Ministerstwo Cyfryzacji

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-53A wer. 2.0

Część 3 - Załączniki

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.

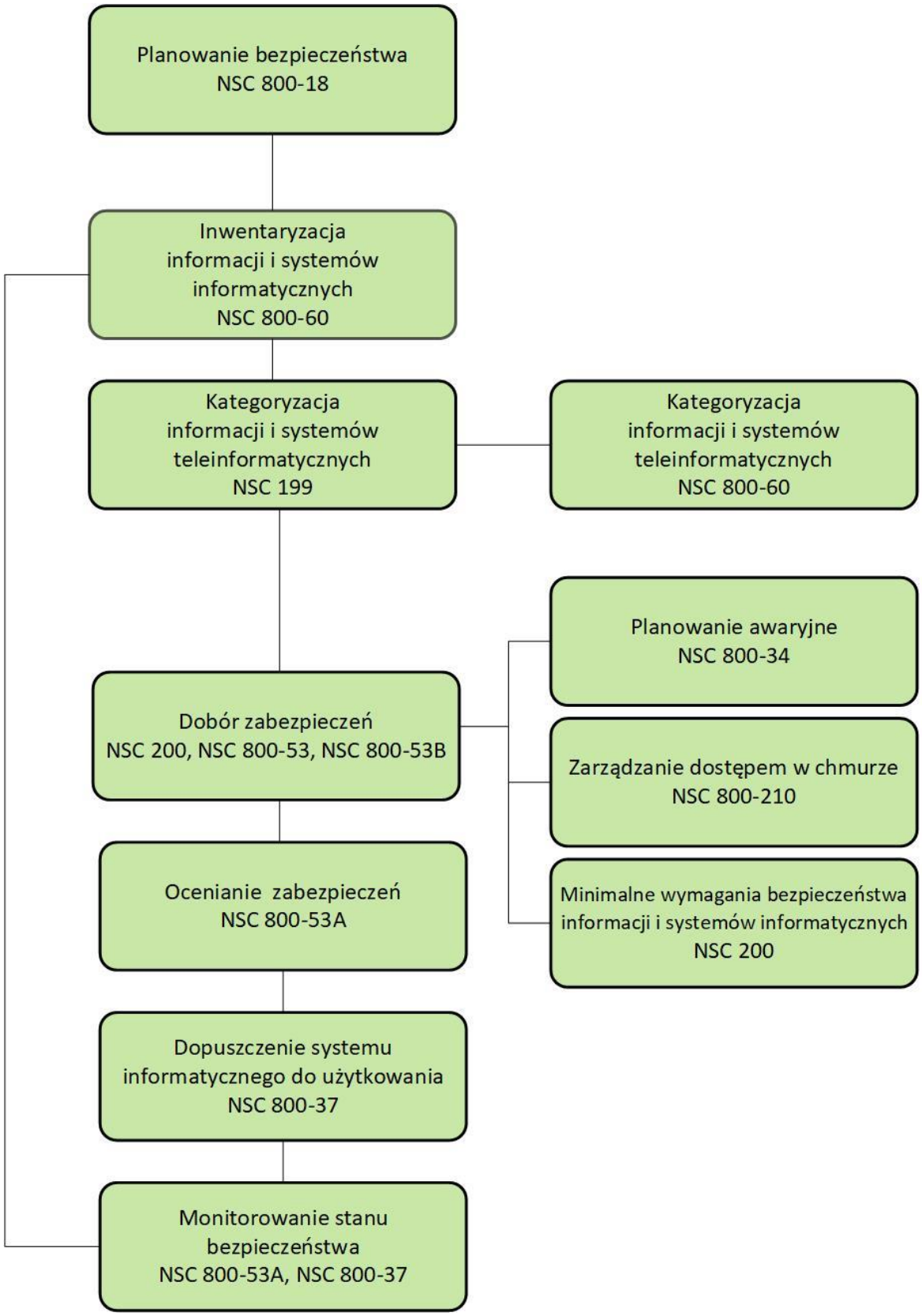
Zestaw publikacji specjalnych obejmuje następujące pozycje:

- 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[53]), 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

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

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

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

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

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

 Narodowe Standardy Cyberbezpieczeństwa

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

 +48222455922

 sekretariat.dc@cyfra.gov.pl

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

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

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

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

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

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

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

Spis treści

ZAŁĄCZNIK A - SŁOWNIK

Patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*

ZAŁĄCZNIK B - AKRONIMY I SKRÓTY

Patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*

ZAŁĄCZNIK C - OPIS METOD OCENY

DEFINICJE METOD OCENY, PRZEDMIOT OCENY I ATRYBUTY

Niniejszy załącznik definiuje trzy metody oceny, które mogą być stosowane przez oceniających w ramach procesu oceny zabezpieczeń i ochrony prywatności:

1. Badanie
2. Wywiad
3. Test

Definicja każdej metody oceny obejmuje typy obiektów, do których można ją zastosować. Zastosowanie każdej metody jest opisane pod względem atrybutów głębokości i zakresu — od poziomu podstawowego, poprzez ukierunkowany aż do kompleksowego. Wartości atrybutów korelują z wymaganiami dotyczącymi pewności określonymi przez organizację.

Atrybut głębokości odnosi się do rygoru i poziomu szczegółowości oceny. W przypadku atrybutu głębokości wartość atrybutu szczegółowego opiera się na rygorze oceny i poziomie szczegółowości określonym dla wartości atrybutu podstawowego. Z kolei wartość atrybutu kompleksowego oparta jest rygorze oceny i poziomie szczegółowości określonym dla wartości atrybutu szczegółowego.

Atrybut zakresu odnosi się do zakresu lub skali realizowanej oceny. W przypadku atrybutu zakresu wartość atrybutu ukierunkowanego oparta jest na liczbie i typie obiektów oceny zdefiniowanych dla wartości atrybutu podstawowego. Jednocześnie wartość atrybutu kompleksowego opiera się na liczbie i typie obiektów oceny zdefiniowanych dla wartości atrybutu szczegółowego.

Zastosowanie pogrubionego tekstu w opisie metody oceny wskazuje na treść, która została dodana i pojawia się po raz pierwszy, sygnalizując większy rygor i poziom szczegółowości dla danej wartości atrybutu.

Metoda oceny Badanie

Przedmiot oceny: Specyfikacje (np. polityki, plany, procedury, wymagania systemowe, projekty)

Mechanizmy (np. funkcje zaimplementowane w sprzęcie, oprogramowaniu, oprogramowaniu układowym)

Działania (np. obsługa systemu, administracja, zarządzanie, ćwiczenia)

Definicja: Proces sprawdzania, inspekcji, przeglądu, obserwacji, badania lub analizy jednego lub większej liczby przedmiotów oceny w celu zapewnienia lepszego zrozumienia bądź uzyskania wyjaśnień lub dowodów, którego wyniki są wykorzystywane do zdefiniowania środków bezpieczeństwa i ochrony prywatności, funkcji, poprawności, kompletności i potencjału poprawy z biegiem czasu.

Wskazówki uzupełniające: Typowe działania oceniającego mogą obejmować przegląd polityk, planów i procedur dotyczących bezpieczeństwa informacji i ochrony prywatności; analizę dokumentacji projektowej systemu i specyfikacji interfejsów; monitorowanie tworzenia kopii zapasowych systemu; przegląd wyników ćwiczebnego wdrożenia planu awaryjnego; obserwację działań związanych z reagowaniem na incydenty; analizę podręczników technicznych i podręczników użytkownika/ administratora; sprawdzanie, badanie lub monitorowanie działania mechanizmu informatycznego w sprzęcie i oprogramowaniu systemowym; lub sprawdzanie, badanie bądź monitorowanie fizycznych środków bezpieczeństwa lub ochrony prywatności związanych z działaniem systemu.

Atrybuty: głębokość, zakres

- **Atrybut głębokości** odnosi się do rygoru i poziomu szczegółowości procesu badania. W przypadku atrybutu głębokości wyróżnia się trzy możliwe wartości: *podstawowy*, *ukierunkowany* i *kompleksowy*.

Badanie podstawowe: Badanie obejmujące ogólne przeglądy, kontrole, monitorowanie lub inspekcje przedmiotu oceny. Badanie podstawowe jest przeprowadzane przy użyciu ograniczonego zbioru dowodów lub dokumentacji (np. opisy funkcjonalne mechanizmów; ogólne opisy procesów dotyczących realizacji działań; rzeczywista dokumentacja dotycząca specyfikacji). Badanie podstawowe daje pewien obraz środków bezpieczeństwa i ochrony prywatności niezbędny do ustalenia, czy wdrożono stosowne zabezpieczenia i czy są one wolne od ewidentnych błędów.

Badanie ukierunkowane: Badanie obejmujące ogólne przeglądy, kontrole, monitorowanie lub inspekcje oraz **bardziej dogłębne badania/analizy** przedmiotu oceny. Badanie ukierunkowane jest przeprowadzane przy użyciu **znaczącej** ilości dowodów lub dokumentacji (np. opisy funkcjonalne **oraz, w stosownych przypadkach i w miarę dostępności, ogólne informacje projektowe dotyczące** mechanizmów; ogólne opisy procesów dotyczących realizacji oraz **procedury wdrażania** dotyczące działań; rzeczywista dokumentacja dotycząca specyfikacji oraz **powiązane dokumenty**). Badanie ukierunkowane daje pewien obraz środków bezpieczeństwa i ochrony prywatności niezbędny do ustalenia, czy wdrożono stosowne zabezpieczenia i czy są one wolne od ewidentnych błędów, a **także czy istnieją solidne podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami.**

Badanie kompleksowe: Badanie obejmujące ogólne przeglądy, kontrole, monitorowanie lub inspekcje oraz bardziej dogłębne, **szczegółowe i dokładne** badania/analizy przedmiotu oceny. Badanie kompleksowe jest przeprowadzane przy użyciu **dużej** ilości dowodów lub dokumentacji (np. opisy funkcjonalne oraz, w stosownych przypadkach i w miarę dostępności, ogólne informacje projektowe, **szczegółowe informacje projektowe oraz informacje wdrożeniowe dotyczące** mechanizmów; ogólne opisy procesów dotyczących realizacji oraz **szczegółowe** procedury wdrażania dotyczące działań;

rzeczywista dokumentacja dotycząca specyfikacji oraz powiązane dokumenty[54]). Badanie **kompleksowe** daje pewien obraz środków bezpieczeństwa i ochrony prywatności niezbędny do ustalenia, czy wdrożono stosowne zabezpieczenia i czy są one wolne od ewidentnych błędów, czy istnieją **dalsze** podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami w **sposób ciągły i spójny oraz czy zapewniono wsparcie dla ciągłego doskonalenia skuteczności zabezpieczeń.**

- **Atrybut zakresu** odnosi się do zakresu lub skali procesu badania i obejmuje typy badanych przedmiotów oceny, liczbę badanych przedmiotów (według typu) oraz konkretne badane przedmioty.[55] W przypadku atrybutu zakresu wyróżnia się trzy możliwe wartości: *podstawowy*, *ukierunkowany* i *kompleksowy*.

  Badanie podstawowe: Badanie wykorzystujące reprezentatywną próbę przedmiotów oceny (według typu i liczby w ramach typu) w celu dostarczenia informacji niezbędnych do ustalenia, czy wdrożono stosowne środki ochrony bezpieczeństwa i prywatności i czy są one wolne od ewidentnych błędów.

  Badanie ukierunkowane: Badanie wykorzystujące reprezentatywną próbę przedmiotów oceny (według typu i liczby w ramach typu) oraz **innych określonych przedmiotów oceny uznanych za szczególnie ważne dla realizacji celu oceny** w celu dostarczenia informacji niezbędnych do ustalenia, czy wdrożono stosowne środki ochrony bezpieczeństwa i prywatności i czy są one wolne od ewidentnych błędów, a także czy istnieją **solidne podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami.**

[54] Przy przejściu od badań podstawowych do ukierunkowanych i kompleksowych prawdopodobnie będzie wymagana dodatkowa dokumentacja dotycząca mechanizmów. Jednocześnie w przypadku badań ukierunkowanych i kompleksowych możliwe jest wykorzystanie takiej samej lub podobnej dokumentacji związanej ze specyfikacjami i działaniami, przy czym na poziomie kompleksowym w odniesieniu do takich dokumentów obowiązuje zwiększony rygor badania.

[55] Organizacja uwzględnia różne czynniki (np. dostępne zasoby, znaczenie oceny, ogólne cele i zadania organizacji w zakresie oceny), konsultuje się z oceniającymi i zapewnia wskazówki dotyczące typów, liczby i konkretnych przedmiotów oceny, które mają zostać zbadane pod kątem konkretnej opisanej wartości atrybutu.

Badanie kompleksowe: Badanie wykorzystujące **odpowiednio dużą** próbę przedmiotów oceny (według typu i liczby w ramach typu) oraz innych określonych przedmiotów oceny uznanych za szczególnie ważne dla realizacji celu oceny w celu dostarczenia informacji niezbędnych do ustalenia, czy wdrożono stosowne środki ochrony bezpieczeństwa i prywatności i czy są one wolne od ewidentnych błędów, istnieją **dalsze** podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami w **sposób ciągły i spójny oraz czy zapewniono wsparcie dla ciągłego doskonalenia skuteczności zabezpieczeń.**

Metoda oceny Wywiad

Przedmiot oceny: Osoby lub grupy osób

Definicja: Proces przeprowadzania dyskusji z osobami lub grupami w organizacji w celu zapewnienia lepszego zrozumienia bądź uzyskania wyjaśnień lub dowodów, których wyniki są wykorzystywane do zdefiniowania środków bezpieczeństwa i ochrony prywatności, funkcji, poprawności, kompletności i potencjału poprawy z biegiem czasu.

Wskazówki uzupełniające: Typowe działania oceniającego mogą obejmować rozmowy z kierownikami organizacji, kluczowym personelem ds. bezpieczeństwa informacji (CIO, SAISO)[56], wyższym personelem ds. ochrony prywatności (SAOP)[57], urzędnikami autoryzującymi, właścicielami informacji, właścicielami systemów i misji, personelem ds. bezpieczeństwa systemu i prywatności, kierownikami ds. bezpieczeństwa systemu i prywatności, personelem kadrowym, kierownikami ds. zasobów ludzkich, prawnikami, kierownikami obiektów, personelem zarządzania kryzysowego, personelem ds. szkoleń, operatorami systemów, administratorami sieci i systemów, kierownikami witryn, personelem ds. bezpieczeństwa fizycznego i użytkownikami.

Atrybuty: głębokość, zakres

- **Atrybut głębokości** odnosi się do rygoru i poziomu szczegółowości procesu wywiadu. W przypadku atrybutu głębokości wyróżnia się trzy możliwe wartości: *podstawowy*, *ukierunkowany* i *kompleksowy*.

  Wywiad podstawowy: Wywiad obejmujący obszerne dyskusje o ogólnym charakterze, prowadzone z pojedynczymi osobami lub grupami osób. Wywiad podstawowy przeprowadza się z wykorzystaniem zestawu pytań ogólnych. Wywiad podstawowy daje pewien obraz środków bezpieczeństwa i ochrony

[56] Definicje: patrz NSC 7298.

[57] Tamże.

prywatności niezbędny do ustalenia, czy wdrożono stosowne zabezpieczenia i czy są one wolne od ewidentnych błędów.

Wywiad ukierunkowany: Wywiad obejmujący obszerne dyskusje o ogólnym charakterze, a **także bardziej szczegółowe dyskusje dotyczące niektórych obszarów**, prowadzone z pojedynczymi osobami lub grupami osób. Wywiad ukierunkowany przeprowadza się z wykorzystaniem zestawu pytań ogólnych oraz **pytań bardziej szczegółowych, jeżeli istnieje potrzeba zapewnienia większej pewności lub gdy odpowiedzi wskazują na potrzebę bardziej dogłębnego badania.** Badanie **ukierunkowane** daje pewien obraz środków bezpieczeństwa i ochrony prywatności niezbędny do ustalenia, czy wdrożono stosowne zabezpieczenia i czy są one wolne od ewidentnych błędów, a **także czy istnieją solidne podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami.**

Wywiad kompleksowy: Wywiad obejmujący obszerne dyskusje o ogólnym charakterze, a **także bardziej szczegółowe dyskusje dotyczące niektórych obszarów**, **prowadzone z pojedynczymi osobami lub grupami osób.** Wywiad ukierunkowany przeprowadza się z wykorzystaniem zestawu pytań ogólnych oraz **pytań bardziej szczegółowych, sondujących, jeżeli istnieje potrzeba zapewnienia większej pewności lub gdy odpowiedzi wskazują na potrzebę bardziej dogłębnego badania.** Wywiad **kompleksowy** daje pewien obraz środków bezpieczeństwa i ochrony prywatności niezbędny do ustalenia, czy wdrożono stosowne zabezpieczenia i czy są one wolne od ewidentnych błędów, czy istnieją **dalsze** podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami w **sposób ciągły i spójny oraz czy zapewniono wsparcie dla ciągłego doskonalenia skuteczności zabezpieczeń.**

- **Atrybut zakresu** odnosi się do zakresu lub skali procesu wywiadu i obejmuje typy (według roli w organizacji i powiązanych obowiązków), liczbę (według typu)

oraz wykaz konkretnych osób, z którymi należy przeprowadzić wywiad.[58]
W przypadku atrybutu zakresu wyróżnia się trzy możliwe wartości: *podstawowy*, *ukierunkowany* i *kompleksowy*.

Wywiad podstawowy: Badanie wykorzystujące reprezentatywną próbkę osób pełniących kluczowe role w organizacji w celu dostarczenia informacji niezbędnych do ustalenia, czy wdrożono stosowne środki bezpieczeństwa i ochrony prywatności i czy są one wolne od ewidentnych błędów.

Wywiad ukierunkowany: Wywiad wykorzystujący reprezentatywną próbkę osób pełniących kluczowe role w organizacji oraz **innych określonych osób uznanych za szczególnie ważne dla realizacji celu oceny** w celu dostarczenia informacji niezbędnych do ustalenia, czy wdrożono stosowne środki ochrony bezpieczeństwa i prywatności i czy są one wolne od ewidentnych błędów, a **także czy istnieją solidne podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami.**

Wywiad kompleksowy: Wywiad wykorzystujący **odpowiednio dużą** próbkę osób pełniących kluczowe role w organizacji oraz innych określonych osób uznanych za szczególnie ważne dla realizacji celu oceny w celu dostarczenia informacji niezbędnych do ustalenia, czy wdrożono stosowne środki ochrony bezpieczeństwa i prywatności i czy są one wolne od ewidentnych błędów, czy istnieją **dalsze** podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami w **sposób ciągły i spójny oraz czy zapewniono wsparcie dla ciągłego doskonalenia skuteczności zabezpieczeń.**

[58] Organizacja uwzględnia różne czynniki (np. dostępne zasoby, znaczenie oceny, ogólne cele i zadania organizacji w zakresie oceny), konsultuje się z oceniającymi i zapewnia wskazówki dotyczące typów, liczby i konkretnych osób, które mają być objęte wywiadem pod kątem konkretnej opisanej wartości atrybutu.

Metoda oceny Test

Przedmiot oceny: Mechanizmy (np. sprzęt, oprogramowanie, oprogramowanie układowe)

Działania (np. obsługa systemu, administracja, zarządzanie, ćwiczenia)

Definicja: Proces testowania jednego lub większej liczby przedmiotów oceny w określonych warunkach w celu porównania oczekiwanego/pożądanego zachowania, którego wyniki są wykorzystywane do zdefiniowania środków bezpieczeństwa i ochrony prywatności, funkcji, poprawności, kompletności i potencjału poprawy z biegiem czasu.[59]

Wskazówki uzupełniające: Typowe działania oceniającego mogą obejmować testowanie mechanizmów kontroli dostępu, identyfikacji i uwierzytelniania oraz audytu; testowanie ustawień konfiguracji bezpieczeństwa i prywatności; testowanie fizycznych urządzeń kontroli dostępu; testy penetracyjne kluczowych komponentów systemu; testowanie operacji tworzenia kopii zapasowych systemu; testowanie zdolności reagowania na incydenty; oraz ćwiczenie zdolności planowania awaryjnego.

Atrybuty: głębokość, zakres

- **Atrybut głębokości** odnosi się do rodzajów testów, które mają być przeprowadzone. W przypadku atrybutu głębokości wyróżnia się trzy możliwe wartości: *podstawowy*, *ukierunkowany* i *kompleksowy*.

  Test podstawowy: Metodologia testów, która zakłada brak znajomości wewnętrznej struktury i sposobu wdrożenia przedmiotu oceny. Test

[59] Testowanie zwykle wykorzystuje się w celu określenia, czy mechanizmy lub działania zachowują zgodność z wcześniej zdefiniowanymi specyfikacjami. Testy mogą być również przeprowadzane w celu określenia charakterystyki środka ochrony bezpieczeństwa lub prywatności, który nie jest powszechnie kojarzony z wcześniej ustalonymi specyfikacjami — np. testy penetracyjne. Wytyczne dotyczące przeprowadzania testów penetracyjnych zawarto w Załączniku D.

podstawowy przeprowadzany jest przy użyciu specyfikacji funkcjonalnej w przypadku mechanizmów oraz z wykorzystaniem ogólnego opisu procesów w przypadku działań. Test podstawowy daje pewien obraz środków bezpieczeństwa i ochrony prywatności niezbędny do ustalenia, czy wdrożono stosowne zabezpieczenia i czy są one wolne od ewidentnych błędów.

Test ukierunkowany: Metodologia testów, która zakłada **pewną** znajomości wewnętrznej struktury i sposobu wdrożenia przedmiotu oceny. Test ukierunkowany przeprowadzany jest przy użyciu specyfikacji funkcjonalnej i **ograniczonych informacji o architekturze systemu (np. ogólny projekt)** w przypadku mechanizmów oraz z wykorzystaniem ogólnego opisu procesów, a **także ogólnego opisu integracji ze środowiskiem operacyjnym** w przypadku działań. Test **ukierunkowany** daje pewien obraz środków bezpieczeństwa i ochrony prywatności niezbędny do ustalenia, czy wdrożono stosowne zabezpieczenia i czy są one wolne od ewidentnych błędów, a **także czy istnieją solidne podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami.**

Test kompleksowy: Metodologia testów, która zakłada **bezpośrednią i znaczącą** znajomość wewnętrznej struktury i sposobu wdrożenia przedmiotu oceny. Test kompleksowy przeprowadzany jest przy użyciu specyfikacji funkcjonalnej, **szczegółowych** informacji o architekturze systemu (np. ogólny projekt, szczegółowy projekt) , **odzwierciedlenia sposobu wdrożenia (np. kod źródłowy, schematy) w** przypadku mechanizmów oraz z wykorzystaniem ogólnego opisu procesów, a także **szczegółowego** opisu integracji ze środowiskiem operacyjnym w przypadku działań. Test kompleksowy daje pewien obraz środków bezpieczeństwa i ochrony prywatności niezbędny do ustalenia, czy wdrożono stosowne zabezpieczenia i czy są one wolne od ewidentnych błędów, czy istnieją **dalsze** podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami w **sposób ciągły i spójny oraz czy zapewniono wsparcie dla ciągłego doskonalenia skuteczności zabezpieczeń.**

- Atrybut *zakresu* odnosi się do zakresu lub skali procesu testowania i obejmuje typy badanych przedmiotów oceny, liczbę badanych przedmiotów (według typu) oraz konkretne badane przedmioty.[60] W przypadku atrybutu zakresu wyróżnia się trzy możliwe wartości: *podstawowy*, *ukierunkowany* i *kompleksowy*.

  Test podstawowy: Test wykorzystujący reprezentatywną próbkę przedmiotów oceny (według typu i liczby w ramach typu) w celu zapewnienia zakresu niezbędnego do ustalenia, czy wdrożono stosowne środki bezpieczeństwa i ochrony prywatności i czy są one wolne od ewidentnych błędów.

  Test ukierunkowany: Test wykorzystujący reprezentatywną próbkę przedmiotów oceny (według typu i liczby w ramach typu) oraz **innych określonych przedmiotów oceny uznanych za szczególnie ważne do realizacji celu oceny** w celu zapewnienia zakresu niezbędnego do ustalenia, czy wdrożono stosowne środki bezpieczeństwa i ochrony prywatności i czy są one wolne od ewidentnych błędów, a **także czy istnieją solidne podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami.**

  Test kompleksowy: Test wykorzystujący **odpowiednio dużą** próbkę przedmiotów oceny (według typu i liczby w ramach typu) oraz innych określonych przedmiotów oceny uznanych za szczególnie ważne dla realizacji celu oceny w celu dostarczenia informacji niezbędnych do ustalenia, czy wdrożono stosowne środki bezpieczeństwa i ochrony prywatności i czy są one wolne od ewidentnych błędów, czy istnieją **dalsze** podstawy do uznania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami w **sposób ciągły i spójny oraz czy zapewniono wsparcie dla ciągłego doskonalenia skuteczności zabezpieczeń.**

[60] Organizacja uwzględnia różne czynniki (np. dostępne zasoby, znaczenie oceny, ogólne cele i zadania organizacji w zakresie oceny), konsultuje się z oceniającymi i zapewnia wskazówki dotyczące typów, liczby i konkretnych przedmiotów oceny, które mają być przetestowane pod kątem konkretnej opisanej wartości atrybutu. W przypadku testowania dotyczącego mechanizmów, atrybut zakresu odnosi się również do samego zakresu przeprowadzanego testowania (np. w przypadku oprogramowania: liczba zadań testowych i modułów objętych testowaniem; w przypadku sprzętu: zakres danych wejściowych, liczba testowanych komponentów i zakres czynników środowiskowych objętych testowaniem).

ZAŁĄCZNIK D - TESTY PENETRACYJNE

NARZĘDZIA I TECHNIKI OCENY UMOŻLIWIAJĄCE IDENTYFIKACJĘ SŁABYCH PUNKTÓW SYSTEMU

Organizacje mogą rozważyć wdrożenie kontrolowanych testów penetracyjnych do swojego arsenału narzędzi i technik wykorzystywanych do oceny środków bezpieczeństwa i ochrony prywatności w systemach organizacyjnych.

Test penetracyjny to specyficzny rodzaj oceny, w ramach której oceniający symulują działania podejmowane przez pewne kategorie atakujących, korzystając ze zdefiniowanej dokumentacji (określającej, jakimi środkami taka kategoria atakujących prawdopodobnie dysponuje) i działając pod innymi określonymi ograniczeniami, aby spróbować obejść zabezpieczenia lub mechanizmy ochrony prywatności systemu.

Testy penetracyjne są realizowane jako kontrolowana próba naruszenia zabezpieczeń i mechanizmów ochrony prywatności zastosowanych w systemie przy użyciu technik atakującego oraz odpowiednich narzędzi sprzętowych i programowych. W ramach testu penetracyjnego przedstawia się wyniki uzyskane przez określonego oceniającego lub grupy oceniających w danym momencie przy użyciu uzgodnionych zasad prowadzenia testów penetracyjnych (*ang.: rules of engagement*) Biorąc pod uwagę złożoność technologii informatycznych powszechnie stosowanych obecnie przez organizacje, testy penetracyjne można postrzegać nie tyle jako środek do weryfikacji zabezpieczeń i mechanizmów ochrony prywatności systemu, ale raczej jako narzędzie służące do lepszego zrozumienia systemu przez organizację, ujawnienia jego słabości lub braków, jak również określenia skali wysiłków, jakie atakujący będą musieli podjąć w celu złamania wdrożonych zabezpieczeń.

Testy penetracyjne mogą odbywać się w sposób zaplanowany lub losowy, zgodnie z polityką i oceną ryzyka organizacji. Można rozważyć przeprowadzanie testów penetracyjnych każdego nowo opracowanego systemu (lub starszego systemu przechodzącego znaczącą modernizację) przed zatwierdzeniem go do eksploatacji, a także stosowanie tego rodzaju testowania w przypadku wprowadzenia istotnych

zmian w środowisku operacyjnym systemu oraz po wykryciu nowego rodzaju ataku, który może mieć wpływ na system. Organizacje aktywnie monitorują środowisko systemowe i krajobraz zagrożeń (np. nowe luki w zabezpieczeniach, techniki ataków, nowe technologie, bezpieczeństwo użytkowników oraz świadomość i szkolenia w zakresie prywatności) w celu zidentyfikowania zmian, które wymagają przeprowadzenia testów penetracyjnych poza ustalonym harmonogramem.

Organizacje określają, które komponenty systemu podlegają testom penetracyjnym, a także profil atakującego, który ma zostać przyjęty podczas testów penetracyjnych.

Ponadto organizacje szkolą wybrany personel w zakresie wykorzystania narzędzi i technik na potrzeby testów penetracyjnych. Odpowiednie narzędzia do realizacji takich testów mają możliwość łatwej aktualizacji listy stosowanych technik ataków i podatności wykorzystywanych podczas ćwiczeń. Organizacje na bieżąco aktualizują listę technik ataku i możliwych do wykorzystania luk w zabezpieczeniach wykorzystywanych w testach penetracyjnych w oparciu o organizacyjną ocenę ryzyka, a także w przypadku zidentyfikowania i zgłoszenia nowych, istotnych luk w zabezpieczeniach bądź też zagrożeń. W miarę możliwości organizacje stosują narzędzia i techniki ataku, które umożliwiają przeprowadzanie automatycznych testów penetracyjnych systemów oraz środków bezpieczeństwa i ochrony prywatności.[61]

Informacje uzyskane w ramach testów penetracyjnych mogą być udostępniane odpowiedniemu personelowi w całej organizacji, aby pomóc w przypisaniu priorytetów do luk w zabezpieczeniach systemu, które ewidentnie są narażone na naruszenie przez atakujących o takim profilu, jaki zastosowano podczas wspomnianych testów. Ustalenie priorytetów pomaga określić skuteczne strategie eliminowania zidentyfikowanych słabych punktów i ograniczania powiązanych

[61] Mimo iż automatyczne narzędzia do testów penetracyjnych zapewniają powtarzalne wyniki i zmniejszają wykorzystywane zasoby, organizacje powinny dokładnie rozważyć potencjalny szkodliwy wpływ takich środków na dostępność systemu. Ponadto testy penetracyjne oparte wyłącznie na automatycznych narzędziach mogą nie odzwierciedlać poziomu zaawansowania prawdziwego atakującego pod względem działań podejmowanych w celu obejścia zabezpieczeń.

zagrożeń dla działalności i zasobów organizacji, osób fizycznych, innych organizacji i państwa wynikających z eksploatacji systemu. Testy penetracyjne można zintegrować z procesem testowania bezpieczeństwa sieci oraz procesem zarządzania poprawkami i lukami w zabezpieczeniach.[62]

ZAGADNIENIA ZWIĄZANE Z TESTAMI PENETRACYJNYMI

Podczas opracowywania i wdrażania programu kontrolowanych testów penetracyjnych organizacje powinny uwzględnić poniższe kryteria. Skuteczny test penetracyjny:

- Wykracza poza wyszukiwanie luk w zabezpieczeniach, aby zapewnić wyraźne dowody na istnienie ryzyka związanego z misją oraz określić skalę wysiłków, jakie atakujący musiałby podjąć, aby spowodować szkodę dla działalności i zasobów organizacji, osób fizycznym, innych organizacji lub państwa.
- Stosuje w odniesieniu do systemu takie podejście, jakie wybrałby atakujący, biorąc pod uwagę luki w zabezpieczeniach, nieprawidłowe konfiguracje systemu, relacje zaufania między organizacjami i słabości architektury testowanego środowiska.
- Ma jasno określony zakres i obejmuje co najmniej:
  - definicję środowiska objętego testowaniem (np. obiekty, użytkownicy, grupy organizacyjne);
  - definicję płaszczyzny ataku, która ma zostać przetestowana (np. serwery, systemy stacjonarne, sieci bezprzewodowe, aplikacje internetowe, systemy wykrywania i zapobiegania włamaniom, zapory ogniowe, konta e-mail, świadomość i przeszkolenie użytkowników w zakresie bezpieczeństwa i prywatności oraz zdolność do reagowania na incydenty, w tym naruszenia dotyczące danych identyfikacyjnych);

[62] Dokument [SP 800-40] zawiera wskazówki dotyczące zarządzania poprawkami i lukami w zabezpieczeniach. Dokument [SP 800-115] zawiera wskazówki dotyczące testowania bezpieczeństwa informacji i sieci.

- definicję symulowanych źródeł zagrożeń (np. określenie wykorzystywanych profili atakujących, takich jak atakujący wewnętrzny, przypadkowy, pojedynczy lub grupa zewnętrznych ukierunkowanych napastników, podmiot narodowy/państwowy lub organizacja przestępcza);
- definicję celów symulowanego atakującego (np. uzyskanie dostępu na poziomie administratora domeny do struktury LDAP [Lightweight Directory Access Protocol] organizacji czy dostęp do informacji w systemie finansowym organizacji i ich modyfikacja);
- określenie wymaganej skali wysiłków atakującego (np. czasu i zasobów);
- zasady prowadzenia testów penetracyjnych:

- Dokładnie dokumentują wszelkie działania wykonane podczas testu, w tym wszelkie wykorzystane luki w zabezpieczeniach, a także sposób, w jaki luki wykorzystano wspólnie w ramach ataków.
- Generują wyniki określające prawdopodobieństwo wystąpienia danego ataku na podstawie skali wysiłków, jakie zespół musiał podjąć w celu dokonania udanej penetracji systemu, stanowiące wskaźnik odporności systemu na penetrację.
- Weryfikują istniejące środki bezpieczeństwa i ochrony prywatności (w tym mechanizmy ograniczania ryzyka, takie jak zapory ogniowe czy systemy wykrywania i zapobiegania włamaniom).
- Zapewniają możliwy do zweryfikowania i powtarzalny rejestr wszystkich czynności wykonywanych podczas testu.
- Zapewniają wyniki umożliwiające podjęcie działań wraz z informacjami o możliwych środkach zaradczych w odniesieniu do przeprowadzonych udanych ataków.

ZAŁĄCZNIK E - RAPORTY Z OCEN

DOKUMENTOWANIE USTALEŃ Z OCENY ŚRODKÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Podstawowym celem *raportów z oceny środków bezpieczeństwa* i *ochrony prywatności* jest przekazanie wyników oceny zabezpieczeń i ochrony prywatności odpowiedniemu personelowi w organizacji. Raport z oceny środków bezpieczeństwa i raport z oceny ochrony prywatności są zawarte w pakiecie autoryzacyjnym systemu wraz z planem bezpieczeństwa systemu i planem ochrony prywatności (lub ich odpowiednikiem w przypadku zabezpieczeń wspólnych), planem działania i etapami wprowadzania zabezpieczeń oraz podsumowaniem. Dostarcza to osobom zatwierdzającym informacji niezbędnych do podejmowania decyzji o rozpoczęciu lub kontynuowaniu eksploatacji systemu w oparciu o występujące ryzyko. W miarę rosnącej dynamizacji procesu oceny i autoryzacji oraz zwiększającego się znaczenia ciągłego monitorowania procesu jako zintegrowanego, nieodzownego elementu cyklu życia systemu, zdolność do częstej aktualizacji raportów z oceny środków bezpieczeństwa staje się kluczowym aspektem programów bezpieczeństwa informacji i ochrony prywatności.

Jednocześnie należy podkreślić związek między kluczowymi artefaktami w pakiecie autoryzacji, tak jak opisano w [NSC 800-37]. Zawarte w pakiecie autoryzacyjnym artefakty stanowią wiarygodny wskaźnik ogólnego ryzyka związanego z bezpieczeństwem i ochroną prywatności systemu, a także zdolności systemu do zapewnienia niezbędnej ochrony dla działalności i zasobów organizacji, osób fizycznych, innych organizacji oraz państwa. Kluczowe artefakty podlegają bieżącej aktualizacji zgodnie z programem ciągłego monitorowania ustanowionym przez organizację.

Raporty z oceny środków ochrony bezpieczeństwa i prywatności stanowią metodyczne i ustrukturyzowane podejście do dokumentowania ustaleń oceniającego oraz zaleceń dotyczących korygowania wszelkich słabości lub braków w środkach bezpieczeństwa

i ochrony prywatności.[63] Niniejszy załącznik zawiera szablon do zgłaszania wyników z ocen środków bezpieczeństwa i ochrony prywatności. Organizacje nie są jednak ograniczone do stosowania wyłącznie formatu przedstawionego w jego treści. Niemniej oczekuje się, że całościowy raport z oceny będzie zawierał informacje podobne do tych wyszczególnionych w szablonie dla każdego ocenianego środka bezpieczeństwa i ochrony prywatności, poprzedzone podsumowaniem zawierającym wykaz wszystkich takich środków podlegających ocenie oraz ogólny stan każdego z nich.

KLUCZOWE ASPEKTY SPORZĄDZANIA RAPORTÓW Z OCENY

W raportach z oceny środków bezpieczeństwa i ochrony prywatności zawarte są następujące elementy:[64]

- Nazwa systemu
- Kategoryzacja bezpieczeństwa
- Oceniane obiekty wraz z datą oceny
- Imię i nazwisko/identyfikacja oceniającego
- Wyniki poprzedniej oceny (jeśli zostały ponownie wykorzystane)
- Środek bezpieczeństwa/ochrony prywatności lub mechanizm usprawniający tenże środek
- Wybrane metody i przedmioty oceny
- Wartości atrybutów głębokości i zakresu

[63] Mimo iż elementem formalnych raportów z oceny środków bezpieczeństwa i ochrony prywatności jest uzasadnienie każdego podjętego ustalenia, raport najpewniej nie będzie zawierał kompletnego zestawu dokumentacji sporządzonej w ramach oceny. Organizacje zachowują jednak część dokumentacji niezbędną do utrzymania ścieżki audytu dowodów oceny, ułatwienia ponownego wykorzystania dowodów i promowania powtarzalności działań realizowanych przez oceniających.

[64] Informacje dostępne w innych kluczowych dokumentach organizacyjnych (np. planach bezpieczeństwa lub ochrony prywatności, ocenach ryzyka, planach działań i etapach wprowadzania zabezpieczeń czy planach oceny środków bezpieczeństwa lub ochrony prywatności) nie muszą być powielane w raportach z oceny środków bezpieczeństwa i ochrony prywatności.

- Podsumowanie wyników oceny (z określeniem „spełnione” lub „niespełnione”)
- Uwagi oceniającego (odnotowane słabe punkty lub braki)
- Zalecenia oceniającego (priorytety, środki zaradcze, działania naprawcze lub usprawnienia)

WYNIKI OCENY

Przy każdym badanym elemencie oceniający wpisuje następujący symbol: spełnione (S) lub niespełnione (N). Przykładową ocenę dla kategorii CP-03 przedstawiono w tabeli 9.

Podczas rzeczywistej oceny środków bezpieczeństwa i ochrony prywatności poczynione ustalenia oraz komentarze i zalecenia są dokumentowane za pośrednictwem odpowiednich formularzy lub platform sprawozdawczych określonych przez organizację. Organizacje zachęca się do opracowania standardowych szablonów sprawozdawczych, zawierających kluczowe elementy oceny opisane powyżej. W miarę możliwości należy stosować automatyzację w celu ograniczenia kosztów oraz zapewnienia terminowości i sprawności w zakresie gromadzenia danych i sprawozdawczości.

CP-03	**SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA**			
	CEL OCENY: *Ustalenie, czy:*		**WYNIK OCENY**	**UWAGI I ZALECENIA OCENIAJĄCEGO**
	CP-03_ODP[01]	***określono okres, w którym należy przeprowadzić szkolenie dot. planowania awaryjnego dla użytkowników obejmujących rolę lub obowiązki, które obejmują sytuacje awaryjne;***	S	Systemowa polityka planowania awaryjnego wyznacza (zdefiniowany przez organizację) okres wynoszący 4 tygodnie.
	CP-03_ODP[02]	***określono częstotliwość, z jaką należy przeprowadzać szkolenia dla użytkowników systemu, których rola lub obowiązki dotyczą planowania awaryjnego;***	S	Systemowa polityka planowania awaryjnego wyznacza częstotliwość roczną.
	CP-03_ODP[03]	***określono częstotliwość, z jaką należy dokonywać przeglądu i aktualizacji treści szkolenia dot. planowania awaryjnego;***	S	Systemowa polityka planowania awaryjnego wyznacza częstotliwość roczną.
	CP-03_ODP[04]	***określono zdarzenia wymagające przeglądu i aktualizacji szkolenia dot. planowania awaryjnego;***	N	Żaden z artefaktów objętych oceną nie wskazuje na zdarzenia wymagające przeglądu i aktualizacji szkolenia w zakresie planowania awaryjnego.
	CP-03a.01	*szkolenie dot. planowania awaryjnego jest zapewniane użytkownikom systemu zgodnie z przypisanymi rolami i obowiązkami w <okresie CP-03_ODP[01]> od objęcia roli lub zakresu*	S	

CP-03	SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA			
		odpowiedzialności, które dotyczą planowania awaryjnego.		
	CP-03a.02	*jeśli wymagają tego zmiany w systemie, przeprowadza się szkolenie dla użytkowników systemu w zakresie reagowania na incydenty zgodnie z przypisanymi rolami i obowiązkami;*	N	Oznaczono jako „niespełnione”. Oceniający nie znaleźli dowodów na to, że szkolenia w zakresie planowania awaryjnego dla użytkowników systemu korzystających z systemu ABC były prowadzone zgodnie z przypisanymi im rolami i obowiązkami w przypadku wprowadzenia istotnych zmian w systemie.
	CP-03a.03	*szkolenie dot. planowania awaryjnego jest następnie zapewniane użytkownikom systemu zgodnie z przypisanymi rolami i obowiązkami z <częstotliwością CP-03_ODP[02]>;*	S	
	CP-03b.[01]	*treść szkolenia dot. planowania awaryjnego jest weryfikowana i aktualizowana <z częstotliwością CP-02_ODP[03]>;*	S	
	CP-03b.[02]	*treść szkolenia dot. planowania awaryjnego jest weryfikowana i aktualizowana po <zdarzeniach CP - 03_ODP[04]>.*	N	Cel CP-03_ODP[04] nie został zdefiniowany. Nie można ocenić tego celu.

Tabela 9: Przykładowe ustalenia z oceny środków bezpieczeństwa i ochrony prywatności

ZAŁĄCZNIK F - BIEŻĄCA OCENA I AUTOMATYZACJA

WYKORZYSTANIE ZAUTOMATYZOWANYCH TECHNIK W CELU USPRAWNIENIA PROCESU OCENY

Bieżąca ocena bezpieczeństwa i ochrony prywatności polega na ciągłym analizowaniu skuteczności wdrożonych środków bezpieczeństwa i ochrony prywatności. Bieżąca ocena to szereg istotnych działań związanych z ciągłym monitorowaniem bezpieczeństwa informacji (*ang.: Information Security Continuous Monitoring — ISCM*).[65]Obejmuje ona trzeci i czwarty etap działania ISCM i jest inicjowana w ramach pierwszego z nich pn. „Wdrożenie" (*ang.: Implement)*, kiedy to rozpoczyna się gromadzenie informacji związanych z bezpieczeństwem zgodnie z częstotliwością zdefiniowaną przez organizację. Bieżąca ocena jest kontynuowana, podczas gdy informacje związane z bezpieczeństwem wygenerowane w trakcie trzeciego etapu działania ISCM są korelowane, analizowane i raportowane kierownictwu wyższego szczebla w ramach czwartego etapu tegoż działania. Jak zaznaczono w [NSC 800-137], informacje związane z bezpieczeństwem są generowane, korelowane, analizowane i raportowane przy użyciu zautomatyzowanych narzędzi, o ile jest to możliwe i praktyczne. Jeżeli okazuje się to niewykonalne lub niepraktyczne, generowanie, korelowanie, analizę i raportowanie w zakresie informacji dotyczących bezpieczeństwa realizuje się metodami ręcznymi lub proceduralnymi. W ten sposób kierownictwo wyższego szczebla otrzymuje informacje związane z bezpieczeństwem niezbędne do podejmowania uzasadnionych, opartych na ryzyku decyzji dotyczących zagrożeń dla misji i działalności w obszarze bezpieczeństwa informacji.[66]

Automatyzacja procesu oceny jest podstawowym elementem pomagającym organizacjom w zarządzaniu ryzykiem związanym z bezpieczeństwem informacji

[65] Dokument [NSC 800-137] zawiera wskazówki dotyczące działań ISCM. Dokument [NSC 800-137A] zawiera wskazówki dotyczące oceny programów działań ISCM.

[66] Ciągłe monitorowanie może być skutecznie stosowane w odniesieniu do środków ochrony prywatności zgodnie z koncepcjami, technikami i zasadami opisanymi w [NSC 800-137]. Wytyczne dotyczące bieżącego monitorowania środków ochrony prywatności zapewniają osoby wyższego szczebla ds. prywatności (SAOP)/kierownicy ds. prywatności (CPO).

i ochroną prywatności. Stale ewoluujące zagrożenia i zmiany w zakresie przetwarzania danych identyfikacyjnych stanowią wyzwanie dla organizacji projektujących, wdrażających i eksploatujących złożone systemy składające się z wielu rodzajów komponentów sprzętowych i oprogramowania, w tym oprogramowania sprzętowego. Posiadanie zdolności do oceny wszystkich wdrożonych środków bezpieczeństwa i ochrony prywatności przy użyciu metod ręcznych lub proceduralnych z wymaganą częstotliwością stało się dla większości organizacji niepraktyczne ze względu na skalę i złożoność ich infrastruktury informatycznej.

Strategia mająca na celu zwiększenie liczby środków bezpieczeństwa i ochrony prywatności, w przypadku których można zautomatyzować proces oceny i monitorowania, zależy od *specyfikacji pożądanego stanu* oraz wyrażenia go w formie, którą można porównać automatycznie (tj. na podstawie danych) ze stanem rzeczywistym. Pożądany stan to zdefiniowana wartość, tj. *specyfikacja*, do której można porównać stan rzeczywisty. Rozbieżność pomiędzy tymi dwoma wartościami wskazuje na wadę co najmniej jednego ze stosowanych zabezpieczeń. Przykładowo polityka organizacji może określać, że konta użytkowników są blokowane po trzech nieudanych próbach logowania. Wówczas w pożądanej specyfikacji stanu określono by, że odpowiednie urządzenia są skonfigurowane do blokowania kont po trzech nieudanych próbach logowania. Jeśli informacje związane z bezpieczeństwem zebrane podczas zautomatyzowanej oceny wskazują, iż dane urządzenie jest skonfigurowane tak, że konta są blokowane dopiero po pięciu nieudanych próbach logowania, to wówczas identyfikowana jest niezgodność między stanem pożądanym (dozwolone trzy próby przed zablokowaniem konta) a stanem rzeczywistym (dozwolone pięć prób przed zablokowaniem konta). Niezgodność może wskazywać na problem ze skutecznością następujących zabezpieczeń wdrożonych zgodnie z NSC 800-53: AC-7 „Nieudane próby logowania”; AC-2 „Zarządzanie kontami”; lub CM-2 „Konfiguracja bazowa”. W przypadku stosowania strategii specyfikacji pożądanego stanu informacje związane z bezpieczeństwem generowane w ramach działań ISCM są równoważne wynikom oceny środków bezpieczeństwa.

W celu skutecznej automatyzacji oceny środków bezpieczeństwa i ochrony prywatności z wykorzystaniem strategii specyfikacji pożądanego stanu należy spełnić następujące warunki wstępne:

- Zdefiniowanie zautomatyzowanych specyfikacji rzeczywistego stanu i zachowania.
- Zdefiniowanie specyfikacji pożądanego stanu (porównywalnych ze stanem rzeczywistym) w oparciu o dane.
- Zdefiniowanie metody obliczania lub identyfikowania wad (tj. różnic między stanem i zachowaniem pożądanym a rzeczywistym).

Po spełnieniu warunków wstępnych system oceny może automatycznie wykryć występujące różnice między stanem pożądanym a rzeczywistym (wady), a następnie wykorzystać te informacje do wygenerowania raportów z oceny środków bezpieczeństwa i ochrony prywatności oraz dostarczyć je wyznaczonemu personelowi za pośrednictwem konsoli zarządzania środkami bezpieczeństwa i prywatności (pulpitu nawigacyjnego).

Jeżeli do przeprowadzania ocen wykorzystywane są zautomatyzowane narzędzia, stosuje się metodę oceny testowej.[67] Organizacja określa i dokumentuje konkretne funkcje[68] oraz środki ochrony prywatności oceniane przez zautomatyzowane narzędzie, jak również częstotliwość oceny takich funkcji lub środków, a także związane z nimi wymagania dotyczące analizy i raportowania.

[67] Jeżeli w celu zapewnienia większego stopnia pewności wymagane jest zwiększenie głębokości i zakresu, zautomatyzowana metoda testowa może zostać uzupełniona przez zastosowanie ręcznych lub proceduralnych metod oceny (tj. wywiad, badanie lub test ręczny).

[68] Jeśli zdefiniowano funkcję bezpieczeństwa lub ochrony prywatności, dokumentuje się proces mapowania wszystkich poszczególnych zabezpieczeń wspierających taką funkcję. W przypadku zdefiniowania przez organizację wielu funkcji oczekuje się istnienia relacji wiele-do-wielu pomiędzy środkami bezpieczeństwa i ochrony prywatności a samymi funkcjami. Więcej informacji na temat oceny funkcji bezpieczeństwa i ochrony prywatności zawarto w punkcie 3.5.

Informacje uzupełniające:

Aby pomóc w automatyzacji bieżących ocen, amerykański Narodowy Instytut Standaryzacji i Technologii (NIST) oraz Agencja Bezpieczeństwa Infrastruktury Cybernetycznej Departamentu Bezpieczeństwa Wewnętrznego (CISA) nawiązały współpracę w celu opracowania procesu opartego na metodzie oceny testowej, zgodnego z ramami zarządzania ryzykiem (ang.: Risk Management Framework) opisanymi w SP 800-37 oraz wytycznymi w zakresie ISCM zawartymi w SP 800-137. Proces automatyzacji ocen opisano w raporcie NIST: NIST Interagency/Internal Report (NISTIR) 8011, Automation Support for Security Control Assessments: Volume 1: Overview [IR 8011-1]. Dokument ten definiuje również konkretne funkcje bezpieczeństwa, a także przedstawia ogólny opis zautomatyzowanego procesu oceny. Konkretne metody automatyzacji oceny indywidualnych funkcji bezpieczeństwa zawarto w dalszych tomach dokumentu NISTIR 8011. Automatyzację metody testowej wykorzystywanej na potrzeby ocen bezpieczeństwa ułatwia program ciągłej diagnostyki i łagodzenia skutków (ang. Continuous Diagnostics and Mitigation — CDM) autorstwa CISA.

REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[69]	
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 systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B

[69] Narodowe Standardy Cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl (www.gov.pl)

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[69]	
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60

PUBLIKACJE ANGLOJĘZYCZNE[70]	
LAWS AND EXECUTIVE ORDERS	
[EGOV]	E-Government Act [includes FISMA] (P.L. 107-347), December 2002. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283
[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.govinfo.gov/content/pkg/PLAW-104publ231/pdf/PLAW-104publ231.pdf
[PRIVACT]	Privacy Act (P.L. 93-579), December 1974. https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf
[USC 3502]	"Definitions," Title 44 U.S. Code, Sec. 3502. 2011 ed. https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44- chap35-subchapI-sec3502
[USC 11101]	"Definitions," Title 40 U.S. Code, Sec. 11101. 2018 ed. https://www.govinfo.gov/app/details/USCODE-2018-title40/USCODE-2018-title40- subtitleIII-chap111-sec11101

[70] Publikacje angielski zostały podane w celach uzupełniających dla osób zainteresowanych. Odniesienia cytowane w tym załączniku to publikacje zewnętrzne, które bezpośrednio wspierają projekty FISMA i prywatności w NIST. Dodatkowe standardy, wytyczne i raporty międzyagencyjne NIST są również przytaczane w całej niniejszej publikacji, w tym w części referencyjnej dotyczącej odpowiednich procedur oceny zabezpieczeń zawartych w rozdziale czwartym. Aby uzyskać dostęp do tych publikacji, podano bezpośrednie linki do strony internetowej NIST.

PUBLIKACJE ANGLOJĘZYCZNE[70]

POLICIES, DIRECTIVES, AND INSTRUCTIONS

[OMB A-130]	Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[OMB M-17-12]	Office of Management and Budget Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf
[CNSSI 1253]	Committee on National Security Systems Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[CNSSI 4009]	Committee on National Security Systems Instruction No. 4009, *Committee on National Security Systems (CNSS) Glossary*, April 2015. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

STANDARDS, GUIDELINES, AND REPORTS

[FIPS 140-3]	National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3
[FIPS 199]	National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

PUBLIKACJE ANGLOJĘZYCZNE[70]	
[FIPS 200]	National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200
[ISO 15026]	International Organization for Standardization/International Electrotechnical Commission (2019) *ISO/IEC/IEEE 15026-1:2019 — Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary* https://www.iso.org/standard/73567.html
[ISO 15288]	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2015) *ISO/IEC/IEEE 15288:2015 — Systems and software engineering — Systems life cycle processes.* https://www.iso.org/standard/63711.html
[ISO 15408]	International Organization for Standardization/International Electrotechnical Commission (2009) *ISO/IEC/IEEE 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model* https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
[ISO 29100]	International Organization for Standardization/International Electrotechnical Commission 29100:2011, Information technology—Security techniques—Privacy framework, December 2011. https://www.iso.org/standard/45123.html
[SP 800-18]	Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1.

PUBLIKACJE ANGLOJĘZYCZNE[70]	
	https://doi.org/10.6028/NIST.SP.800-18r1
[SP 800-30]	Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1
[FIPS 140-3]	National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3
[FIPS 199]	National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199
[FIPS 200]	National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200
[SP 800-37]	Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2
[SP 800-39]	Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.

PUBLIKACJE ANGLOJĘZYCZNE[70]	
	https://doi.org/10.6028/NIST.SP.800-39
[SP 800-40]	Souppaya MP, Scarfone KA (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3. https://doi.org/10.6028/NIST.SP.800-40r3
[SP 800-47]	Dempsey KL, Pillitteri VY, Regenscheid A (2021) Managing the Security of Information Exchanges. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47, Rev. 1. https://doi.org/10.6028/NIST.SP.800-47r1
[SP 800-53]	Joint Task Force Transformation Initiative (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 20, 2020. https://doi.org/10.6028/NIST.SP.800-53r5
[SP 800-53B]	Joint Task Force (2020) Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B. https://doi.org/10.6028/NIST.SP.800-53B
[SP 800-60-1]	Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

PUBLIKACJE ANGLOJĘZYCZNE[70]	
[SP 800-60-2]	Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1
[SP 800-115]	Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115
[SP 800-128]	Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128
[SP 800-137]	Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137
[SP 800-137A]	Dempsey KL, Pillitteri VY, Baer C, Niemeyer R, Rudman R, Urban S (2020) Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137A. https://doi.org/10.6028/NIST.SP.800-137A
[SP 800-161]	Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161.

PUBLIKACJE ANGLOJĘZYCZNE[70]	
	https://doi.org/10.6028/NIST.SP.800-161
[SP 800-181]	Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1
[IR 8011-1]	Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 1: Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 1. https://doi.org/10.6028/NIST.IR.8011-1
[IR 8011-2]	Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 2. https://doi.org/10.6028/NIST.IR.8011-2
[IR 8011-3]	Dempsey KL, Eavy P, Goren N, Moore G (2018) Automation Support for Security Control Assessments: Volume 3: Software Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 3. https://doi.org/10.6028/NIST.IR.8011-3
[IR 8011-4]	Dempsey KL, Takamura E, Eavy P, Moore G (2020) Automation Support for Security Control Assessments: Volume 4: Software Vulnerability Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 4. https://doi.org/10.6028/NIST.IR.8011-4

PUBLIKACJE ANGLOJĘZYCZNE[70]	
[IR 8062]	Brooks S, Garcia M, Lefkovitz N, Lightman S, Nadeau E (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062
	WHITE PAPERS, WEBSITES, AND DATA SETS
[FedRAMP]	General Services Administration (2022) *Federal Risk and Authorization Management Program (FedRAMP).* https://www.fedramp.gov
[NARA CUI]	National Archives and Records Administration (2022) *Controlled Unclassified Information (CUI) Registry*. https://www.archives.gov/cui
[OSCAL]	National Institute of Standards and Technology (2022) *OSCAL: the Open Security Controls Assessment Language.* https://pages.nist.gov/OSCAL/
[OSCAL content]	National Institute of Standards and Technology (2022) *oscal-content* [usnistgov Git Repository]. https://github.com/usnistgov/oscal-content
[SEI]	Weinstock CB, Lipson HF, Goodenough J (2007) Arguing Security – Creating Security Assurance Cases. (Software Engineering Institute, Carnegie Mellon University, Pittsburg, PA.). https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_293637.pdf