczeństwa lub raporcie z oceny ochrony prywatności. Także powinna być zgodna z ustawodawstwem, zasadami, dyrektywami, standardami i wytycznymi.

Podczas walidacji wyników poprzedniej oceny w celu ponownego wykorzystania bierze się pod uwagę następujące elementy:

- **Zmieniające się w czasie warunki związane z środkami bezpieczeństwa i zabezpieczeniami prywatności**. Środki bezpieczeństwa i zabezpieczenia prywatności, które zostały uznane za skuteczne podczas poprzednich ocen, mogą okazać się nieskuteczne ze względu na zmieniające się warunki w systemie lub jego środowisku eksploatacji, w tym pojawiające się informacje o zagrożeniach. Wyniki oceny, które wcześniej zostały uznane za akceptowalne, mogą nie stanowić już wiarygodnego dowodu na określenie skuteczności środków bezpieczeństwa lub zabezpieczeń prywatności, dlatego może być wymagane ponowne przeprowadzenie oceny. Zastosowanie wyników poprzedniej oceny

do bieżącej oceny wymaga określenia wszelkich zmian, które zaszły od czasu przeprowadzenia poprzedniej oceny, oraz wpływu tych zmian na poprzednie wyniki. Na przykład, ponowne wykorzystanie wyników poprzedniej oceny w ramach badania zasad i procedur bezpieczeństwa lub ochrony prywatności organizacji może być dopuszczalne, jeśli zostanie stwierdzone, że nie nastąpiły żadne znaczące zmiany w zidentyfikowanych zasadach i procedurach. Ponowne wykorzystanie wyników oceny uzyskanych podczas poprzedniej autoryzacji systemu jest ekonomiczną metodą wspierania działań związanych z ciągłym monitorowaniem i spełniania wymogów rocznego raportowania, jeśli związane z nimi zabezpieczenia nie uległy zmianie i istnieją odpowiednie podstawy, aby być pewnym co do ich zastosowania.

- C**zas, jaki upłynął od przeprowadzenia poprzednich ocen**. Ogólnie rzecz biorąc, wraz z upływem czasu między przeprowadzeniem bieżącej i poprzedniej oceny maleje wiarygodność i użyteczność wyników poprzedniej oceny. Dzieje się tak przede wszystkim dlatego, że jest wysoce prawdopodobne, iż system lub środowisko, w którym on działa, ulegnie zmianie wraz z upływem czasu, co może unieważnić pierwotne warunki lub założenia, na których oparto poprzednią ocenę.
- **Stopień niezależności poprzednich ocen**. Niezależność oceniającego może być czynnikiem krytycznym w przypadku niektórych rodzajów ocen. Stopień niezależności wymagany przy poszczególnych ocenach powinien być spójny. Na przykład, nie zaleca się ponownego wykorzystania wyników poprzedniej samooceny, w której nie wymagano niezależności oceniającego, gdy obecna ocena wymaga większego stopnia niezależności.

#### *3.2.3.6. KWESTIE ZWIĄZANE Z SYSTEMEM ZEWNĘTRZNYM*

Procedury oceny opisane w rozdziale 4 muszą być odpowiednio dostosowane do potrzeb oceny systemów zewnętrznych.[50] Z uwagi na to, że organizacja nie zawsze ma bezpośrednią kontrolę nad środkami bezpieczeństwa lub zabezpieczeniami prywatności stosowanymi w systemach zewnętrznych lub wystarczający wgląd w rozwój, wdrażanie i ocenę tych zabezpieczeń, konieczne może być zastosowanie alternatywnych podejść do oceny, co powoduje konieczność dostosowania procedur oceny opisanych w rozdziale 4. Jeśli wymagania dotyczące zapewnienia uzgodnionych środków bezpieczeństwa lub zabezpieczeń prywatności w systemie są udokumentowane w umowach lub porozumieniach o poziomie usług, oceniający dokonują przeglądu tych umów lub porozumień i odpowiednio dostosowują procedury oceny do oceny środków bezpieczeństwa lub zabezpieczeń prywatności lub wyników oceny środków bezpieczeństwa i zabezpieczeń prywatności przedstawionych w umowach lub porozumieniach. Ponadto oceniający biorą pod uwagę wszelkie inne oceny, które zostały przeprowadzone lub są w trakcie przeprowadzania dla systemów zewnętrznych, na których można polegać w odniesieniu do bezpieczeństwa ocenianego systemu. Istotne informacje pochodzące z tych ocen, o ile zostaną uznane za wiarygodne, są włączane odpowiednio do sprawozdania z oceny bezpieczeństwa lub sprawozdania z oceny ochrony prywatności.

### *3.2.4. OPRACOWYWANIE PROCEDUR OCENY ZABEZPIECZEŃ SPECYFICZNYCH DLA DANEJ ORGANIZACJI*

W oparciu o zasady organizacji, wymagania misji lub funkcji biznesowych oraz ocenę ryzyka, organizacje mogą zdecydować się na opracowanie i wdrożenie

[50] System zewnętrzny to system lub komponent systemu, który znajduje się poza granicą autoryzacji ustanowioną przez organizację i nad którym organizacja zazwyczaj nie ma bezpośredniej kontroli w zakresie stosowania wymaganych środków bezpieczeństwa i zabezpieczeń prywatności lub oceny skuteczności zabezpieczeń. [NSC 800-37] i [NSC 800-53] zawierają dodatkowe wytyczne dotyczące systemów zewnętrznych oraz skutków stosowania środków bezpieczeństwa i zabezpieczeń prywatności w środowiskach zewnętrznych.

dodatkowych (specyficznych dla danej organizacji) zabezpieczeń lub zabezpieczeń rozszerzonych dla swoich systemów, które wykraczają poza zakres [NSC 800-53].

Takie zabezpieczenia zostaną udokumentowane w planie bezpieczeństwa i planie ochrony prywatności jako zabezpieczenia niewystępujące w NSC 800-53. Aby ocenić zabezpieczenia niewystępujące w NSC 800-53, oceniający do opracowania procedur oceny dla tych zabezpieczeń i zabezpieczeń rozszerzonych powinni wykorzystać wytyczne zawarte w rozdziale 2. Opracowane procedury oceny są następnie włączane do planu oceny, stosownie do potrzeb.

### *3.2.5. OPTYMALIZACJA WYBRANYCH PROCEDUR OCENY W CELU ZAPEWNIENIA MAKSYMALNEJ SKUTECZNOŚCI*

Oceniający mogą elastycznie organizować plany oceny, które odpowiadają potrzebom organizacji i zapewniają najlepszą możliwość uzyskania dowodów niezbędnych do określenia skuteczności środków bezpieczeństwa lub zabezpieczeń prywatności przy jednoczesnym obniżeniu ogólnych kosztów oceny. Łączenie i konsolidacja procedur oceny to jeden z obszarów cechujących się elastycznością. Podczas oceny systemu wielokrotnie stosuje się metody oceny w odniesieniu do różnych obiektów oceny w ramach danej kategorii zabezpieczeń. Aby zaoszczędzić czas, zmniejszyć koszty oceny i zmaksymalizować przydatność wyników oceny, oceniający dokonują przeglądu wybranych procedur oceny dla kategorii zabezpieczeń i łączą lub konsolidują procedury (lub części procedur), gdy tylko jest to możliwe lub wykonalne. Przykładowo, oceniający mogą skonsolidować wywiady z kluczowymi pracownikami organizacji, którzy zajmują się różnymi zagadnieniami związanymi z bezpieczeństwem lub ochroną prywatności. Oceniający mogą mieć także inne możliwości dokonania znaczącej konsolidacji i obniżenia kosztów poprzez jednoczesne badanie wszystkich zasad i procedur z kategorii środków bezpieczeństwa i zabezpieczeń prywatności lub poprzez organizowanie grup powiązanych zasad i procedur, które mogą być badane jako jednolita całość. Uzyskanie i zbadanie ustawień konfiguracyjnych z podobnych komponentów

sprzętu i oprogramowania w systemie to kolejny przykład, który może znacznie usprawnić proces oceny.

Dodatkowym obszarem do rozważenia przy optymalizacji procesu oceny jest kolejność, w jakiej oceniane są zabezpieczenia. Ocena niektórych zabezpieczeń przed innymi może dostarczyć przydatnych informacji, które ułatwią zrozumienie i bardziej efektywną ocenę pozostałych zabezpieczeń. Na przykład, zabezpieczenia takie jak CM-2 (Konfiguracja podstawowa), CM-8 (Inwentaryzacja komponentów systemu), PL-2 (Plany bezpieczeństwa systemu i ochrony prywatności), RA-2 (Kategoryzacja bezpieczeństwa) i RA-3 (Szacowanie ryzyka) tworzą ogólne opisy systemu. Ocena powiązanych zabezpieczeń na wczesnym etapie procesu oceny może zapewnić podstawowe zrozumienie systemu, które może pomóc w ocenie innych zabezpieczeń. W NSC 800-53, w sekcji *Omówienie*, dla każdego zabezpieczenia określono *Zabezpieczenia powiązane*, które mogą dostarczyć informacji przydatnych przy organizowaniu procedur oceny. Na przykład, AC-19 (Kontrola dostępu do urządzeń przenośnych) wymienia zabezpieczenia MP-4 (Przechowywanie nośników danych) i MP-5 (Transport nośników danych) jako powiązane z AC-19. Ponieważ AC-19 jest powiązane z MP-4 i MP-5, odpowiednia kolejność przeprowadzenia oceny dla AC-19, MP-4 i MP-5 może ułatwić ponowne wykorzystanie informacji uzyskanych w ramach oceny jednego zabezpieczenia do oceny innych, powiązanych z nim zabezpieczeń.

### *3.2.6. FINALIZOWANIE PLANU OCENY I UZYSKANIE ZGODY NA JEGO REALIZACJĘ*

Po wybraniu procedur oceny (w tym opracowaniu niezbędnych metod nie zawartych w katalogu procedur NSC 800-53A), dostosowaniu procedur do warunków specyficznych dla systemu/platformy i organizacji, optymalizacji procedur pod kątem efektywności oraz uwzględnieniu możliwości wystąpienia nieoczekiwanych zdarzeń, które mogą mieć wpływ na ocenę, następuje finalizacja planu oceny i ustalenie harmonogramu, w tym kluczowych etapów procesu oceny. Po sporządzeniu planu oceny, plan jest przeglądany i zatwierdzany przez

odpowiednich pracowników organizacji[51] w celu zagwarantowania, że jest on kompletny, zgodny z celami organizacji w zakresie bezpieczeństwa i ochrony prywatności oraz z dokonaną przez organizację oceną ryzyka, a także w sposób ekonomiczny pozwala zarządzać ryzykiem w odniesieniu do metod i obiektów oceny, atrybutów szczegółowości i zakresu stosowania oraz zasobów przeznaczonych na przeprowadzenie oceny.

## 3.3. PRZEPROWADZANIE OCEN ŚRODKÓW BEZPIECZEŃSTWA I ZABEZPIECZEŃ PRYWATNOŚCI

Tabela 3 przedstawia podsumowanie celu, ról i oczekiwanych rezultatów etapu pt. *Przeprowadzenie oceny środków bezpieczeństwa i zabezpieczeń prywatności*.

| **Cel** | **Przeprowadzenie oceny środków bezpieczeństwa i zabezpieczeń prywatności zgodnie z planem oceny oraz udokumentowanie wyników w raporcie (raportach) z oceny środków bezpieczeństwa i zabezpieczeń prywatności.** |
|---|---|
| **Role podstawowe** | Osoba oceniająca zabezpieczenia. |
| **Role pomocnicze** | SSO i SPO, właściciele systemu, inżynierowie bezpieczeństwa systemów i ochrony prywatności i danych osobowych, architekci bezpieczeństwa informacji oraz architekci ochrony prywatności i ochrony danych osobowych, administratorzy systemu, użytkownicy systemu.[52] |

[51] Organizacje ustanawiają proces zatwierdzania planu oceny bezpieczeństwa i zabezpieczeń prywatności z udziałem określonych osób należących do organizacji (np. właścicieli systemu, dostawców zabezpieczeń wspólnych, SSO i SPO, SISO, SAOP/inspektorów ochrony danych, osób autoryzujących) wyznaczonych jako organy zatwierdzające.

[52] Definicja ról – patrz NSC 800-18; NSC 800-37; NSC 7298.

| | |
|---|---|
| **Cel** | **Przeprowadzenie oceny środków bezpieczeństwa i zabezpieczeń prywatności zgodnie z planem oceny oraz udokumentowanie wyników w raporcie (raportach) z oceny środków bezpieczeństwa i zabezpieczeń prywatności.** |
| **Rezultaty** | • Zabezpieczenia objęte zakresem i zabezpieczenia rozszerzone są oceniane zgodnie z planem(-ami) oceny bezpieczeństwa i ochrony prywatności.<br>• Opracowanie raportów z oceny bezpieczeństwa i ochrony prywatności dokumentujące skuteczność zabezpieczeń oraz zidentyfikowane wady/braki. |

**Tabela 3. Podsumowanie etapu przeprowadzenia oceny środków bezpieczeństwa i zabezpieczeń prywatności.**

Po zatwierdzeniu planu oceny przez organizację, oceniający lub zespół ds. oceny realizuje/realizują plan zgodnie z przyjętym harmonogramem. Określenie wielkości i składu organizacyjnego zespołu ds. oceny (tj. umiejętności, wiedzy technicznej i doświadczenia w zakresie przeprowadzania oceny posiadanych przez osoby wchodzące w skład zespołu) jest jedną z decyzji dotyczących zarządzania ryzykiem podejmowanych przez organizację wnioskującą o przeprowadzenie oceny i inicjującą ją. Wyniki oceny zabezpieczeń są dokumentowane w raportach z oceny, które są kluczowymi elementami pakietu autoryzacyjnego opracowywanego przez właścicieli systemu i dostawców zabezpieczeń wspólnych dla osób autoryzujących.[53] Raporty z oceny zawierają informacje od osób oceniających (w formie ustaleń z oceny), które są niezbędne do określenia skuteczności środków bezpieczeństwa i zabezpieczeń prywatności zastosowanych w systemie.[54] Raporty

[53] Zgodnie z [NSC 800-37], pakiet autoryzacyjny składa się z planu bezpieczeństwa, planu ochrony prywatności, raportu z oceny bezpieczeństwa, raportu z oceny prywatności oraz planu i etapów działania (*ang. Plan Of Action And Milestones - POA&M*).

[54] Dodatkowe informacje na temat oceny zabezpieczeń wspólnych i części zabezpieczeń hybrydowych dziedziczonych od dostawcy zabezpieczeń wspólnych znajdują się w rozdziale 3.2.3.

z oceny są ważnym czynnikiem w określaniu ryzyka przez osobę zatwierdzającą. Organizacje mogą zdecydować się na opracowanie podsumowania oceny na podstawie szczegółowych ustaleń, które są generowane przez osoby oceniające podczas oceny środków bezpieczeństwa i oceny zabezpieczeń prywatności. Podsumowanie oceny może stanowić dla osoby zatwierdzającej skróconą wersję raportu z oceny, skoncentrowaną na najważniejszych elementach oceny, streszczeniu najważniejszych ustaleń i zaleceniach dotyczących wyeliminowania wad i braków w ocenianych środkach bezpieczeństwa lub zabezpieczeniach prywatności. Załącznik E zawiera informacje na temat zalecanej zawartości raportów z oceny.

Cele oceny osiąga się dzięki zastosowaniu wyznaczonych metod oceny do wybranych przedmiotów oceny oraz zebraniu lub przedstawieniu dowodów niezbędnych do dokonania ustalenia związanego z każdym celem oceny. Każde ustalenie[55] zawarte w procedurze oceny przeprowadzonej przez oceniającego prowadzi do jednego z następujących ustaleń:

- satysfakcjonujące/osiągnięte (S) albo
- niesatysfakcjonujące/nieosiągnięte (N).

Stwierdzenie, że cel został osiągnięty oznacza, że - dla części zabezpieczenia, którego dotyczy ustalenie – cel oceny dla zabezpieczenia został osiągnięty i daje w pełni akceptowalny wynik.

Stwierdzenie, że cel nie został osiągnięty (nieosiągnięty) wskazuje – dla części zabezpieczenia, którego dotyczy ustalenie – na potencjalne nieprawidłowości w działaniu lub wdrożeniu zabezpieczenia, które mogą wymagać eliminacji przez organizację. Stwierdzenie, że cel nie został osiągnięty może również wskazywać, że oceniający nie był w stanie uzyskać informacji wystarczających do dokonania ustaleń wymaganych w oświadczeniu o ustaleniu stanu faktycznego z powodów określonych w raporcie z oceny. W przypadku ustaleń oceny wskazującej, że cel

[55] Dodatkowe informacje na temat ustaleń i wyników oceny znajdują się w załączniku E.

nie został osiągnięty, organizacje mogą zdecydować się na zdefiniowanie podkategorii ustaleń wskazujących na dotkliwość i/lub krytyczność wykrytych wad lub braków oraz potencjalne negatywne skutki dla działalności organizacji (tj. kluczowych działań, funkcjonowania, wizerunku lub reputacji), aktywów organizacji, osób fizycznych, innych organizacji lub państwa. Zdefiniowanie takich podkategorii może pomóc w ustaleniu priorytetów dla niezbędnych działań ograniczających ryzyko.

Ustalenia oceniającego są bezstronnym, rzeczowym sprawozdaniem z tego, co zostało stwierdzone w odniesieniu do ocenianego zabezpieczenia. Dla każdego stwierdzenia, że cel nie został osiągnięty oceniający wskazują, na które części zabezpieczeń dane ustalenie ma wpływ (tj. aspekty zabezpieczeń, które zostały uznane za nieosiągnięte lub nie mogły zostać ocenione) i opisują, jak rzeczywisty stan zabezpieczeń różni się od stanu planowanego lub oczekiwanego/pożądanego. Potencjalne zagrożenia dla poufności, integralności, i dostępności lub ryzyka utraty prywatności wynikające ze stwierdzenia, że cel nie został osiągnięty, są również odnotowywane przez oceniającego w raporcie z oceny.

Działania związane z określaniem i akceptacją ryzyka są prowadzone przez organizację po dokonaniu oceny jako część strategii zarządzania ryzykiem ustalonej przez organizację. W działania związane z zarządzaniem ryzykiem po dokonaniu oceny zaangażowane jest kierownictwo wyższego szczebla organizacji, np. kierownik jednostki organizacyjnej, właściciel misji/biznesu, IO/S, RE, oraz AO w porozumieniu z odpowiednim personelem pomocniczym organizacji (np. SISO, SAOP/inspektorzy ochrony danych, CIO, właściciele systemu, dostawcy zabezpieczeń wspólnych oraz oceniający).[56]

Wyniki oceny kontroli środków bezpieczeństwa i zabezpieczeń prywatności są udokumentowane na poziomie szczegółowości odpowiednim dla danej oceny zgodnie z formatem raportowania określonym w zasadach organizacji

[56] Definicja ról – patrz NSC 800-18; NSC 800-37; NSC 7298.

i rekomendacjach NSC. Format raportowania jest odpowiedni do rodzaju przeprowadzanej oceny (np. samoocena dokonywana przez właścicieli systemu i dostawców zabezpieczeń wspólnych, niezależna weryfikacja i walidacja, niezależne oceny wspierające proces autoryzacji, oceny automatyczne, niezależne audyty lub inspekcje).

Właściciele systemu i dostawcy zabezpieczeń wspólnych polegają na fachowej wiedzy i ocenie osób przeprowadzających kontrolę, którzy oceniają mechanizmy środków bezpieczeństwa i ochrony prywatności w systemie i dziedziczone przez system oraz przedstawiają zalecenia dotyczące dalszego postępowania na podstawie wyników oceny zabezpieczeń (np. akceptują ryzyko, odrzucają ryzyko, ograniczają ryzyko poprzez usunięcie wad lub braków w zabezpieczeniach oraz zmniejszenie lub wyeliminowanie zidentyfikowanych podatności).

Wyniki oceny opracowane przez oceniającego (tj. wnioski „satysfakcjonujący" lub „niesatysfakcjonujący", identyfikacja elementów środka bezpieczeństwa lub zabezpieczenia prywatności, który nie dał zadowalającego wyniku, oraz opis wynikających z tego potencjalnych zagrożeń dla systemu lub jego środowiska eksploatacji) są przekazywane właścicielom systemu i dostawcom zabezpieczeń wspólnych we wstępnych raportach z oceny środków bezpieczeństwa i raportach z oceny ochrony prywatności.

Właściciele systemów i dostawcy zabezpieczeń wspólnych mogą zdecydować się na działanie zgodnie z zaleceniami oceniającego przed skompletowaniem raportów z oceny, jeśli istnieją konkretne możliwości skorygowania wad lub braków w zakresie środków bezpieczeństwa lub zabezpieczeń prywatności albo skorygowania i/lub wyjaśnienia nieporozumień lub interpretacji wyników oceny.[57] Środki bezpieczeństwa lub ochrony prywatności, które zostały

[57] Korekta wad lub braków w zakresie środków bezpieczeństwa lub zabezpieczeń prywatności lub realizacja zaleceń po wstępnej analizie sprawozdań z oceny środków bezpieczeństwa lub ochrony prywatności przez właścicieli systemów lub dostawców zabezpieczeń wspólnych nie mają na celu zastąpienia formalnego procesu reagowania na ryzyko, który ma miejsce po dostarczeniu sprawozdań końcowych. Jest to raczej okazja dla właściciela systemu lub dostawcy zabezpieczeń wspólnych do zajęcia się wadami lub brakami, które mogą być szybko skorygowane. Jednak w sytuacjach, gdy istnieją

zmodyfikowane w trakcie tego procesu, są ponownie oceniane przez oceniającego przed sporządzeniem końcowych raportów z oceny.

### 3.4. ANALIZA WYNIKÓW PRZEDSTAWIONYCH W RAPORCIE Z OCENY

Tabela 4 zawiera podsumowanie celu, ról i oczekiwanych rezultatów etapu: *Analiza wyników przedstawionych w raporcie z oceny*.

| | |
|---|---|
| **Cel** | **Analiza ryzyka wynikającego ze zidentyfikowanych wad i braków w zakresie zabezpieczeń oraz określenie podejścia do reagowania na ryzyko zgodnie z priorytetami organizacji** |
| **Role podstawowe** | Właściciele systemu lub dostawcy zabezpieczeń wspólnych, jednostki zatwierdzające. |
| **Role pomocnicze** | Osoby odpowiedzialne za bezpieczeństwo systemów i za ochronę prywatności, inżynierowie ds. bezpieczeństwa i prywatności, architekci ds. prywatności i ochrony danych osobowych. |
| **Rezultaty** | • Analiza wyników oceny zabezpieczeń.<br>• Podejmowanie kolejnych działań w celu zarządzania ryzykiem.<br>• Aktualizacja artefaktów pakietu autoryzacyjnego (np. plany bezpieczeństwa i ochrony prywatności, sprawozdania z oceny środków bezpieczeństwa i ochrony prywatności oraz plany działania i kluczowe punkty) w celu odzwierciedlenia aktualnego stanu systemu lub zabezpieczeń wspólnych |

**Tabela 4. Podsumowanie wyników przedstawionych w raporcie z oceny.**

Wyniki oceny zabezpieczeń ostatecznie wpływają na wdrożenie zabezpieczeń, treść planów bezpieczeństwa i planów ochrony prywatności oraz odpowiednich planów

ograniczone zasoby na naprawę wad i braków wykrytych podczas oceny środków bezpieczeństwa lub zabezpieczeń prywatności, organizacje mogą zdecydować, że czekanie na ostateczną ocenę ryzyka w celu ustalenia priorytetów działań naprawczych jest lepszym rozwiązaniem.

i etapów działania. Wyniki oceny środków bezpieczeństwa ostatecznie wpływają na wdrożenie środków bezpieczeństwa, treść planów bezpieczeństwa i planów ochrony prywatności oraz odpowiednich planów i etapów działania. W związku z tym właściciele systemu i dostawcy zabezpieczeń wspólnych dokonują przeglądu raportów z oceny bezpieczeństwa, raportów z oceny ochrony prywatności oraz zaktualizowanej dokumentacji i artefaktów oceny ryzyka, a następnie - w porozumieniu z wyznaczonymi osobami z organizacji (np. osobami autoryzującymi, CIO, SISO, SAOP/inspektorem ochrony danych, właścicielem informacji lub władającym informacją) – określają odpowiednie działania, które należy podjąć w odpowiedzi na wady i braki stwierdzone podczas oceny. Dzięki zastosowaniu oznaczeń „osiągnięty" i „nieosiągnięty" format raportowania wyników oceny zapewnia osobom z organizacji wgląd w konkretne wady i braki w zakresie środków bezpieczeństwa lub zabezpieczeń prywatności w ramach systemu lub dziedziczone przez system oraz ułatwia zdyscyplinowane i zorganizowane podejście do reagowania na ryzyko zgodnie z priorytetami organizacyjnymi. Na przykład, właściciele systemu lub dostawcy zabezpieczeń wspólnych w porozumieniu z wyznaczonymi osobami z organizacji mogą zdecydować, że pewne ustalenia oceny oznaczone jako „nieosiągnięte" nie stanowią istotnego ryzyka dla organizacji i mogą zostać zaakceptowane. Z drugiej strony właściciele systemów lub dostawcy zabezpieczeń wspólnych mogą zdecydować, że niektóre ustalenia oznaczone jako „nieosiągnięte" są istotne i wymagają działań naprawczych. We wszystkich przypadkach organizacja dokonuje przeglądu każdego ustalenia oceny „nieosiągnięte" i stosuje swój osąd w odniesieniu do wagi ustalenia oraz tego, czy jest ono na tyle istotne, aby uzasadniać dalsze badanie lub działania naprawcze[58].

Zaangażowanie kierownictwa wyższego szczebla w proces ograniczania ryzyka może być konieczne w celu zapewnienia efektywnej alokacji zasobów organizacji

[58] Potencjalne działania w odpowiedzi na ryzyko obejmują akceptację ryzyka, ograniczanie ryzyka, odrzucenie ryzyka oraz transfer/dzielenie ryzyka. [NSC 800-39] zawiera wytyczne dotyczące działań podejmowanych w odpowiedzi na ryzyko z perspektywy zarządzania ryzykiem.

zgodnie z jej priorytetami, zapewnienia w pierwszej kolejności zasobów dla systemów, które wspierają najbardziej krytyczne i wrażliwe misje organizacji, lub usunięcia braków, które stwarzają największe ryzyko. Ostatecznie wyniki oceny i wszelkie późniejsze działania naprawcze (oparte na zaktualizowanej ocenie ryzyka) powodują aktualizację kluczowych artefaktów wykorzystywanych przez osoby autoryzujące do określania ryzyka związanego z bezpieczeństwem i ochroną prywatności systemu oraz jego zdatności do uzyskania zezwolenia na działanie. Artefakty te obejmują plany bezpieczeństwa i plany ochrony prywatności, raporty z oceny bezpieczeństwa i prywatności oraz odpowiednie plany i etapy działania.

## 3.5. OCENA ZDOLNOŚCI DO ZAPEWNIENIA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Zgodnie z [NSC 800-53], organizacje mogą zdefiniować zestaw zdolności do zapewnienia bezpieczeństwa (*ang. security capabilities*) i do ochrony prywatności (*ang. privacy capabilities*) jako prekursor procesu wyboru środków bezpieczeństwa i zabezpieczeń prywatności.

W pojęciu zdolności[59] uznaje się, że ochrona prywatności osób fizycznych i informacji przetwarzanych przez systemy rzadko wynika z pojedynczego zabezpieczenia lub środka zaradczego w zakresie bezpieczeństwa lub ochrony prywatności. W większości przypadków taka ochrona wynika z wyboru i wdrożenia zestawu wzajemnie wzmacniających się środków bezpieczeństwa i ochrony prywatności. Każde zabezpieczenie przyczynia się do ogólnej zdolności zdefiniowanej przez organizację, przy czym niektóre zabezpieczenia potencjalnie przyczyniają się w większym stopniu, a inne w mniejszym stopniu. Przykładowo, organizacje mogą chcieć zdefiniować zdolność bezpiecznego uwierzytelniania

[59] Zdolność do ochrony lub zdolność do ochrony prywatności to połączenie wzajemnie wzmacniających się środków bezpieczeństwa lub zabezpieczeń prywatności (tj. zabezpieczeń i środków zaradczych) wdrażanych za pomocą środków technicznych (tj. funkcjonalności sprzętu, oprogramowania użytkowego i oprogramowania układowego), środków fizycznych (tj. urządzeń fizycznych i środków ochronnych) oraz środków proceduralnych (tj. procedur wykonywanych przez osoby fizyczne).

zdalnego, którą można osiągnąć poprzez wdrożenie zestawu środków bezpieczeństwa z NSC 800-53 (np. IA-02(01), IA-02(02), IA-02(08)], czy SC-08(01)).

Zdolność do zapewnienia bezpieczeństwa i zdolność do ochrony prywatności mogą dotyczyć różnych obszarów, w tym środków technicznych, środków fizycznych, środków proceduralnych lub dowolnej ich kombinacji. Stosując koncepcję zdolności, organizacje mogą uzyskać większą przejrzystość i lepsze zrozumienie związków (tj. zależności) między zabezpieczeniami, wpływu poszczególnych błędów w zabezpieczeniach na zdolności zdefiniowane przez organizację oraz potencjalnej dotkliwości wad lub braków w zakresie zabezpieczeń. Jednak w sytuacji, gdy na określone zdolności mają wpływ niepowodzenia poszczególnych zabezpieczeń i ochrony prywatności, podejście oparte na analizie zdolności może zwiększyć złożoność ocen i wymagać analizy przyczyn źródłowych niepowodzenia w celu określenia, które zabezpieczenie lub zabezpieczenia przyczynia(ją) się do niepowodzenia. Im większa liczba zabezpieczeń wchodzi w skład zdolności zdefiniowanej przez organizację, tym trudniejsze może być ustalenie pierwotnej przyczyny niepowodzeń. Między określonymi zdolnościami mogą również występować interakcje, co może przyczynić się do złożoności ocen. Jeśli okaże się, że zabezpieczenie nie przyczynia się ani do osiągnięcia zdefiniowanej zdolności, ani do ogólnego bezpieczeństwa i ochrony prywatności systemu, organizacja powraca do etapu wyboru ram zarządzania ryzykiem (RMF), dostosowuje zestaw zabezpieczeń i dokumentuje uzasadnienie w planie bezpieczeństwa systemu lub planie ochrony prywatności.

Tradycyjnie oceny przeprowadza się dla każdego zabezpieczenia z osobna, a ich wyniki określa się jako pozytywne (tzn. wymagania ws. zabezpieczenia spełnione) lub negatywne (tzn. wymagania ws. zabezpieczenia niespełnione). Jednakże niepowodzenie pojedynczego zabezpieczenia lub w niektórych przypadkach, niepowodzenie wielu zabezpieczeń może nie mieć wpływu na ogólną zdolność w zakresie ochrony prywatności i bezpieczeństwa wymaganą przez organizację. Nie oznacza to, że takie zabezpieczenia nie przyczyniają się do zapewnienia bezpieczeństwa lub ochrony prywatności systemu lub organizacji

(zgodnie z definicjami zawartymi w wymaganiach dotyczących bezpieczeństwa i ochrony prywatności w fazie inicjacji cyklu życia rozwoju systemu), ale raczej, że takie zabezpieczenia mogą nie wspierać poszczególnych zdolności do ochrony prywatności lub zapewnienia bezpieczeństwa. Ponadto nie każdy wdrożony środek bezpieczeństwa i ochrony prywatności koniecznie wspiera lub musi wspierać zdolności zdefiniowane przez organizację.

Gdy organizacje stosują koncepcję zdolności, automatyczne i przeprowadzone przez człowieka oceny uwzględniają wszystkie środki bezpieczeństwa i ochrony prywatności, które składają się na zdolności bezpieczeństwa i zdolności ochrony prywatności. Oceniający mają świadomość, w jaki sposób zabezpieczenia współdziałają w celu zapewnienia takich zdolności. W ten sposób, gdy w ocenach zidentyfikowana zostanie awaria zdolności, można przeprowadzić analizę pierwotnej przyczyny w celu określenia konkretnego zabezpieczenia lub zabezpieczeń, które są odpowiedzialne za niepowodzenie, na podstawie ustalonych relacji między zabezpieczeniami. Co więcej, zastosowanie szerszej konstrukcji zdolności pozwala organizacjom ocenić dotkliwość podatności wykrytych w ich systemach i organizacjach oraz określić, czy awaria danego środka bezpieczeństwa lub zabezpieczenia ochrony prywatności (związana podatnością) lub decyzja o niewdrażaniu danego zabezpieczenia podczas wstępnego procesu dostosowywania (etap wyboru w RMF) wpływa na ogólną zdolność potrzebną do zapewnienia bezpieczeństwa misji i działalności gospodarczej. Przykładowo, awaria zabezpieczenia uznanego za krytyczne dla danej zdolności do ochrony może mieć wyższy stopień dotkliwości niż awaria zabezpieczenia o mniejszym znaczeniu dla tej zdolności.

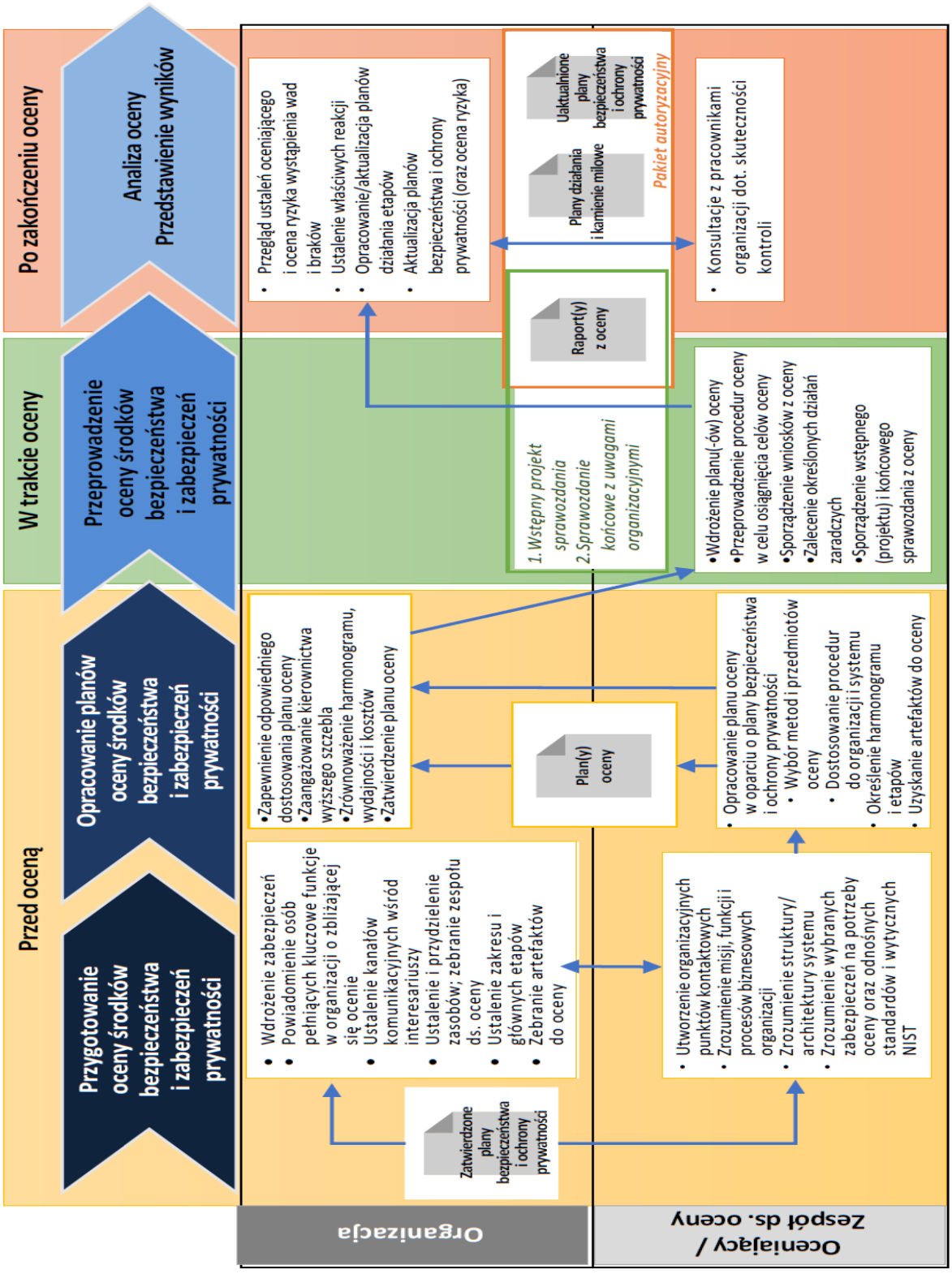
Ostatecznie decyzje dotyczące autoryzacji (tzn. decyzje dotyczące akceptacji ryzyka) są podejmowane na podstawie stopnia, w jakim skutecznie osiągnięto pożądane zdolności do ochrony i zdolności do ochrony prywatności oraz w jakim spełniają one wymagania dotyczące bezpieczeństwa i ochrony prywatności określone przez organizację. Decyzje oparte na ryzyku są bezpośrednio związane

z tolerowaniem przez organizację ryzyka, które jest określone w ramach strategii zarządzania ryzykiem w organizacji.

**OCENY OPARTE NA ZDOLNOŚCIACH**

Podział zabezpieczeń ze względu na zdolność zapewnienia bezpieczeństwa oraz zdolność do ochrony prywatności wymaga przeprowadzenia analizy przyczyn źródłowych w celu ustalenia, czy usterkę danej zdolności można przypisać do niepowodzenia jednego lub większej liczby środków bezpieczeństwa lub zabezpieczeń prywatności na podstawie ustalonych zależności między zabezpieczeniami. Za taką analizą przyczyn źródłowych przemawia struktura procedur oceny w niniejszej publikacji z rozkładem na poziomie dowodów i oznaczeniem celów oceny powiązanych z konkretną treścią środków bezpieczeństwa i zabezpieczeń prywatności. Dlatego oceny środków bezpieczeństwa i zabezpieczeń prywatności (zdefiniowanych jako część zdolności) mogą być dostosowane w oparciu o wytyczne zawarte w sekcji 3.2.3 i [NSC 800-137] w zakresie określania nakładów zasobów (np. częstotliwości i poziomu wysiłku) związanych z takimi ocenami. To doprecyzowanie w ocenach jest niezbędne do wspierania opracowanych przez organizacje strategii ciągłego monitorowania oraz bieżących decyzji liderów wyższego szczebla dotyczących autoryzacji.

Rysunek 8 przedstawia podsumowanie procesu oceny środków bezpieczeństwa i zabezpieczeń prywatności, w tym działania podejmowane przed oceną, w trakcie oceny i po jej zakończeniu.




**Rysunek 8. Przegląd procesu oceny środków bezpieczeństwa i zabezpieczeń prywatności.**

ROZDZIAŁ CZWARTY

# 4. PROCEDURY OCENY ŚRODKÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

*Rozdział 4 znajduje się w części 2 rekomendacji NSC 800-53A.*

*Patrz: plik: NSC 800-53A wer. 2.0_Część 2.*

## ZAŁĄCZNIKI

***Załączniki A do F znajdują się w części 3 rekomendacji NSC 800-53A.***

***Patrz plik: NSC 800-53A wer. 2.0_ Część 3.***