Kancelaria Prezesa
Rady Ministrów

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-53A wer. 1.0

Załącznik F - Procedury oceny bezpieczeństwa

21 grudnia 2022

Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji

Tworzenie skutecznych planów oceny

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

PREAMBUŁA

Szanowni Państwo,

oddajemy w Państwa ręce zestaw publikacji specjalnych - 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.

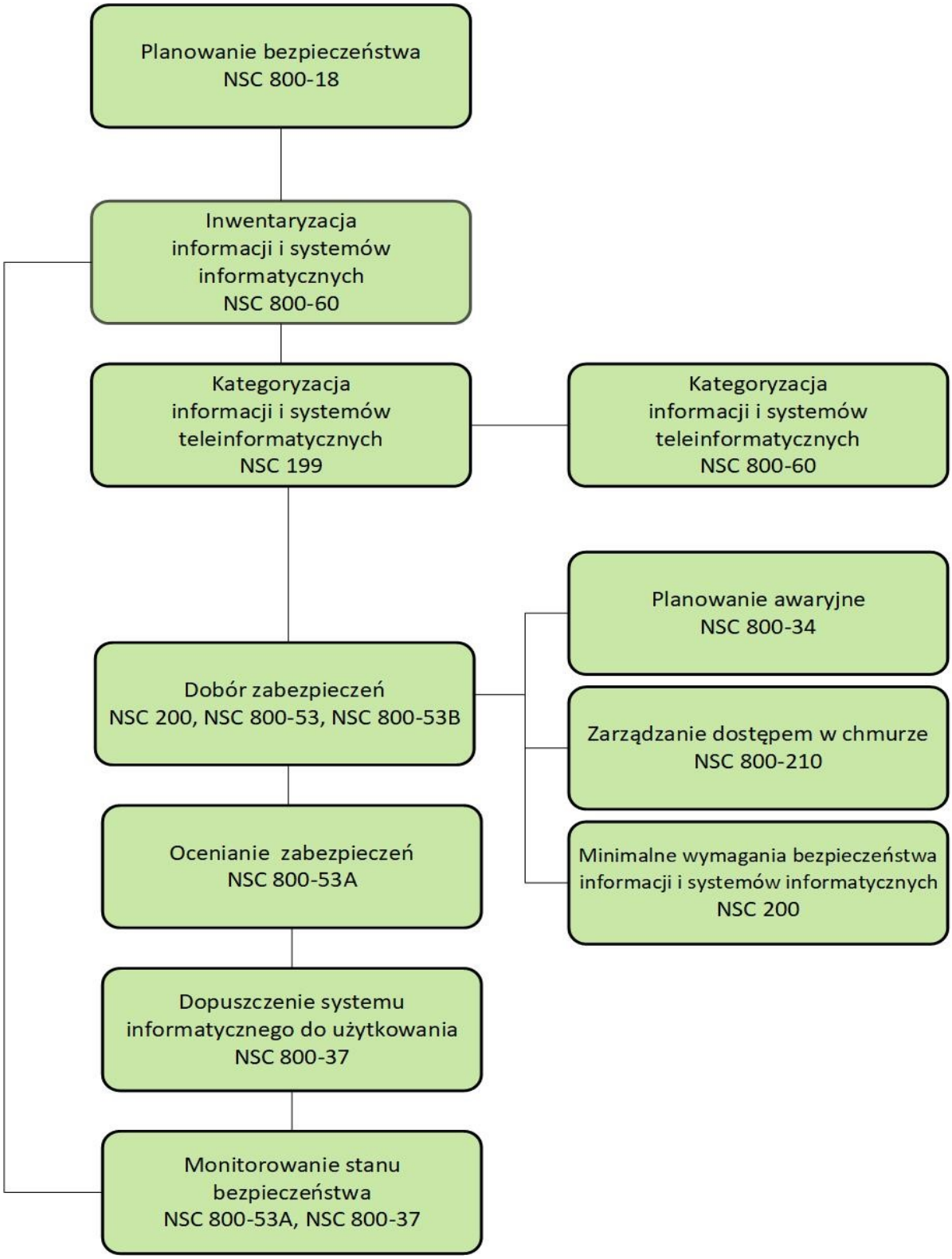
Zestaw publikacji specjalnych obejmuje następujące pozycje:

- 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 systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53.
- NSC 800-53A, Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A.
- 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.

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

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

Niniejsza publikacja NSC 800-53A, ***Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny. Załącznik F - Procedury oceny bezpieczeństwa*** , opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-53A, Rev. 4., *Assessing Security and Privacy Controls in Federal Information Systems and Organizations. Building Effective Assessment Plans.*

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.

Spis treści

CELE, METODY I OBIEKTY DO OCENY ŚRODKÓW BEZPIECZEŃSTWA

Załącznik zawiera katalog procedur oceny środków bezpieczeństwa i usprawnień zabezpieczeń zawartych w standardzie NSC 800-53 wer. 1.[2] Oceniający wybierają procedury oceny z katalogu zgodnie z wytycznymi podanymi w sekcji 3.2 standardu NSC 800-53A. Ponieważ treść planu bezpieczeństwa ma wpływ na opracowanie planu oceny w zakresie ochrony, a także proces oceny, w katalogu prawdopodobnie znajdą się procedury oceny, których osoby oceniające nie będą stosować, ponieważ: (I) kojarzone środki bezpieczeństwa lub zabezpieczenia rozszerzone nie są zawarte w planie ochrony systemu informacyjnego; (II) środki bezpieczeństwa lub zabezpieczenia rozszerzone nie są poddawane ocenie w tym konkretnym okresie.

Cele oceny są kolejno ponumerowane. Najpierw zgodnie ze schematem numeracji zawartej w standardzie NSC 800-53 wer. 1. Następnie, w razie potrzeby, w celu dalszego podziału wymogów bezpieczeństwa lub ochrony prywatności, aby ułatwić ocenę, stosuje się kolejne numery lub litery w nawiasach kwadratowych [ ], w przeciwieństwie do nawiasów okrągłych ( ), w celu dokonania tego wyróżnienia (np. CP-9(a), CP-9(a)[1], CP-9(a)[2], CP-9(b)[1], CP-9(b)[2], CP-9(c)[1], CP-9(c)[2], CP-9(d) itd.). Początkowy znak w nawiasie kwadratowym jest zawsze liczbą. W przypadku niektórych środków bezpieczeństwa, kolumna z początkowym oznaczeniem zabezpieczenia (np. CP-9, CP-9(a), CP-9(b) i CP-9(c)) jest po prostu miejscem, które ułatwia rozdział zabezpieczenia przy zachowaniu schematu formatowania. Chociaż w przypadku każdej określonej metody oceny nie jest to wyraźnie zaznaczone w procedurze oceny, wartości atrybutu szczegółowości i zasięgu, opisane w Załączniku D, są przypisywane przez organizację i stosowane przez osobę oceniającą / zespół oceniający w trakcie wykonywania metody oceny w odniesieniu do obiektu oceny.

[2] W przypadku jakichkolwiek różnic między celami oceny określonymi w ocenie środków bezpieczeństwa, a podstawowymi celami wyrażonymi w oświadczeniach o stosowanych środkach zabezpieczeń określonych w standardzie NSC 800-53 wer. 1, zabezpieczenia podstawowe i zabezpieczenia rozszerzone zawarte w NSC 800-53 wer. 1 pozostają ostateczne.

Jeżeli zabezpieczenie posiada jakiekolwiek zabezpieczenia rozszerzające (oznaczone sekwencyjnymi numerami w nawiasach okrągłych, na przykład CP-9 (3) dla trzeciego zabezpieczenia rozszerzającego zabezpieczenie CP-9), cele oceny są opracowywane dla każdego rozszerzenia przy użyciu tego samego procesu, co dla zabezpieczenia podstawowego. Wynikowe cele oceny są numerowane sekwencyjnie w taki sam sposób, jak procedura oceny zabezpieczenia podstawowego, najpierw zgodnie ze schematem numeracji zawartym w standardzie NSC 800-53 wer. 1, a następnie, aby ułatwić ocenę, przy użyciu sekwencyjnych numerów lub liter w nawiasach w celu dalszego podziału wymagań dotyczących rozszerzeń zabezpieczeń (np. CP-9(3)[1], CP-9(3)[2]).

Ten sam obiekt oceny może pojawić się na wielu listach obiektów w różnych procedurach oceny. Może być wykorzystywany w wielu kontekstach w celu uzyskania niezbędnych informacji lub dowodów dotyczących określonego aspektu oceny. Oceniający korzystają z ogólnych odniesień, w stosownych przypadkach, w celu uzyskania informacji niezbędnych do dokonania określonych ustaleń wymaganych w ramach celu oceny. Na przykład, odniesienie do polityki kontroli dostępu pojawia się w procedurach oceny zabezpieczeń AC-2 i AC-7. W przypadku procedury oceny zabezpieczenia AC-2, osoby oceniające korzystają z polityki kontroli dostępu w celu znalezienia informacji na temat tej części polityki, która dotyczy zarządzania kontami w systemie informacyjnym. W przypadku procedury oceny zabezpieczenia AC-7, osoby oceniające korzystają z polityki kontroli dostępu w celu znalezienia informacji na temat tej części polityki, która dotyczy nieudanych prób logowania do systemu informacyjnego. Oceniający są odpowiedzialni za łączenie i konsolidację procedur oceny, gdy tylko jest to możliwe lub praktyczne. Optymalizacja procedur oceny może zaoszczędzić czas, zmniejszyć koszty oceny i zmaksymalizować użyteczność wyników oceny. Oceniający optymalizują procedury oceniania poprzez określenie najlepszej kolejności ich przeprowadzania. Ocena niektórych środków bezpieczeństwa przed innymi, może dostarczyć informacji ułatwiających zrozumienie i ocenę tych innych środków bezpieczeństwa.

WSKAZÓWKI IMPLEMENTACYJNE

1. Ze standardu NSC 800-53A Załącznik F należy wybrać tylko te procedury oceny, które odpowiadają środkom bezpieczeństwa i zabezpieczeniom rozszerzonym zawartym w zatwierdzonym planie bezpieczeństwa i które mają być uwzględnione w ocenie.
2. Procedury oceny wybrane z Załącznika F są przykładowymi procedurami, które służą jako punkt wyjścia dla organizacji przygotowujących się do oceny. Te procedury oceny są dostosowane do potrzeb, zgodnie z wytycznymi zawartymi w sekcji 3.2 standardu NSC 800-53A, w celu dostosowania procedur do konkretnych wymagań organizacji i środowiska pracy.
3. W odniesieniu do procedur oceny wymienionych w Załączniku F, osoby oceniające muszą stosować jedynie te procedury, metody i obiekty, które są niezbędne do ostatecznego stwierdzenia, że dany cel środka bezpieczeństwa jest satysfakcjonujący (został spełniony) lub niesatysfakcjonujący (nie został spełniony) - patrz sekcja 3.3.
4. W odniesieniu do każdej metody oceny, osoby oceniające stosują wartości dotyczące atrybutu szczegółowości i zakresu stosowania (opisane w Załączniku D), współmierne do charakterystyki systemu informacyjnego (w tym wymogów w zakresie wiarygodności) oraz konkretnego działania związanego z oceną, które pomaga określić skuteczność ocenianych środków bezpieczeństwa. Wartości wybrane dla atrybutów szczegółowości i zasięgu wskazują na względny wysiłek wymagany do zastosowania metody oceny do ocenianego obiektu (tj. rygor i zakres działań związanych z oceną). Atrybuty szczegółowości i zasięgu, choć nie są powtarzane w każdej procedurze oceny przedstawionej w niniejszym załączniku, można przedstawić w następujący sposób:

Rozmowa kwalifikacyjna:[*wartości atrybutu oceny*: <szczegółowość>, <zasięg>]. [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie awaryjne i realizację planu].

5. Oceniający mogą znaleźć przydatne informacje dotyczące oceny w sekcji dodatkowych wytycznych dla każdego środka bezpieczeństwa opisanego w standardzie NSC 800-53 wer. 1. Informacje te mogą być wykorzystane do przeprowadzenia bardziej skutecznych ocen w odniesieniu do stosowanej procedury oceny.

Uwaga: Oceniając zgodność organizacji ze standardami NSC, audytorzy, osoby oceniające, inspektorzy generalni, biegli i/lub rzeczoznawcy, biorą pod uwagę intencje koncepcji i zasad bezpieczeństwa sformułowanych w poszczególnych wytycznych oraz sposób, w jaki organizacja zastosowała wytyczne w kontekście swoich szczególnych obowiązków służbowych, środowiska operacyjnego i unikalnych warunków organizacyjnych.

OSTRZEŻENIE

Chociaż zestaw potencjalnych metod oceny został włączony do poniższego katalogu procedur oceniania, nie muszą one być ani obowiązkowe, ani wyłączne. W zależności od szczególnych właściwości systemu informacyjnego lub działalności organizacji, które mają być poddane ocenie, nie wszystkie czynności oceny mogą być wymagane, a także mogą być również stosowane inne metody. Ponadto zestaw potencjalnych przedmiotów oceny wymienionych w katalogu nie jest obowiązkowy, lecz jest to pakiet, z którego można wybrać niezbędny i wystarczający zbiór przedmiotów do danej oceny w celu stwierdzenia stosownych ustaleń.

KATEGORIA AC - KONTROLA DOSTĘPU

AC-1	**POLITYKA I PROCEDURY KONTROLI DOSTĘPU**			
	CEL OCENY: **Ustalenie, czy organizacja:**			
	AC-1(a)(1)	**AC-1(a)(1)[1]**	*opracowuje i dokumentuje politykę kontroli dostępu, która dotyczy:*	
			AC-1(a)(1)[1][a]	*celu;*
			AC-1(a)(1)[1][b]	*zakresu stosowania;*
			AC-1(a)(1)[1][c]	*ról;*
			AC-1(a)(1)[1][d]	*odpowiedzialności;*
			AC-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			AC-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			AC-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		AC-1(a)(1)[2]	*określa personel lub role, którym ma być rozpowszechniona polityka kontroli dostępu;*	
		AC-1(a)(1)[3]	*rozpowszechnia zasady kontroli dostępu personelu lub ról zdefiniowanych przez organizację;*	
	AC-1(a)(2)	**AC-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrażanie zasad kontroli dostępu i związanych z nimi zabezpieczeń kontroli dostępu;*	
		AC-1(a)(2)[2]	*określa personel lub role, którym procedury mają być rozpowszechniane;*	
		AC-1(a)(2)[3]	*rozpowszechnia personelowi lub rolom procedury określone w organizacji;*	
	AC-1(b)(1)	**AC-1(b)(1)[1]**	*określa częstotliwość przeglądania i aktualizowania bieżących zasad kontroli dostępu;*	
		AC-1(b)(1)[2]	*określa częstotliwość przeglądania i aktualizowania bieżących zasad kontroli dostępu;*	

AC-1	**POLITYKA I PROCEDURY KONTROLI DOSTĘPU**		
	AC-1(b)(2)	**AC-1(b)(2)[1]**	*określa częstotliwość przeglądu i aktualizacji stosowanych procedur kontroli dostępu;*
		AC-1(b)(2)[2]	*przegląda i aktualizuje bieżące procedury kontroli dostępu z częstotliwością zdefiniowaną w organizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród: Zasady i procedury kontroli dostępu; Inne stosowne dokumenty lub rejestry*]. **Wywiad:** [*wybierz spośród:* Personel organizacji z obowiązkami w zakresie kontroli dostępu; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

AC-2	**ZARZĄDZANIE KONTAMI**		
	CEL OCENY: *Określić, czy organizacja:*		
	AC-2(a)	**AC-2(a)[1]**	*definiuje typy kont systemu informacyjnego, które mają być zidentyfikowane i wybrane do obsługi misji organizacyjnych/funkcji biznesowych;*
		AC-2(a)[2]	*identyfikuje i wybiera zdefiniowane w organizacji typy kont systemu informacyjnego do obsługi misji organizacyjnych/funkcji biznesowych;*
	AC-2(b)	*przypisuje menedżerów kont dla kont systemu informacyjnego;*	
	AC-2(c)	*ustanawia warunki członkostwa w grupach i rolach;*	
	AC-2(d)	*określa dla każdego konta (zgodnie z wymaganiami):*	
		AC-2(d)[1]	*autoryzowanych użytkowników systemu informacyjnego;*
		AC-2(d)[2]	*przynależność do grupy i roli;*
		AC-2(d)[3]	*autoryzacje dostępu (tj. uprawnienia);*
		AC-2(d)[4]	*inne atrybuty;*
	AC-2(e)	**AC-2(e)[1]**	*definiuje personel lub role wymagane do zatwierdzania żądań utworzenia kont systemu informacyjnego;*

AC-2	**ZARZĄDZANIE KONTAMI**			
		AC-2(e)[2]	*wymaga zatwierdzenia przez personel lub role zdefiniowane przez organizację, żądań tworzenia kont systemu informacyjnego;*	
	AC-2(f)	**AC-2(f)[1]**	*określa procedury lub warunki, aby:*	
			AC-2(f)[1][a]	*tworzyć konta w systemie informacyjnym;*
			AC-2(f)[1][b]	*włączać konta w systemie informacyjnym;*
			AC-2(f)[1][c]	*modyfikować konta w systemie informacyjnym;*
			AC-2(f)[1][d]	*wyłączyć konta w systemie informacyjnym;*
			AC-2(f)[1][e]	*usuwać konta w systemie informacyjnym;*
		AC-2(f)[2]	*zgodnie z określonymi przez organizację procedurami lub warunkami:*	
			AC-2(f)[2][a]	*tworzy konta w systemie informacyjnym;*
			AC-2(f)[2][b]	*umożliwia korzystanie z kont systemu informacyjnego;*
			AC-2(f)[2][c]	*modyfikuje konta w systemie informacyjnym;*
			AC-2(f)[2][d]	*wyłącza konta w systemie informacyjnym;*
			AC-2(f)[2][e]	*usuwa konta z systemu informacyjnego;*
	AC-2(g)	*monitoruje korzystanie z kont systemu informacyjnego;*		
	AC-2(h)	*powiadamia menedżerów kont, gdy:*		
		AC-2(h)(1)	*konta nie są już wymagane;*	
		AC-2(h)(2)	*użytkownicy zostają zwolnieni lub przeniesieni;*	
		AC-2(h)(3)	*poszczególne systemy informacyjne wymagają zmian:*	
	AC-2(l)	*upoważnia do dostępu do systemu informacyjnego na podstawie:*		
		AC-2(l)(1)	*ważnego upoważnienia dostępu;*	

AC-2	**ZARZĄDZANIE KONTAMI**		
		AC-2(I)(2)	*zamierzonego wykorzystania systemu;*
		AC-2(I)(3)	*innych atrybutów wymaganych przez organizację lub powiązanych z nimi misji/ funkcji biznesowych;*
	AC-2(j)	**AC-2(j)[1]**	*określa częstotliwość przeglądów kont pod kątem zgodności z wymogami zarządzania kontami;*
		AC-2(j)[2]	*przegląda konta pod kątem zgodności z wymaganiami zarządzania kontami z częstotliwością określoną przez organizację;*
	AC-2(k)	*ustanawia proces ponownego wystawiania poświadczeń konta udostępnionego/grupy (jeśli jest wdrożona), gdy osoby są usuwane z grupy.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzania kontem; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz aktywnych kont systemowych wraz z nazwą osoby kojarzonej z każdym kontem; wykaz warunków członkostwa w grupach i rolach; powiadomienia lub rejestry niedawno przeniesionych, wydzielonych lub zwolnionych pracowników; lista ostatnio wyłączonych kont systemu informacyjnego wraz z nazwą osoby kojarzonej z każdym kontem; rekordy autoryzacji dostępu; przeglądy zgodności z przepisami dotyczącymi zarządzania kontami; rejestry monitorowania systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania kontem w systemie informacyjnym; zautomatyzowane mechanizmy wdrażania zarządzania kontem].		

AC-2(1)	**ZARZĄDZANIE KONTAMI | *ZAUTOMATYZOWANE ZARZĄDZANIE KONTAMI SYSTEMU***
	CEL OCENY: *Określić, czy organizacja wykorzystuje zautomatyzowane mechanizmy wspierające zarządzanie kontami systemów informacyjnych.*

AC-2(1)	**ZARZĄDZANIE KONTAMI | *ZAUTOMATYZOWANE ZARZĄDZANIE KONTAMI SYSTEMU***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące ZARZĄDZANIE KONTAMI; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracyjne systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; programiści systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające funkcje zarządzania kontami].

AC-2(2)	**ZARZĄDZANIE KONTAMI | *USUWANIE KONT TYMCZASOWYCH/ AWARYJNYCH***	
	CEL OCENY: *Określić, czy:*	
	AC-2(2)[1]	*organizacja określa okres, po upływie którego system informacyjny automatycznie usuwa lub wyłącza konta tymczasowe i awaryjne; oraz*
	AC-2(2)[2]	*system informacyjny automatycznie usuwa lub wyłącza konta tymczasowe i awaryjne po okresie zdefiniowanym przez organizację dla każdego typu konta.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzanie kontami; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wygenerowana przez system informacyjny lista kont tymczasowych usuniętych i/lub wyłączonych; wygenerowany przez system informacyjny wykaz kont awaryjnych, usuniętych i/lub wyłączonych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; programiści systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające funkcje zarządzania kontami].	

AC-2(3)	**ZARZĄDZANIE KONTAMI | *WYŁĄCZANIE KONT NIEAKTYWNYCH***	
	CEL OCENY: *Określić, czy:*	
	AC-2(3)[1]	*organizacja określa okres czasu, po którym system informacyjny automatycznie wyłącza nieaktywne konta; oraz*
	AC-2(3)[2]	*system informacyjny automatycznie wyłącza nieaktywne konta po upływie określonego przez organizację okresu czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzanie kontami; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wygenerowana przez system informacyjny lista kont tymczasowych usuniętych i/lub wyłączonych; wygenerowany przez system informacyjny wykaz kont awaryjnych, usuniętych i/lub wyłączonych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; programiści systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające funkcje zarządzania kontami].	

AC-2(4)	**ZARZĄDZANIE KONTAMI | *ZAUTOMATYZOWANE DZIAŁANIA AUDYTOWE***		
	CEL OCENY: *Określić, czy:*		
	AC-2(4)[1]	*system informacyjny automatycznie kontroluje następujące działania na koncie:*	
		AC-2(4)[1][a]	*tworzenie;*
		AC-2(4)[1][b]	*modyfikacje;*
		AC-2(4)[1][c]	*włączanie;*
		AC-2(4)[1][d]	*wyłączanie;*

AC-2(4)	**ZARZĄDZANIE KONTAMI | *ZAUTOMATYZOWANE DZIAŁANIA AUDYTOWE***		
		AC-2(4)[1][e]	*usuwanie;*
	AC-2(4)[2]	*organizacja określa personel lub role, które należy powiadomić o następujących działaniach związanych z rachunkiem:*	
		AC-2(4)[2][a]	*tworzenie;*
		AC-2(4)[2][b]	*modyfikacje;*
		AC-2(4)[2][c]	*włączanie;*
		AC-2(4)[2][d]	*wyłączanie;*
		AC-2(4)[2][e]	*usuwanie;*
	AC-2(4)[3]	*system informacyjny powiadamia określony przez organizację personel lub role o następujących czynnościach związanych z kontem:*	
		AC-2(4)[3][a]	*tworzenie;*
		AC-2(4)[3][b]	*modyfikacje;*
		AC-2(4)[3][c]	*włączanie;*
		AC-2(4)[3][d]	*wyłączanie;*
		AC-2(4)[3][e]	*usuwanie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; powiadomienia o utworzeniu, modyfikacji, włączeniu, wyłączeniu i usunięciu konta; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające funkcje zarządzania kontami].		

AC-2(5)	**ZARZĄDZANIE KONTAMI | *WYLOGOWANIE PO OKREŚLONYM OKRESIE NIEAKTYWNOŚCI***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-2(5)[1]	*definiuje, albo okres oczekiwanej nieaktywności, który wymaga wylogowania się użytkowników, albo opisuje, kiedy użytkownicy są zobowiązani do wylogowania się; oraz*
	AC-2(5)[2]	*wymaga, aby użytkownicy wylogowali się po osiągnięciu zdefiniowanego przez organizację okresu braku aktywności lub zgodnie ze zdefiniowanym przez organizację opisem momentu wylogowania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzania kontami; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; raporty o naruszeniach bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; użytkownicy, którzy muszą przestrzegać zasad wylogowania po określonym okresie nieaktywności].	

AC-2(6)	**ZARZĄDZANIE KONTAMI | *DYNAMICZNE ZARZĄDZANIE UPRAWNIENIAMI***	
	CEL OCENY: *Określić, czy:*	
	AC-2(6)[1]	*organizacja definiuje listę dynamicznego zarządzania uprawnieniami, które mają być wdrażane przez system informacyjny; oraz*
	AC-2(6)[2]	*system informacyjny implementuje zdefiniowaną przez organizację listę możliwości dynamicznego zarządzania uprawnieniami.*

AC-2(6)	**ZARZĄDZANIE KONTAMI | *DYNAMICZNE ZARZĄDZANIE UPRAWNIENIAMI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista dynamicznego zarządzania uprawnieniami; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; programiści systemów]. **Test**: [*wybierz spośród:* System informacyjny wdrażający dynamiczne zarządzanie uprawnieniami].

AC-2(7)	**ZARZĄDZANIE KONTAMI | *SCHEMATY KONTROLI DOSTĘPU OPARTE NA ROLACH***		
	CEL OCENY: *Określić, czy organizacja:*		
	AC-2(7)(a)	*ustanawia i administruje uprzywilejowanymi kontami użytkowników zgodnie ze schematem dostępu opartego na rolach, który organizuje dozwolony dostęp do systemu informacyjnego i uprawnienia do ról;*	
	AC-2(7)(b)	*monitoruje przypisania uprzywilejowanych ról;*	
	AC-2(7)(c)	**AC-2(7)(c)[1]**	*określa działania, które należy podjąć w przypadku, gdy przydział uprzywilejowanych ról nie jest już właściwy; oraz*
		AC-2(7)(c)[2]	*podejmuje działania zdefiniowane przez organizację, gdy przypisanie uprzywilejowanych ról nie jest już właściwe.*

AC-2(7)	**ZARZĄDZANIE KONTAMI | *SCHEMATY KONTROLI DOSTĘPU OPARTE NA ROLACH***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; generowana przez system informacyjny lista kont uprzywilejowanych użytkowników i związanych z nimi ról; zapisy działań podejmowanych w przypadku, gdy przypisanie uprzywilejowanych ról nie jest już właściwe; zapisy z audytu systemu informacyjnego; sprawozdania z audytu i monitorowania; zapisy z monitorowania systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające funkcje zarządzania kontami; zautomatyzowane mechanizmy monitorowania przydziałów uprzywilejowanych ról].

AC-2(8)	**ZARZĄDZANIE KONTAMI | *TWORZENIE KONTA DYNAMICZNEGO***	
	CEL OCENY: *Określić, czy:*	
	AC-2(8)[1]	*organizacja definiuje konta systemu informacyjnego, które mają być dynamicznie tworzone przez system informacyjny; oraz*
	AC-2(8)[2]	*system informacyjny dynamicznie tworzy konta systemu informacyjnego zdefiniowane przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; generowany przez system wykaz kont systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; programiści systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające funkcje zarządzania kontami].	

AC-2(9)	**ZARZĄDZANIE KONTAMI | *ZARZĄDZANIE KONTAMI WSPÓLNYMI \ GRUPOWYMI***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-2(9)[1]	*określa warunki zakładania kont wspólnych/grupowych; oraz*
	AC-2(9)[2]	*zezwala wyłącznie na korzystanie z kont wspólnych/grupowych, które spełniają określone przez organizację warunki dotyczące ustanawiania tego rodzaju kont.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; generowany przez system wykaz kont wspólnych/grupowych i powiązanych ról; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące zarządzanie kontami wspólnymi/grupowymi].	

AC-2(10)	**ZARZĄDZANIE KONTAMI | *REFERENCYJNE ZAMYKANIE KONTA WSPÓLNEGO/ GRUPOWEGO***
	CEL OCENY: *Ustalić, czy system informacyjny zamyka konto wspólne / konto grupowe, gdy członkowie opuszczają grupę.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry dotyczące zamykania dostępu do konta; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

AC-2(10)	**ZARZĄDZANIE KONTAMI | *REFERENCYJNE ZAMYKANIE KONTA WSPÓLNEGO/ GRUPOWEGO***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; programiści systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające funkcje zarządzania kontami].

AC-2(11)	**ZARZĄDZANIE KONTAMI | *WARUNKI UŻYTKOWANIA***	
	CEL OCENY: *Określić, czy:*	
	AC-2(11)[1]	*organizacja określa okoliczności i/lub warunki użytkowania, które mają być egzekwowane w odniesieniu do kont systemu informacyjnego;*
	AC-2(11)[2]	*organizacja określa konta systemu informacyjnego, w stosunku do których mają być egzekwowane okoliczności i/lub warunki użytkowania określone przez organizację; oraz*
	AC-2(11)[3]	*system informacyjny egzekwuje okoliczności i/lub warunki korzystania z kont systemu informacyjnego określone przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; generowany przez system wykaz kont systemu informacyjnego i związane z tym przypisanie okoliczności użytkowania i/lub warunków użytkowania; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; programiści systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające funkcje zarządzania kontami].	

AC-2(12)	**ZARZĄDZANIE KONTAMI | *MONITOROWANIE KONTA, NIETYPOWE UŻYTKOWANIE KONTA***		
	CEL OCENY: *Określić, czy organizacja:*		
	AC-2(12)(a)	**AC-2(12)(a)[1]**	*definiuje nietypowe użycie konta systemu informacyjnego, które ma być monitorowane;*
		AC-2(12)(a)[2]	*monitoruje konta systemów informacyjnych pod kątem nietypowego użycie, według zdefiniowanych przez organizację zasad;*
	AC-2(12)(b)	**AC-2(12)(b)[1]**	*określa personel lub role, do których należy zgłaszać nietypowe korzystanie z kont systemu informacyjnego; oraz*
		AC-2(12)(b)[2]	*zgłasza nietypowe korzystanie z kont systemu informacyjnego do personelu lub ról zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z monitorowania systemu informacyjnego; zapisy z audytu systemu informacyjnego; sprawozdania z monitorowania i śledzenia audytów; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające funkcje zarządzania kontami].		

AC-2(13)	**ZARZĄDZANIE KONTAMI | *WYŁĄCZANIE KONT DOSTĘPOWYCH UŻYTKOWNIKOM WYSOKIEGO RYZYKA***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-2(13)[1]	*definiuje okres czasu, w którym konta są zablokowane po wykryciu znaczącego ryzyka, jakie stwarzają użytkownicy takich kont; oraz*

AC-2(13)	**ZARZĄDZANIE KONTAMI | *WYŁĄCZANIE KONT DOSTĘPOWYCH UŻYTKOWNIKOM WYSOKIEGO RYZYKA***	
	AC-2(13)[2]	*wyłącza konta użytkowników stwarzających istotne ryzyko w określonym przez organizację okresie czasu, od którego ryzyko zostało wykryte.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zarządzanie kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; generowany przez system wykaz kont wyłączonych (nieaktywnych); wykaz aktywności użytkowników stwarzających istotne ryzyko organizacyjne; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające funkcje zarządzania kontami].	

AC-3	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU**
	CEL OCENY: *Określenie, czy system informacyjny wykonuje zatwierdzone upoważnienia do logicznego dostępu do informacji i zasobów systemu zgodnie z obowiązującymi zasadami kontroli dostępu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące egzekwowania prawa dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista zatwierdzonych uprawnień (uprawnień użytkownika); rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania zasad kontroli dostępu].

AC-3(1)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *OGRANICZONY DOSTĘP DO FUNKCJI UPRZYWILEJOWANYCH***
[Włączone do AC-6].	

AC-3(2)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *PODWÓJNA AUTORYZACJA***	
	CEL OCENY: *Określić, czy:*	
	AC-3(2)[1]	*organizacja definiuje uprzywilejowane polecenia i/lub inne działania, dla których ma być egzekwowana podwójna autoryzacja; oraz*
	AC-3(2)[2]	*system informacyjny narzuca podwójną autoryzację dla zdefiniowanych przez organizację uprzywilejowanych poleceń i/lub innych zdefiniowanych przez organizację działań.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące egzekwowania prawa dostępu i podwójnej autoryzacji; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista uprzywilejowanych poleceń wymagających podwójnej autoryzacji; lista działań wymagających podwójnej organizacji; lista zatwierdzonych uprawnień (uprawnień użytkownika); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Mechanizmy podwójnej autoryzacji realizujące politykę kontroli dostępu].	

AC-3(3)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *OBOWIĄZKOWA KONTROLA DOSTĘPU***	
	CEL OCENY: *Określić, czy:*	
	AC-3(3)[1]	*organizacja określa zasady obowiązkowej kontroli dostępu, które mają być egzekwowane we wszystkich podmiotach i obiektach;*

AC-3(3)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *OBOWIĄZKOWA KONTROLA DOSTĘPU***				
	AC-3(3)[2]	*organizacja określa podmioty, w których mają być egzekwowane określone przez organizację zasady obowiązkowej kontroli dostępu;*			
	AC-3(3)[3]	*organizacja określa obiekty, w których mają być egzekwowane określone przez organizację zasady obowiązkowej kontroli dostępu;*			
	AC-3(3)[4]	*organizacja definiuje podmioty, którym można wyraźnie przyznać uprawnienia, tak, aby nie były one limitowane przez ograniczenia określone w innym miejscu tego zabezpieczenia;*			
	AC-3(3)[5]	*organizacja określa uprawnienia, które mogą być przyznane podmiotom określonym przez organizację;*			
	AC-3(3)[6]	*system informacyjny narzuca organizacyjnie zdefiniowane reguły obowiązkowej kontroli dostępu w odniesieniu do wszystkich podmiotów i obiektów, w których ustalono, że:*			
		AC-3(3)[6](a)	*reguła ta jest jednolicie egzekwowana w odniesieniu do wszystkich podmiotów i obiektów znajdujących się w granicach systemu informacyjnego*		
		AC-3(3)[6](b)	*podmiot, któremu udzielono dostępu do informacji, nie jest upoważniony do wykonywania następujących działań:*		
			AC-3(3)[6](b)(1)	*przekazywania informacji nieupoważnionym podmiotom lub obiektom;*	
			AC-3(3)[6](b)(2)	*przyznawania swoich przywilejów innym podmiotom;*	
			AC-3(3)[6](b)(3)	*zmiany jednego lub kilku atrybutów bezpieczeństwa w:*	
				AC-3(3)[6](b)(3)[a]	*podmiotach;*
				AC-3(3)[6](b)(3)[b]	*obiektach;*
				AC-3(3)[6](b)(3)[c]	*systemie informacyjnym; lub*

AC-3(3)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *OBOWIĄZKOWA KONTROLA DOSTĘPU***				
				AC-3(3)[6](b)(3)[d]	*komponentach systemu;*
			AC-3(3)[6](b)(4)	*wyboru atrybutów bezpieczeństwa i wartości atrybutów, które mają być kojarzone z nowo utworzonymi lub zmodyfikowanymi obiektami; lub*	
			AC-3(3)[6](b)(5)	*zmiany zasad regulujących kontrolę dostępu; oraz*	
		AC-3(3)[6](c)	*podmiotom określonym przez organizację można wyraźnie przyznać uprawnienia określone przez organizację w taki sposób, że nie są one ograniczone przez niektóre lub wszystkie z powyższych ograniczeń.*		
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; zasady obowiązkowej kontroli dostępu; procedury dotyczące egzekwowania prawa dostępu; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista podmiotów i obiektów (tj. użytkowników i zasobów) wymagających realizacji polityki obowiązkowej kontroli dostępu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające obowiązkową kontrolę dostępu].				

AC-3(4)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *UZNANIOWA KONTROLA DOSTĘPU***	
	CEL OCENY: *Określić, czy:*	
	AC-3(4)[1]	*organizacja określa zasady polityki uznaniowej kontroli dostępu, które mają być stosowane wobec określonych podmiotów i obiektów;*

<table>
<tr><td colspan="5">AC-3(4) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | UZNANIOWA KONTROLA DOSTĘPU</td></tr>
<tr><td></td><td colspan="4">AC-3(4)[2] system informacyjny narzuca organizacyjnie zdefiniowaną politykę uznaniowej kontroli dostępu określonym podmiotom i obiektom, w których polityka określa, że podmiot uzyskał dostęp do informacji i może wykonać jedną lub więcej z poniższych czynności:</td></tr>
<tr><td></td><td></td><td>AC-3(4)[2](a)</td><td colspan="2">przekazywać informacje innym podmiotom lub obiektom;</td></tr>
<tr><td></td><td></td><td>AC-3(4)[2](b)</td><td colspan="2">przyznawać swoje przywileje innym podmiotom;</td></tr>
<tr><td></td><td></td><td rowspan="5">AC-3(4)[2](c)</td><td colspan="2">zmienić atrybuty bezpieczeństwa w:</td></tr>
<tr><td></td><td></td><td>AC-3(4)[2](c)[a]</td><td>podmiotach;</td></tr>
<tr><td></td><td></td><td>AC-3(4)[2](c)[b]</td><td>obiektach;</td></tr>
<tr><td></td><td></td><td>AC-3(4)[2](c)[c]</td><td>systemie informacyjnym; lub</td></tr>
<tr><td></td><td></td><td>AC-3(4)[2](c)[d]</td><td>komponentach systemu;</td></tr>
<tr><td></td><td></td><td>AC-3(4)[2](d)</td><td colspan="2">wybrać opcję atrybuty bezpieczeństwa, które mają być kojarzone z nowo utworzonymi lub zmienionymi obiektami; lub</td></tr>
<tr><td></td><td></td><td>AC-3(4)[2](e)</td><td colspan="2">zmienić zasady regulujące kontrolę dostępu.</td></tr>
<tr><td></td><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:

Sprawdź: [wybierz spośród: Zasady kontroli dostępu; zasady uznaniowej kontroli dostępu; procedury dotyczące egzekwowania prawa dostępu; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista podmiotów i obiektów (tj. użytkowników i zasobów) wymagających stosowania zasad uznaniowej kontroli dostępu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów].

Test: [wybierz spośród: Zautomatyzowane mechanizmy wdrażające zasady uznaniowej kontroli dostępu].</td></tr>
</table>

AC-3(5)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *INFORMACJE DOTYCZĄCE BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy:*	
	AC-3(5)[1]	*organizacja określa informacje istotne dla bezpieczeństwa, do których system informacyjny uniemożliwia dostęp z wyjątkiem sytuacji, gdy system znajduje się w stanie nieoperacyjnym; oraz*
	AC-3(5)[2]	*system informacyjny uniemożliwia dostęp do zdefiniowanych przez organizację informacji dotyczących bezpieczeństwa z wyjątkiem sytuacji, gdy system znajduje się w stanie nieoperacyjnym.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące egzekwowania prawa dostępu; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy uniemożliwiające dostęp do informacji dotyczących bezpieczeństwa w ramach systemu informacyjnego].	

AC-3(6)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *OCHRONA INFORMACJI UŻYTKOWNIKA I SYSTEMU***
[Włączone do MP-4 oraz SC-28].	

AC-3(7)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *KONTROLA DOSTĘPU DO ROLI (RBAC)***	
	CEL OCENY: *Określić, czy:*	
	AC-3(7)[1]	*organizacja definiuje role w zakresie kontroli dostępu do systemu informacyjnego;*

AC-3(7)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *KONTROLA DOSTĘPU DO ROLI (RBAC)***		
	AC-3(7)[2]	*organizacja definiuje użytkowników uprawnionych do pełnienia ról zdefiniowanych przez organizację;*	
	AC-3(7)[3]	*system informacyjny kontroluje dostęp w oparciu o zdefiniowane przez organizację role i użytkowników upoważnionych do pełnienia tych ról;*	
	AC-3(7)[4]	*system informacyjny wymusza stosowanie zasad kontroli dostępu opartych na rolach, przez:*	
		AC-3(7)[4][a]	*podmioty, oraz*
		AC-3(7)[4][b]	*obiekty.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityki kontroli dostępu do roli (RBAC); procedury dotyczące egzekwowania prawa dostępu; plan bezpieczeństwa, dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista ról, użytkowników i związanych z nimi uprawnieniami wymaganymi do kontroli dostępu do systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające zasady kontroli dostępu oparte na rolach].	

AC-3(8)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *ODWOŁANIE ZEZWOLEŃ NA DOSTĘP***	
	CEL OCENY: *Określić, czy:*	
	AC-3(8)[1]	*organizacja określa zasady dotyczące terminów cofnięcia uprawnień dostępu; oraz*
	AC-3(8)[2]	*system informacyjny egzekwuje odwołania zezwoleń na dostęp wynikające ze zmian w zakresie atrybutów bezpieczeństwa podmiotów i obiektów w oparciu o zdefiniowane organizacyjnie zasady określające czas cofnięcia uprawnień dostępu.*

AC-3(8)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *ODWOŁANIE ZEZWOLEŃ NA DOSTĘP***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące egzekwowania prawa dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zasady zarządzania odwoływaniem zezwoleń na dostęp, rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test:** [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania dostępu].

AC-3(9)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *KONTROLOWANE UDOSTĘPNIENIE INFORMACJI***		
	CEL OCENY: *Określić, czy:*		
	AC-3(9)[1]	*organizacja określa system informacyjny lub komponent systemu autoryzowany do odbioru informacji udostępnianych spoza ustalonej granicy systemu informacyjnego udostępniającego te informacje;*	
	AC-3(9)[2]	*organizacja określa środki bezpieczeństwa, które mają być zapewnione przez określony przez organizację system informacyjny lub komponent systemu, odbierający informacje udostępniane z systemu informacyjnego zlokalizowanego poza ustaloną granicą systemu informacyjnego organizacji;*	
	AC-3(9)[3]	*organizacja określa środki bezpieczeństwa, które mają być stosowane do sprawdzania zawartości informacji przeznaczonych do udostępnienia;*	
	AC-3(9)[4]	*system informacyjny nie udostępnia informacji poza ustaloną granicą systemu, chyba, że:*	
		AC-3(9)[4](a)	*określony przez organizację współpracującą system informacyjny lub element systemu zapewnia określone przez organizację środki bezpieczeństwa; oraz*

AC-3(9)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *KONTROLOWANE UDOSTĘPNIENIE INFORMACJI***		
		AC-3(9)[4](b)	*środki bezpieczeństwa określone przez organizację są wykorzystywane do weryfikowania informacji przeznaczonych do udostępnienia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące egzekwowania prawa dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz środków bezpieczeństwa zapewnianych przez system informacyjny lub jego części składowe; wykaz środków bezpieczeństwa weryfikujących informacje przeznaczone do udostępnienia; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test:** [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania dostępu].		

AC-3(10)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *NADZOROWANE OBEJŚCIE MECHANIZMÓW KONTROLI DOSTĘPU***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-3(10)[1]	*określa warunki stosowania nadzorowanych obejść mechanizmów zautomatyzowanej kontroli dostępu; oraz*
	AC-3(10)[2]	*stosuje nadzorowane obejścia mechanizmów zautomatyzowanej kontroli dostępu w warunkach określonych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące egzekwowania prawa dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; warunki stosowania nadzorowanych obejść mechanizmów zautomatyzowanej kontroli dostępu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AC-3(10)	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | *NADZOROWANE OBEJŚCIE MECHANIZMÓW KONTROLI DOSTĘPU***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test:** [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania dostępu].

AC-4	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI**	
	CEL OCENY: *Określić, czy:*	
	AC-4[1]	*organizacja określa zasady kontroli przepływu informacji w celu nadzorowania przepływem informacji w ramach systemu oraz pomiędzy połączonymi systemami; oraz*
	AC-4[2]	*system informacyjny egzekwuje zatwierdzone upoważnienia do kontrolowania przepływu informacji w ramach systemu oraz pomiędzy połączonymi systemami, w oparciu o zasady kontroli przepływu informacji określone przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; podstawowa konfiguracja bazowa systemu informacyjnego; lista zezwoleń na przepływ informacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].	

AC-4(1)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *ATRYBUTY BEZPIECZEŃSTWA PODMIOTU LUB OBIEKTU***		
	CEL OCENY: *Określić, czy:*		
	AC-4(1)[1]	*organizacja definiuje politykę kontroli przepływu informacji, jako podstawę do podejmowania decyzji dotyczących kontroli przepływu;*	
	AC-4(1)[2]	*organizacja określa, że atrybuty bezpieczeństwa powinny być kojarzone z informacjami, źródłami i obiektami docelowymi;*	
	AC-4(1)[3]	*organizacja definiuje następujące obiekty, które mają być kojarzone z atrybutami bezpieczeństwa zdefiniowanymi przez organizację:*	
		AC-4(1)[3][a]	*informacja;*
		AC-4(1)[3][b]	*źródło;*
		AC-4(1)[3][c]	*miejsce przeznaczenia; oraz*
	AC-4(1)[4]	*system informacyjny wykorzystuje zdefiniowane przez organizację atrybuty bezpieczeństwa związane z informacjami zdefiniowanymi przez organizację, źródłami i obiektami docelowymi, w celu egzekwowania zdefiniowanych przez organizację zasad kontroli przepływu informacji, jako podstawy do podejmowania decyzji dotyczących kontroli przepływu.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista atrybutów bezpieczeństwa i związanych z nimi informacji, źródeł i obiektów docelowych wymuszających stosowanie zasad kontroli przepływu informacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].		

AC-4(2)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *PRZETWARZANIE DOMEN***	
	CEL OCENY: *Określić, czy:*	
	AC-4(2)[1]	*organizacja definiuje politykę kontroli przepływu informacji, jako podstawę do podejmowania decyzji dotyczących kontroli przepływu; oraz*
	AC-4(2)[2]	*system informacyjny wykorzystuje chronione przetwarzanie domen do egzekwowania zdefiniowanej organizacyjnie polityki kontroli przepływu informacji, jako podstawy do podejmowania decyzji w zakresie kontroli przepływu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; lista atrybutów bezpieczeństwa i związanych z nimi informacji, źródeł i obiektów docelowych egzekwujących zasady kontroli przepływu informacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].	

AC-4(3)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *DYNAMICZNA KONTROLA PRZEPŁYWU INFORMACJI***	
	CEL OCENY: *Określić, czy:*	
	AC-4(3)[1]	*organizacja określa politykę egzekwowania dynamicznej kontroli przepływu informacji; oraz*
	AC-4(3)[2]	*system informacyjny wdraża dynamiczną kontrola przepływu informacji w oparciu o zasady określone przez organizację.*

AC-4(3)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *DYNAMICZNA KONTROLA PRZEPŁYWU INFORMACJI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; lista atrybutów bezpieczeństwa i związanych z nimi informacji, źródeł i obiektów docelowych egzekwujących zasady kontroli przepływu informacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].

AC-4(4)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *SPRAWDZANIE ZAWARTOŚCI ZASZYFROWANEJ INFORMACJI***		
	CEL OCENY: *Określić, czy:*		
	AC-4(4)[1]	*organizacja określa procedurę lub metodę, którą należy zastosować, aby uniemożliwić zaszyfrowanym informacjom obejście mechanizmów kontroli zawartości;*	
	AC-4(4)[2]	*system informacyjny uniemożliwia zaszyfrowanym informacjom obejście mechanizmów kontroli zawartości, poprzez wykonywanie jednej lub więcej z następujących czynności:*	
		AC-4(4)[2][a]	*odszyfrowanie informacji;*
		AC-4(4)[2][b]	*blokowanie przepływu zaszyfrowanych informacji;*
		AC-4(4)[2][c]	*rozłączanie sesji komunikacyjnych usiłujących przekazać zaszyfrowane informacje; oraz/lub*
		AC-4(4)[2][d]	*zastosowanie określonej przez organizację procedury lub metody.*

AC-4(4)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *SPRAWDZANIE ZAWARTOŚCI ZASZYFROWANEJ INFORMACJI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].

AC-4(5)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *WBUDOWANE RODZAJE DANYCH***	
	CEL OCENY: *Określić, czy:*	
	AC-4(5)[1]	*organizacja określa ograniczenia, które mają być egzekwowane przy osadzanie określonych typów danych w miejsce innych typów danych; oraz*
	AC-4(5)[2]	*system informacyjny wymusza określone przez organizację ograniczenia dotyczące osadzania typów danych w miejsce innych typów danych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz ograniczeń, jakie należy wprowadzić w zakresie osadzania typów danych w miejsce innych typów danych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].	

AC-4(6)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *METADANE***	
	CEL OCENY: *Określić, czy:*	
	AC-4(6)[1]	*organizacja definiuje metadane, jako środek egzekwowania kontroli przepływu informacji; oraz*
	AC-4(6)[2]	*system informacyjny wymusza kontrolę przepływu informacji w oparciu o zdefiniowane przez organizację metadane.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rodzaje metadanych stosowane do wykonywania decyzji dotyczących kontroli przepływu informacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].	

AC-4(7)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *MECHANIZMY PRZEPŁYWU JEDNOKIERUNKOWEGO***	
	CEL OCENY: *Określić, czy:*	
	AC-4(7)[1]	*organizacja definiuje jednokierunkowy przepływ informacji, który ma być egzekwowany przez system informacyjny; oraz*
	AC-4(7)[2]	*system informacyjny narzuca organizacyjnie zdefiniowany jednokierunkowy przepływ informacji przy użyciu mechanizmów sprzętowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; mechanizmy sprzętowe	

AC-4(7)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *MECHANIZMY PRZEPŁYWU JEDNOKIERUNKOWEGO***
	systemów informacyjnych i związane z nimi konfiguracje; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Mechanizmy sprzętowe wdrażające politykę egzekwowania przepływu informacji].

AC-4(8)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *FILTRY POLITYKI BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy:*	
	AC-4(8)[1]	*organizacja definiuje filtry polityki bezpieczeństwa, jako podstawę do egzekwowania decyzji dotyczących kontroli przepływu;*
	AC-4(8)[2]	*organizacja określa przepływy informacji, dla których decyzje dotyczące kontroli przepływu mają być stosowane i egzekwowane; oraz*
	AC-4(8)[3]	*system informacyjny wymusza kontrolę przepływu informacji za pomocą filtrów polityki bezpieczeństwa zdefiniowanych przez organizację, jako podstawę do podejmowania decyzji dotyczących kontroli przepływu informacji zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz filtrów polityki bezpieczeństwa regulujących decyzje dotyczące kontroli przepływu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [**wybierz spośród:**: Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].	

AC-4(9)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *OCENA PRZEZ UPRAWNIONĄ OSOBĘ***	
	CEL OCENY: *Określić, czy:*	
	AC-4(9)[1]	*organizacja definiuje przepływy informacji wymagające oceny przez upoważnione osoby;*
	AC-4(9)[2]	*organizacja określa warunki, na jakich należy egzekwować stosowanie oceny przez osoby uprawnione w odniesieniu do przepływów informacji zdefiniowanych przez organizację; oraz*
	AC-4(9)[3]	*system informacyjny wymusza stosowanie przez uprawnioną osobę ocen przepływu informacji organizacyjnych w warunkach zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; ewidencja oceny przez uprawnioną osobę w zakresie przepływów informacji; wykaz warunków wymagających oceny przez uprawnioną osobę w zakresie przepływów informacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za egzekwowanie przepływu informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wymuszające oceny przez uprawnioną osobę].	

AC-4(10)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *WŁĄCZANIE/ WYŁĄCZANIE FILTRÓW POLITYKI BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy:*	
	AC-4(10)[1]	*organizacja definiuje filtry polityk bezpieczeństwa, które mogą być włączania/wyłączane przez uprzywilejowanych administratorów;*

AC-4(10)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *WŁĄCZANIE/ WYŁĄCZANIE FILTRÓW POLITYKI BEZPIECZEŃSTWA***	
	AC-4(10)[2]	*zdefiniowane przez organizację warunki, w których uprzywilejowani administratorzy mają możliwość włączania/wyłączania zdefiniowanych przez organizację filtrów polityki bezpieczeństwa; oraz*
	AC-4(10)[3]	*system informacyjny zapewnia uprawnionym administratorom możliwość włączania/wyłączania zdefiniowanych przez organizację filtrów polityki bezpieczeństwa na warunkach zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; zasady przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista filtrów reguł bezpieczeństwa włączonych/wyłączanych przez uprzywilejowanych administratorów; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za włączanie/wyłączenie filtrów polityki bezpieczeństwa; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].	

AC-4(11)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *KONFIGURACJA FILTRÓW POLITYKI BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy:*	
	AC-4(11)[1]	*organizacja definiuje filtry polityk bezpieczeństwa, które uprzywilejowani administratorzy mają możliwość skonfigurowania do obsługi różnych polityk bezpieczeństwa; oraz*
	AC-4(11)[2]	*system informacyjny zapewnia uprawnionym administratorom możliwość konfigurowania zdefiniowanych przez organizację filtrów polityki bezpieczeństwa w celu obsługi różnych polityk bezpieczeństwa.*

AC-4(11)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *KONFIGURACJA FILTRÓW POLITYKI BEZPIECZEŃSTWA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz filtrów polityki bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konfigurację filtrów polityki bezpieczeństwa; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].

AC-4(12)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *IDENTYFIKATORY TYPU DANYCH***	
	CEL OCENY: *Określić, czy:*	
	AC-4(12)[1]	*organizacja definiuje identyfikatory typu danych, które mają być używane przy przekazywaniu informacji pomiędzy różnym oraz domenami bezpieczeństwa w celu weryfikacji danych istotnych dla decyzji dotyczących przepływu informacji; oraz*
	AC-4(12)[2]	*system informacyjny, podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa, używa zdefiniowanych przez organizację identyfikatorów typu danych w celu weryfikacji danych istotnych dla decyzji dotyczących przepływu informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz identyfikatorów typów danych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AC-4(12)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *IDENTYFIKATORY TYPU DANYCH***
	Wywiad: [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania zasad egzekwowania przepływu informacji].

AC-4(13)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *DEKOMPOZYCJA INFORMACJI NA ODPOWIEDNIE PODSKŁADNIKI***	
	CEL OCENY: *Określić, czy:*	
	AC-4(13)[1]	*organizacja definiuje istotne dla polityki części składowe w celu zdekomponowania informacji i poddania ich mechanizmom egzekwowania polityki przy przekazywaniu takich informacji pomiędzy różnymi domenami bezpieczeństwa; oraz*
	AC-4(13)[2]	*system informacyjny, przy przekazywaniu informacji pomiędzy różnymi domenami bezpieczeństwa, rozkłada informacje na określone przez organizację części składowe, istotne z punktu widzenia polityki, w celu poddania ich mechanizmom egzekwowania polityki.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].	

AC-4(14)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *POLITYKA STOSOWANIA FILTRÓW BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy:*	
	AC-4(14)[1]	*organizacja definiuje istotne dla polityki części składowe w celu zdekomponowania informacji w celu poddania ich mechanizmom egzekwowania polityki przy przekazywaniu takich informacji pomiędzy różnymi domenami bezpieczeństwa; oraz*
	AC-4(14)[2]	*system informacyjny, podczas przekazywania informacji pomiędzy różnymi domenami bezpieczeństwa, rozkłada informacje na określone przez organizację części składowe, istotne z punktu widzenia polityki, w celu poddania ich mechanizmom egzekwowania polityki.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz filtrów polityki bezpieczeństwa; lista filtrów polityki zawartości danych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].	

AC-4(15)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *WYKRYWANIE INFORMACJI NIEAKCEPTOWANYCH***	
	CEL OCENY: *Określić, czy:*	
	AC-4(15)[1]	*organizacja definiuje nieakceptowane informacje, które mają być identyfikowane podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa;*
	AC-4(15)[2]	*organizacja określa politykę bezpieczeństwa, która wymaga, aby w przypadku wykrycia obecności informacji nieakceptowanych, zabroniony był transfer zdefiniowanych przez organizację informacji nieakceptowanych pomiędzy różnymi domenami bezpieczeństwa; oraz*

AC-4(15)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *WYKRYWANIE INFORMACJI NIEAKCEPTOWANYCH***	
	AC-4(15)[3]	*System informacyjny, przekazując informacje pomiędzy różnymi domenami bezpieczeństwa, bada informacje pod kątem obecności informacji zdefiniowanych przez organizację, jako nieakceptowane i zakazuje przekazywania takich informacji zgodnie ze zdefiniowaną przez organizację polityką bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz rodzajów informacji nieobjętych zakazem oraz informacji powiązanych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].	

AC-4(16)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | PRZEKAZYWANIE INFORMACJI POMIĘDZY SYSTEMAMI INFORMACYJNYMI**
[Włączone do: AC-4].	

AC-4(17)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *UWIERZYTELNIANIE DOMEN***		
	CEL OCENY: *Ustalenie, czy system informacyjny w sposób jednoznaczny identyfikuje i uwierzytelnia:*		
	AC-4(17)[1]	**AC-4(17)[1][a]**	*punkty źródłowe przekazywania informacji;*
		AC-4(17)[1][b]	*punkty docelowe przekazywania informacji;*
	AC-4(17)[2]	*przez jedną lub więcej z poniższych:*	
		AC-4(17)[2][a]	*organizację;*
		AC-4(17)[2][b]	*system;*

AC-4(17)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *UWIERZYTELNIANIE DOMEN***		
		AC-4(17)[2][c]	*aplikację; oraz/lub*
		AC-4(17)[2][d]	*osobę.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; procedury dotyczące identyfikacji i uwierzytelniania domeny źródłowej i docelowej; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki egzekwowania przepływu informacji].		

AC-4(18)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *POWIĄZANIE ATRYBUTÓW BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy:*	
	AC-4(18)[1]	*organizacja określa wiążące techniki, które mają być stosowane w celu ułatwienia egzekwowania polityki przepływu informacji; oraz*
	AC-4(18)[2]	*system informacyjny wiąże atrybuty bezpieczeństwa z informacjami przy użyciu zdefiniowanych przez organizację technik wiązania w celu ułatwienia egzekwowania polityki przepływu informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka egzekwowania przepływu informacji; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz technik wiązania atrybutów bezpieczeństwa z informacjami; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AC-4(18)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *POWIĄZANIE ATRYBUTÓW BEZPIECZEŃSTWA***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie przepływu informacji; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania przepływu informacji].

AC-4(19)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *UWIERZYTELNIANIE METADANYCH***
	CEL OCENY: *Ustalić, czy system informacyjny, przy przesyłaniu informacji pomiędzy różnymi domenami bezpieczeństwa, stosuje taką samą politykę bezpieczeństwa filtrowania do metadanych, jaką stosuje się do przesyłania danych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka egzekwowania przepływu informacji; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz kryteriów filtrowania polityki bezpieczeństwa stosowanych w odniesieniu do metadanych oraz przesyłania danych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie przepływu informacji; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania przepływu informacji].

AC-4(20)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *ZATWIERDZONE ROZWIĄZANIA BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-4(20)[1]	*definiuje rozwiązania w zatwierdzonych konfiguracjach do sterowania przepływem informacji wewnątrz domen bezpieczeństwa;*

AC-4(20)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *ZATWIERDZONE ROZWIĄZANIA BEZPIECZEŃSTWA***	
	AC-4(20)[2]	*określa informacje, dla których zdefiniowane przez organizację rozwiązania w zatwierdzonych konfiguracjach, mają być stosowane do kontroli przepływu tych informacji wewnątrz domen bezpieczeństwa; oraz*
	AC-4(20)[3]	*wykorzystuje zdefiniowane organizacyjnie rozwiązania w zatwierdzonych konfiguracjach do sterowania przepływem zdefiniowanych organizacyjnie informacji wewnątrz domen bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka egzekwowania przepływu informacji; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista rozwiązań w zatwierdzonych konfiguracjach; zatwierdzone podstawowe konfiguracje bazowe; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie przepływu informacji; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania przepływu informacji].	

AC-4(21)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *FIZYCZNA LUB LOGICZNA SEPARACJA PRZEPŁYWÓW INFORMACJI***	
	CEL OCENY: *Określić, czy:*	
	AC-4(21)[1]	*organizacja definiuje wymaganą separację przepływów informacji według rodzajów informacji;*
	AC-4(21)[2]	*organizacja określa mechanizmy i/lub techniki, które mają być stosowane do logicznej lub fizycznej separacji przepływów informacji; oraz*

AC-4(21)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *FIZYCZNA LUB LOGICZNA SEPARACJA PRZEPŁYWÓW INFORMACJI***	
	AC-4(21)[3]	*system informacyjny dokonuje logicznej lub fizycznej separacji przepływów informacji przy użyciu zdefiniowanych przez organizację mechanizmów i/lub technik w celu osiągnięcia zdefiniowanego przez organizację wymaganego odseparowania poszczególnych rodzajów informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka egzekwowania przepływu informacji; polityka kontroli przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz wymaganej separacji przepływu informacji według typów informacji; wykaz mechanizmów i/lub technik stosowanych do logicznej lub fizycznej separacji przepływu informacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie przepływu informacji; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania przepływu informacji].	

AC-4(22)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *TYLKO DOSTĘP***
	CEL OCENY: *Ustalenie, czy system informacyjny zapewnia dostęp z pojedynczego urządzenia do platform komputerowych, aplikacji lub danych znajdujących się w wielu różnych domenach bezpieczeństwa, zapobiegając jednocześnie przepływowi informacji między różnymi domenami bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka egzekwowania przepływu informacji; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

AC-4(22)	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | *TYLKO DOSTĘP***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie przepływu informacji; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania przepływu informacji].

AC-5	**ROZDZIAŁ OBOWIĄZKÓW**	
	CEL OCENY: *Określić, czy organizacja:*	
AC-5(a)	**AC-5(a)[1]**	*określa obowiązki organizacyjne poszczególnych osób*
	AC-5(a)[2]	*rozdziela obowiązki organizacyjne poszczególnych osób;*
AC-5(b)	*dokumentuje rozdział zadań osób; oraz*	
AC-5(c)	*określa uprawnienia dostępu do systemu informacyjnego.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące podziałów odpowiedzialności i rozdziału obowiązków; ustawienia konfiguracji systemu informacyjnego i związana z nimi dokumentacja; wykaz podziałów odpowiedzialności i rozdziału obowiązków; uprawnienia dostępu do systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określanie odpowiednich podziałów odpowiedzialności i rozdzielanie obowiązków; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki rozdziału obowiązków].	

AC-6	**ZASADA WIEDZY KONIECZNEJ**
	CEL OCENY: *Ustalić, czy organizacja stosuje zasadę wiedzy koniecznej, umożliwiając dostęp tylko autoryzowanym użytkownikom oraz procesom działającym w imieniu użytkowników, które są niezbędne do realizacji przydzielonych zadań zgodnie z misją organizacji i funkcjami biznesowymi.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zasada wiedzy koniecznej; lista przydzielonych uprawnień dostępu (uprawnień użytkownika); ustawienia konfiguracji systemu informacyjnego i związana z nimi dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określenie najmniejszych uprawnień niezbędnych do realizacji określonych zadań; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zapewniające funkcje najniższych uprawnień].

AC-6(1)	**ZASADA WIEDZY KONIECZNEJ | *UPOWAŻNIONY DOSTĘP DO FUNKCJI BEZPIECZEŃSTWA***		
	CEL OCENY: *Określić, czy organizacja:*		
	AC-6(1)[1]	*definiuje informacje istotne dla bezpieczeństwa, do których dostęp musi być jednoznacznie autoryzowany;*	
	AC-6(1)[2]	*definiuje funkcje bezpieczeństwa wdrożone w:*	
		AC-6(1)[2][a]	*sprzęcie;*
		AC-6(1)[2][b]	*oprogramowaniu;*
		AC-6(1)[2][c]	*oprogramowaniu układowym;*
	AC-6(1)[3]	*jednoznacznie zezwala na dostęp do:*	
		AC-6(1)[3][a]	*funkcji bezpieczeństwa zdefiniowanych przez organizację; oraz*

AC-6(1)	**ZASADA WIEDZY KONIECZNEJ | *UPOWAŻNIONY DOSTĘP DO FUNKCJI BEZPIECZEŃSTWA***		
		AC-6(1)[3][b]	*informacji dotyczących bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** *[wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zasada wiedzy koniecznej; wykaz funkcji bezpieczeństwa (wdrożonych w sprzęcie, oprogramowaniu i oprogramowaniu układowym) oraz informacji istotnych z punktu widzenia bezpieczeństwa, do których dostęp musi być wyraźnie dozwolony; ustawienia konfiguracji systemu informacyjnego i związana z nimi dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określenie najmniejszych uprawnień niezbędnych do realizacji określonych zadań; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zapewniające funkcje najniższych uprawnień].		

AC-6(2)	**ZASADA WIEDZY KONIECZNEJ | *NIEUPRZYWILEJOWANY DOSTĘP DO FUNKCJI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-6(2)[1]	*definiuje funkcje bezpieczeństwa lub informacje istotne dla bezpieczeństwa, do których mają dostęp użytkownicy kont lub ról w systemie informacyjnym; oraz*
	AC-6(2)[2]	*wymaga, aby użytkownicy kont lub ról w systemie informacyjnym, mający dostęp do zdefiniowanych przez organizację funkcji bezpieczeństwa lub informacji istotnych z punktu widzenia bezpieczeństwa, korzystali z kont nieuprzywilejowanych lub ról przy dostępie do funkcji niezwiązanych z bezpieczeństwem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zasada wiedzy koniecznej; wykaz funkcji bezpieczeństwa generowanych przez system lub informacji istotnych dla bezpieczeństwa przypisanych do kont lub ról systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z nimi dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AC-6(2)	**ZASADA WIEDZY KONIECZNEJ | *NIEUPRZYWILEJOWANY DOSTĘP DO FUNKCJI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za określenie najmniejszych uprawnień niezbędnych do realizacji określonych zadań; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zapewniające funkcje najniższych uprawnień].

AC-6(3)	**ZASADA WIEDZY KONIECZNEJ | *DOSTĘP SIECIOWY DO UPRZYWILEJOWANYCH POLECEŃ***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-6(3)[1]	*definiuje dostęp sieciowy do uprzywilejowanych poleceń, autoryzowany tylko w przypadku istotnych potrzeb operacyjnych;*
	AC-6(3)[2]	*definiuje istotne potrzeby operacyjne, dla których dostęp sieciowy do zdefiniowanych przez organizację poleceń uprzywilejowanych ma być wyłącznie autoryzowany;*
	AC-6(3)[3]	*zezwala na dostęp sieciowy do zdefiniowanych przez organizację poleceń uprzywilejowanych tylko dla określonych przez organizację istotnych potrzeb operacyjnych; oraz*
	AC-6(3)[4]	*dokumentuje w planie bezpieczeństwa systemu informacyjnego uzasadnienie autoryzowanego dostępu do sieci i do zdefiniowanych przez organizację uprzywilejowanych poleceń.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zasada wiedzy koniecznej; plan bezpieczeństwa; procedury dotyczące najmniejszych uprawnień; plan bezpieczeństwa; ustawienia konfiguracji systemu informacyjnego i związana z nimi dokumentacja; zapisy z audytu systemu informacyjnego; wykaz potrzeb operacyjnych w zakresie autoryzacji dostępu do sieci dla uprzywilejowanych poleceń; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określenie zasad wiedzy koniecznej niezbędnej do realizacji określonych zadań; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zapewniające funkcje najniższych uprawnień].	

AC-6(4)	**ZASADA WIEDZY KONIECZNEJ | *ODDZIELNE DOMENY PRZETWARZANIA***
	CEL OCENY: *Ustalić, czy system informacyjny zapewnia oddzielne domeny przetwarzania w celu umożliwienia szczegółowego przydzielania uprawnień użytkownikom.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zasada wiedzy koniecznej; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określenie zasad wiedzy koniecznej niezbędnej do realizacji określonych zadań; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zapewniające funkcje najniższych uprawnień].

AC-6(5)	**ZASADA WIEDZY KONIECZNEJ | *UPRZYWILEJOWANE KONTA***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-6(5)[1]	*określa personel lub role, którym uprzywilejowane konta w systemie informacyjnym mają być ograniczone; oraz*
	AC-6(5)[2]	*ogranicza uprzywilejowane konta w systemie informacyjnym do personelu lub ról zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zasada wiedzy koniecznej; lista wygenerowanych przez systemu kont uprzywilejowanych; lista personelu zarządzającego systemem; ustawienia konfiguracyjne systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AC-6(5)	**ZASADA WIEDZY KONIECZNEJ | *UPRZYWILEJOWANE KONTA***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za określenie najmniejszych uprawnień niezbędnych do realizacji określonych zadań; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zapewniające funkcje najniższych uprawnień].

AC-6(6)	**ZASADA WIEDZY KONIECZNEJ | *OGRANICZONY DOSTĘP PRZEZ UŻYTKOWNIKÓW SPOZA ORGANIZACJI***
	CEL OCENY: *Ustalenie, czy organizacja zabrania uprzywilejowanego dostępu do systemu informacyjnego użytkownikom niebędących pracownikami (współpracownikami) organizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zasada wiedzy koniecznej; lista generowanych przez system kont uprzywilejowanych; lista użytkowników spoza organizacji; ustawienia konfiguracyjne systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określenie najmniejszych uprawnień niezbędnych do realizacji określonych zadań; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zabraniające uprzywilejowanego dostępu do systemu informacyjnego].

AC-6(7)	**ZASADA WIEDZY KONIECZNEJ | *PRZEGLĄD UPRAWNIEŃ UŻYTKOWNIKA***		
	CEL OCENY: *Określić, czy organizacja:*		
	AC-6(7)(a)	**AC-6(7)(a)[1]**	*definiuje role lub klasy użytkowników, do których przypisane są uprawnienia;*

AC-6(7)	**ZASADA WIEDZY KONIECZNEJ | *PRZEGLĄD UPRAWNIEŃ UŻYTKOWNIKA***		
		AC-6(7)(a)[2]	*definiuje częstotliwość przeglądania uprawnień przypisanych do ról lub klas użytkowników zdefiniowanych przez organizację, w celu potwierdzenia potrzeby takich uprawnień;*
		AC-6(7)(a)[3]	*dokonuje przeglądu uprawnień przypisanych do ról lub klas użytkowników z częstotliwością określoną przez organizację, w celu potwierdzenia potrzeby takich uprawnień; oraz*
	AC-6(7)(b)	*w razie potrzeby, przydziela lub odbiera przywileje w celu właściwego odzwierciedlenia misji organizacji/ potrzeb biznesowych.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zasada wiedzy koniecznej; lista wygenerowanych przez system ról lub klas użytkowników i przydzielonych im uprawnień; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; przeglądów oceny uprawnień przypisanych do ról, klas lub użytkowników; rejestru usunięcia lub zmiany przypisania uprawnień dla ról lub klas użytkowników; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację najniższych uprawnień niezbędnych do realizacji określonych zadań; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania przeglądu uprawnień użytkownika].		

AC-6(8)	**ZASADA WIEDZY KONIECZNEJ | *POZIOMY UPRAWNIEŃ DO URUCHAMIANIA KODU***	
	CEL OCENY: *Określić, czy:*	
	AC-6(8)[1]	*organizacja definiuje oprogramowanie, które nie powinno być wykonywane na wyższych poziomach uprawnień, niż programiści tworzący oprogramowanie (tworzący kod); oraz*

AC-6(8)	**ZASADA WIEDZY KONIECZNEJ | *POZIOMY UPRAWNIEŃ DO URUCHAMIANIA KODU***	
	AC-6(8)[2]	*system informacyjny uniemożliwia wykonywanie oprogramowania zdefiniowanego przez organizację na wyższym poziomie uprawnień niż programiści tworzący oprogramowanie (tworzący kod).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zasada wiedzy koniecznej; lista programów, które nie powinny być wykonywane na wyższym poziomie uprawnień niż programiści tworzący oprogramowanie (tworzący kod); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określenie najmniejszych uprawnień niezbędnych do realizacji określonych zadań; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test: [wybierz spośród:**: Zautomatyzowane mechanizmy zapewniające funkcje wdrożenie najniższych uprawnień do realizacji aplikacji].	

AC-6(9)	**ZASADA WIEDZY KONIECZNEJ | *KONTROLA WYKORZYSTANIA UPRZYWILEJOWANYCH FUNKCJI***
	CEL OCENY: *Ustalenie, czy system informacyjny dokonuje kontroli wykonywania funkcji uprzywilejowanych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zasada wiedzy koniecznej; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz funkcji uprzywilejowanych podlegających kontroli; wykaz zdarzeń podlegających kontroli; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację najniższych uprawnień niezbędnych do realizacji określonych zadań; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy kontrolujące realizację funkcji zasady wiedzy koniecznej].

AC-6(10)	**ZASADA WIEDZY KONIECZNEJ | *ODMOWA WYKONYWANIA PRZEZ NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW UPRZYWILEJOWANYCH FUNKCJI***	
	CEL OCENY: *Ustalenie, czy system informacyjny uniemożliwia nieuprzywilejowanym użytkownikom wykonywanie uprzywilejowanych funkcji, takich jak:*	
	AC-6(10)[1]	*dezaktywacja wdrożonych środków bezpieczeństwa/środków zaradczych;*
	AC-6(10)[2]	*omijanie środków bezpieczeństwa/środków zaradczych; lub*
	AC-6(10)[3]	*zmiana wdrożonych środków bezpieczeństwa/środków zaradczych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zasada wiedzy koniecznej; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista funkcji uprzywilejowanych i przypisanych powiązań do konta użytkownika; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określenie zasad wiedzy koniecznej niezbędnej do realizacji określonych zadań; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: **[wybierz spośród:**: Zautomatyzowane mechanizmy zapewniające nieuprzywilejowanym użytkownikom funkcje najniższych uprawnień].	

AC-7	**NIEUDANE PRÓBY LOGOWANIA**		
	CEL OCENY: *Określić, czy:*		
	AC-7(a)	**AC-7(a)[1]**	*organizacja określa liczbę następujących po sobie nieważnych prób logowania do systemu informacyjnego przez użytkownika w określonym przez organizację okresie czasu;*
		AC-7(a)[2]	*organizacja definiuje okres czasu, pozwalający użytkownikom systemu informacyjnego na zdefiniowaną przez organizację liczbę następujących po sobie nieważnych prób logowania;*

<table>
<tr><th colspan="5">AC-7 NIEUDANE PRÓBY LOGOWANIA</th></tr>
<tr><td rowspan="6"></td><td></td><td>AC-7(a)[3]</td><td colspan="2">system informacyjny wymusza ograniczenie określonej przez organizację liczby następujących po sobie nieważnych prób logowania przez użytkownika w określonym przez organizację okresie czasu;</td></tr>
<tr><td rowspan="4">AC-7(b)</td><td>AC-7(b)[1]</td><td colspan="2">organizacja definiuje okres czasu blokady konta/węzła sieciowego lub algorytm opóźnienia logowania, który ma być automatycznie wymuszony przez system informacyjny w przypadku przekroczenia maksymalnej liczby nieudanych prób logowania;</td></tr>
<tr><td rowspan="3">AC-7(b)[2]</td><td colspan="2">system informacyjny, po przekroczeniu maksymalnej liczby nieudanych prób logowania, automatycznie:</td></tr>
<tr><td>AC-7(b)[2][a]</td><td>blokuje konto/węzeł sieciowy przez określony przez organizację okres czasu;</td></tr>
<tr><td>AC-7(b)[2][b]</td><td>blokuje konto/węzeł sieciowy do momentu odblokowania go przez administratora; lub</td></tr>
<tr><td>AC-7(b)[2][c]</td><td>opóźnia kolejne logowanie według zdefiniowanego przez organizację algorytmu opóźnienia.</td></tr>
<tr><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Zasady kontroli dostępu; procedury dotyczące nieudanych prób logowania; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów; administratorzy systemu/sieci].
Test: [wybierz spośród: Zautomatyzowane mechanizmy wdrażania zasad kontroli dostępu rejestrujących nieudane próby logowania].</td></tr>
</table>

AC-7(1)	NIEUDANE PRÓBY LOGOWANIA | *ZAUTOMATYZOWANE ZAMKNIĘCIE KONTA*
[Włączone do: AC-7].	

AC-7(2)	**NIEUDANE PRÓBY LOGOWANIA | *USUWANIE INFORMACJI Z URZĄDZEŃ PRZENOŚNYCH***	
	CEL OCENY: *Określić, czy:*	
	AC-7(2)[1]	*organizacja definiuje urządzenia przenośne, które mają być czyszczone/usuwane po zdefiniowanej przez organizację liczbie kolejnych, nieudanych prób logowania urządzeń;*
	AC-7(2)[2]	*organizacja definiuje wymagania/techniki oczyszczania/wyłączania, które mają być stosowane, gdy zdefiniowane przez organizację urządzenia przenośne są oczyszczane/wyłączane po określonej liczbie następujących po sobie, nieudanych prób logowania urządzeń;*
	AC-7(2)[3]	*organizacja określa liczbę następujących po sobie, nieudanych prób logowania, które umożliwiłyby dostęp do urządzeń przenośnych, zanim system informacyjny oczyści/wyłączy informacje z tych urządzeń; oraz*
	AC-7(2)[4]	*system informacyjny oczyszcza/usuwa informacje z urządzeń przenośnych zdefiniowanych przez organizację w oparciu o zdefiniowane przez organizację wymagania/techniki oczyszczania/usuwania, po zdefiniowanej przez organizację liczbie kolejnych, nieudanych prób logowania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące nieudanych prób logowania na urządzeniach przenośnych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz urządzeń przenośnych, które mają zostać oczyszczone/wyłączone po zdefiniowanych przez organizację kolejnych, nieudanych próbach logowania urządzeń; wykaz wymogów lub technik oczyszczania/wyłączania urządzeń przenośnych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania polityki kontroli dostępu w przypadku nieudanych prób logowania].	

AC-8	**POWIADAMIANIE O ZASADACH UŻYCIA SYSTEMU**			
	CEL OCENY: *Określić, czy:*			
	AC-8(a)	**AC-8(a)[1]**	*organizacja definiuje komunikat lub baner informujący o użyciu systemu, który ma być wyświetlany przez system informacyjny użytkownikom przed przyznaniem dostępu do system;*	
		AC-8(a)[2]	*system informacyjny, przed udzieleniem dostępu do systemu informacyjnego, wyświetla użytkownikom zdefiniowany przez organizację komunikat z powiadomieniem lub baner, który zgodne z obowiązującymi przepisami, rozporządzeniami wykonawczymi, dyrektywami, zasadami, przepisami, normami i wytycznymi zawiera informacje o prywatności i bezpieczeństwie oraz stwierdza, że:*	
			AC-8(a)[2](1)	*użytkownicy mają dostęp do systemu informacyjnego organizacji;*
			AC-8(a)[2](2)	*korzystanie z systemu informacyjnego może być monitorowane, rejestrowane i poddawane kontroli;*
			AC-8(a)[2](3)	*nieautoryzowane korzystanie z systemu informacyjnego jest zabronione i podlega sankcjom karnym i cywilnym;*
			AC-8(a)[2](4)	*korzystanie z systemu informacyjnego oznacza zgodę na monitorowanie i rejestrowanie;*
	AC-8(b)	*system informacyjny utrzymuje komunikat powiadomienia lub baner na ekranie do czasu potwierdzenia przez użytkowników warunków użytkowania i podjęcia przez nich wyraźnych działań w celu zalogowania się lub uzyskania dalszego dostępu do systemu informacyjnego;*		
	AC-8(c)	*w odniesieniu do systemów publicznie dostępnych:*		
		AC-8(c)(1)	**AC-8(c)(1)[1]**	*organizacja określa warunki korzystania z systemu, które mają być wyświetlane przez system informacyjny przed udzieleniem dalszego dostępu;*

<table>
<tr><th colspan="5">AC-8 POWIADAMIANIE O ZASADACH UŻYCIA SYSTEMU</th></tr>
<tr><td rowspan="4"></td><td rowspan="3"></td><td></td><td>AC-8(c)(1)[2]</td><td>system informacyjny, przed udzieleniem dalszego dostępu, wyświetla warunki zdefiniowane przez organizację;</td></tr>
<tr><td>AC-8(c)(2)</td><td colspan="2">system informacyjny zawiera odniesienia, jeśli takie istnieją, do monitorowania, rejestrowania lub kontroli, które są zgodne z zasadami ochrony prywatności dla takich systemów, które generalnie zakazują tych działań; oraz</td></tr>
<tr><td>AC-8(c)(3)</td><td colspan="2">system informacyjny zawiera opis dozwolonych sposobów korzystania z systemu.</td></tr>
<tr><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Zasady kontroli dostępu; polityka bezpieczeństwa i prywatności, procedury dotyczące powiadamiania o zasadach użycia systemu; udokumentowane zatwierdzanie komunikatów lub banerów dotyczących wykorzystania systemu informacyjnego; zapisy z audytu systemu informacyjnego; potwierdzenia użytkownika dotyczące komunikatu lub baneru dotyczącego powiadomienia; dokumentacja projektowa systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; komunikaty powiadamiające wykorzystywane przez system informacyjny; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za udzielanie porad prawnych; deweloperzy systemów].
Test: [wybierz spośród: Zautomatyzowane mechanizmy wdrażania systemu wykorzystywania powiadomień].</td></tr>
</table>

<table>
<tr><th colspan="2">AC-9 POWIADAMIANIE O ZALOGOWANIU</th></tr>
<tr><td rowspan="2"></td><td>CEL OCENY:
Ustalić, czy system informacyjny powiadamia użytkownika, po pomyślnym zalogowaniu (dostępie) do systemu, o dacie i godzinie ostatniego logowania (dostępu).</td></tr>
<tr><td>POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Zasady kontroli dostępu; procedury dotyczące powiadamiania o zalogowaniu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; komunikaty powiadomień systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].</td></tr>
</table>

AC-9	**POWIADAMIANIE O ZALOGOWANIU**
	Wywiad: [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające politykę kontroli dostępu w odniesieniu do poprzedniego powiadomienia o logowaniu].

AC-9(1)	**POWIADAMIANIE O ZALOGOWANIU | *NIEPOPRAWNE LOGOWANIE***
	CEL OCENY: *Ustalenie, czy system informacyjny powiadamia użytkownika, po udanym zalogowaniu/udanym dostępie, o liczbie nieudanych prób logowania/udanego dostępu od ostatniego udanego logowania/udanego dostępu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące powiadamiania o zalogowaniu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające politykę kontroli dostępu w odniesieniu do poprzedniego powiadomienia o logowaniu].

AC-9(2)	**POWIADAMIANIE O ZALOGOWANIU | *POMYŚLNE / NIEUDANE LOGOWANIA***	
	CEL OCENY: *Określić, czy:*	
	AC-9(2)[1]	*organizacja określa okres czasu, w którym system informacyjny musi powiadomić użytkownika o liczbie:*
		AC-9(2)[1][a] *udanych logowań/dostęp; i/lub*
		AC-9(2)[1][b] *nieudanych próbach logowania/dostępu;*
	AC-9(2)[2]	*system informacyjny, w określonym przez organizację okresie czasu, powiadamia użytkownika o liczbie:*
		AC-9(2)[2][a] *udanych logowań/dostępach; i/lub*

AC-9(2)	**POWIADAMIANIE O ZALOGOWANIU | *POMYŚLNE / NIEUDANE LOGOWANIA***	
	AC-9(2)[2][b]	*nieudanych próbach logowania/dostępu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące powiadamiania o zalogowaniu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające politykę kontroli dostępu w odniesieniu do poprzedniego powiadomienia o logowaniu].	

AC-9(3)	**POWIADAMIANIE O ZALOGOWANIU | *POWIADOMIENIE O ZMIANACH W KONCIE***	
	CEL OCENY: *Określić, czy:*	
	AC-9(3)[1]	*organizacja definiuje cechy/parametry bezpieczeństwa konta użytkownika;*
	AC-9(3)[2]	*organizacja określa okres czasu, w którym muszą nastąpić zmiany w zdefiniowanych przez organizację cechach/parametrach bezpieczeństwa konta użytkownika; oraz*
	AC-9(3)[3]	*system informacyjny powiadamia użytkownika o zmianach w zdefiniowanych przez organizację cechach/parametrach bezpieczeństwa konta użytkownika w określonym przez organizację okresie czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące powiadamiania o zalogowaniu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AC-9(3)	**POWIADAMIANIE O ZALOGOWANIU | *POWIADOMIENIE O ZMIANACH W KONCIE***
	Wywiad: [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające politykę kontroli dostępu w odniesieniu do poprzedniego powiadomienia o logowaniu].

AC-9(4)	**POWIADAMIANIE O ZALOGOWANIU | *DODATKOWE INFORMACJE DOTYCZĄCE LOGOWANIA***	
	CEL OCENY: *Określić, czy:*	
	AC-9(4)[1]	*organizacja określa informacje, które mają być zawarte oprócz daty i godziny ostatniego logowania (dostępu); oraz*
	AC-9(4)[2]	*system informacyjny powiadamia użytkownika, po pomyślnym zalogowaniu się (dostępie), o informacjach zdefiniowanych przez organizację, które oprócz daty i godziny ostatniego logowania (dostępu), mają być zawarte w uzupełnieniu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące powiadamiania o zalogowaniu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające politykę kontroli dostępu w odniesieniu do poprzedniego powiadomienia o logowaniu].	

AC-10	**KONTROLA ILOŚCI RÓWNOCZESNYCH SESJI**	
	CEL OCENY: *Określić, czy:*	
	AC-10[1]	*organizacja definiuje konta i/lub typy kont dla całego systemu informacyjnego;*

AC-10	**KONTROLA ILOŚCI RÓWNOCZESNYCH SESJI**	
	AC-10[2]	*organizacja określa liczbę jednoczesnych sesji, które mają być dozwolone dla każdego zdefiniowanego przez organizację konta i/lub typu konta; oraz*
	AC-10[3]	*system informacyjny ogranicza liczbę jednoczesnych sesji dla każdego zdefiniowanego przez organizację konta i/lub typu konta do określonej przez organizację liczby jednoczesnych dozwolonych sesji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące kontroli ilości równoczesnych sesji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania zasad kontroli dostępu dotyczące kontroli ilości równoczesnych sesji].	

AC-11	**ZAMKNIĘCIE / BLOKADA SESJI**		
	CEL OCENY: *Określić, czy:*		
	AC-11(a)	**AC-11(a)[1]**	*organizacja określa okres braku aktywności użytkownika, po którym system informacyjny inicjuje zamknięcie/blokadę sesji;*
		AC-11(a)[2]	*system informacyjny uniemożliwia dalszy dostęp do systemu poprzez inicjowanie zamknięcia/blokady sesji po określonym przez organizację okresie braku aktywności użytkownika lub po otrzymaniu żądania od użytkownika; oraz*
	AC-11(b)	*system informacyjny utrzymuje zamknięcie/blokadę sesji do czasu przywrócenia przez użytkownika dostępu przy użyciu ustalonych procedur identyfikacji i uwierzytelniania.*	

AC-11	**ZAMKNIĘCIE / BLOKADA SESJI**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zamknięcia / blokady sesji; procedury dotyczące identyfikacji i uwierzytelniania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania zasad kontroli dostępu dotyczące zamknięcia / blokady sesji].

AC-11(1)	**ZAMKNIĘCIE / BLOKADA SESJI | *WYGASZACZ EKRANU***
	CEL OCENY: *Ustalenie, czy informacje wcześniej widoczne na ekranie zastępowane są system przez informacyjny wygaszaczem ekranu ukazującym publicznie dostępny obraz.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zamknięcia / blokady sesji; ekran wyświetlacza z włączoną funkcją zamknięcia / blokada sesji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Mechanizmy blokady / zamknięcia sesji systemu informacyjnego].

AC-12	**ZAKOŃCZENIE SESJI**	
	CEL OCENY: *Określić, czy:*	
	AC-12[1]	*organizacja określa warunki lub zdarzenia wymagające rozłączenia sesji; oraz*

AC-12	**ZAKOŃCZENIE SESJI**	
	AC-12[2]	*system informacyjny automatycznie kończy sesję użytkownika po wystąpieniu warunków zdefiniowanych przez organizację lub po wystąpieniu zdarzeń wymagających rozłączenia sesji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zakończenia sesji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista warunków lub zdarzeń powodujących konieczność rozłączenia sesji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące zakończenie sesji użytkownika].	

AC-12(1)	**ZAKOŃCZENIE SESJI | *WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA/ WYŚWIETLANIE KOMUNIKATU WYLOGOWANIA***		
	CEL OCENY: *Określić, czy:*		
	AC-12(1)(a)	**AC-12(1)(a)[1]**	*organizacja definiuje zasoby informacyjne, dla których wymagane jest uwierzytelnienie użytkownika w celu uzyskania dostępu do tych zasobów;*
		AC-12(1)(a)[2]	*system informacyjny zapewnia możliwość wylogowania się w przypadku sesji komunikacyjnych inicjowanych przez użytkownika, ilekroć uwierzytelnianie jest wykorzystywane do uzyskania dostępu do zdefiniowanych przez organizację zasobów informacyjnych; oraz*
	AC-12(1)(b)	*system informacyjny wyświetla użytkownikom jednoznaczny komunikat o wylogowaniu, informujący o bezpiecznym zakończeniu uwierzytelnionych sesji komunikacyjnych.*	

AC-12(1)	**ZAKOŃCZENIE SESJI | *WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA/ WYŚWIETLANIE KOMUNIKATU WYLOGOWANIA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zakończenia sesji; rejestr wiadomości o wylogowaniu się użytkownika; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Mechanizmy blokady / zamknięcia sesji systemu informacyjnego].

AC-13	**NADZÓR I PRZEGLĄD – KONTROLA DOSTĘPU**
[Włączone do: AC-2 oraz AU-6].	

AC-14	**DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA**		
	CEL OCENY: *Określić, czy organizacja:*		
	AC-14(a)	**AC-14(a)[1]**	*definiuje działania użytkownika, które mogą być wykonywane w systemie informacyjnym bez identyfikacji lub uwierzytelnienia zgodnego z misją organizacji/funkcjami biznesowymi;*
		AC-14(a)[2]	*identyfikuje zdefiniowane przez organizację działania użytkowników, które mogą być wykonywane w systemie informacyjnym bez identyfikacji lub uwierzytelnienia zgodnego z misją organizacji/funkcjami biznesowymi; oraz*
	AC-14(b)	*dokumentuje i uzasadnienia w planie bezpieczeństwa systemu informacyjnego, działania użytkowników niewymagające identyfikacji lub uwierzytelnienia.*	

AC-14	**DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; lista działań użytkownika, które mogą być wykonywane bez identyfikacji lub uwierzytelnienia; plan bezpieczeństwa; lista działań użytkownika, które mogą być wykonywane bez identyfikacji lub uwierzytelnienia; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

AC-14(1)	**DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA | *NIEZBĘDNE ZASTOSOWANIA***
[Włączone do: AC-14].	

AC-15	**ZAUTOMATYZOWANE ZNAKOWANIE**
[Włączone do: MP-3].	

AC-16	**ATRYBUTY BEZPIECZEŃSTWA**			
	CEL OCENY: *Określić, czy organizacja:*			
	AC-16(a)	**AC-16(a)[1]**	*definiuje rodzaje atrybutów bezpieczeństwa, które mogą być związane z informacjami:*	
			AC-16(a)[1][a]	*przechowywanych;*
			AC-16(a)[1][b]	*przetwarzanych; l/lub*
			AC-16(a)[1][c]	*przesyłanych;*
		AC-16(a)[2]	*definiuje wartości atrybutów bezpieczeństwa dla zdefiniowanych przez organizację typów atrybutów bezpieczeństwa;*	

<table>
<tr><th colspan="5">AC-16 ATRYBUTY BEZPIECZEŃSTWA</th></tr>
<tr><td></td><td></td><td>AC-16(a)[3]</td><td colspan="2">zapewnia środki umożliwiające powiązanie zdefiniowanych przez organizację typów atrybutów bezpieczeństwa i wartości atrybutów bezpieczeństwa z informacjami:</td></tr>
<tr><td></td><td></td><td></td><td>AC-16(a)[3][a]</td><td>przechowywanych;</td></tr>
<tr><td></td><td></td><td></td><td>AC-16(a)[3][b]</td><td>przetwarzanych; i/lub</td></tr>
<tr><td></td><td></td><td></td><td>AC-16(a)[3][c]</td><td>przesyłanych;</td></tr>
<tr><td></td><td>AC-16(b)</td><td colspan="3">zapewnia powiązanie atrybutu bezpieczeństwa z informacjami i jego trwałość;</td></tr>
<tr><td></td><td>AC-16(c)</td><td>AC-16(c)[1]</td><td colspan="2">definiuje systemy informacyjne, dla których mają być ustanowione dozwolone, zdefiniowane przez organizację systemy bezpieczeństwa atrybutu;</td></tr>
<tr><td></td><td></td><td>AC-16(c)[2]</td><td colspan="2">definiuje atrybuty bezpieczeństwo, które są dozwolone dla systemów informacyjnych zdefiniowanych przez organizację;</td></tr>
<tr><td></td><td></td><td>AC-16(c)[3]</td><td colspan="2">ustanawia dozwolone, określone przez organizację, atrybuty bezpieczeństwa zdefiniowanych przez organizację systemów informacyjnych;</td></tr>
<tr><td></td><td>AC-16(d)</td><td>AC-16(d)[1]</td><td colspan="2">definiuje wartości lub zakresy dla każdego z ustalonych atrybutów bezpieczeństwa; oraz</td></tr>
<tr><td></td><td></td><td>AC-16(d)[2]</td><td colspan="2">określa dozwolone, zdefiniowane przez organizację wartości lub zakresy dla każdego z ustalonych atrybutów bezpieczeństwa.</td></tr>
<tr><td></td><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:

Sprawdź: [wybierz spośród: Zasady kontroli dostępu; procedury dotyczące powiązania atrybutów bezpieczeństwa przechowywanymi, przetwarzanymi i przesyłanymi informacjami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

Wywiad: [wybierz spośród: Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów].

Test: [wybierz spośród: Zdolności organizacyjne wspierające i utrzymujące powiązanie atrybutów bezpieczeństwa z przechowywanymi, przetwarzanymi i przesyłanymi informacjami].</td></tr>
</table>

AC-16(1)	**ATRYBUTY BEZPIECZEŃSTWA | *DYNAMICZNE KOJARZENIE ATRYBUTÓW***	
	CEL OCENY: *Określić, czy:*	
	AC-16(1)[1]	*organizacja definiuje podmioty i obiekty, z którymi atrybuty bezpieczeństwa mają być dynamicznie kojarzone w miarę tworzenia i powiązania informacji;*
	AC-16(1)[2]	*organizacja definiuje polityki bezpieczeństwa wymagające od systemu informacyjnego dynamicznego powiązania atrybutów bezpieczeństwa z określonymi przez organizację podmiotami i obiektami; oraz*
	AC-16(1)[3]	*system informacyjny dynamicznie kojarzy atrybuty bezpieczeństwa ze zdefiniowanymi przez organizację podmiotami i obiektami, zgodnie ze zdefiniowanymi przez organizację politykami bezpieczeństwa, w miarę tworzenia i kojarzenia informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące dynamicznego powiązania atrybutów bezpieczeństwa z informacjami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające dynamiczne powiązanie atrybutów bezpieczeństwa z informacjami].	

AC-16(2)	**ATRYBUTY BEZPIECZEŃSTWA | *ZMIANA WARTOŚCI ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY***
	CEL OCENY: *Określenie, czy system informacyjny zapewnia upoważnionym osobom (lub procesom działającym w ich imieniu) możliwość zdefiniowania lub zmiany wartości powiązanych atrybutów bezpieczeństwa.*

AC-16(2)	**ATRYBUTY BEZPIECZEŃSTWA | *ZMIANA WARTOŚCI ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zmian wartości atrybutów bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista osób upoważnionych do zmiany atrybutów bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zmianę wartości atrybutów bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy pozwalające na zmianę wartości atrybutów bezpieczeństwa].

AC-16(3)	**ATRYBUTY BEZPIECZEŃSTWA | *UTRZYMANIE KOJARZENIA ATRYBUTÓW PRZEZ SYSTEM INFORMACYJNY***	
	CEL OCENY: *Określić, czy:*	
	AC-16(3)[1]	*organizacja definiuje atrybuty bezpieczeństwa, które mogą być kojarzone z określonymi przez organizację podmiotami i przedmiotami;*
	AC-16(3)[2]	*organizacja określa podmioty i obiekty, które wymagają powiązania i integralności bezpieczeństwa atrybutów z takimi podmiotami i obiektami, które mają być utrzymywane; oraz*
	AC-16(3)[3]	*system informacyjny utrzymuje powiązanie i integralność atrybutów bezpieczeństwa zdefiniowanych przez organizację, które są przypisane do zdefiniowanych przez organizację podmiotów i obiektów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące powiązania atrybutów bezpieczeństwa z informacjami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy utrzymujące powiązanie i integralność atrybutów bezpieczeństwa z informacjami].	

AC-16(4)	**ATRYBUTY BEZPIECZEŃSTWA | *KOJARZENIE ATRYBUTÓW PRZEZ AUTORYZOWANY PERSONEL***	
	CEL OCENY: *Określić, czy:*	
	AC-16(4)[1]	*organizacja definiuje atrybuty bezpieczeństwa, jako kojarzone z podmiotami i przedmiotami przez uprawnione osoby (lub procesy działające w imieniu osób);*
	AC-16(4)[2]	*organizacja definiuje podmioty i obiekty wymagające skojarzenia zdefiniowanych przez organizację atrybutów bezpieczeństwa przez uprawnione osoby (lub procesy działające w imieniu osób); oraz*
	AC-16(4)[3]	*system informacyjny wspiera kojarzenie zdefiniowanych przez organizację atrybutów bezpieczeństwa ze zdefiniowanymi podmiotami i obiektami przez uprawnione osoby organizacyjne (lub procesy działające w imieniu osób).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące powiązania atrybutów bezpieczeństwa z informacjami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista użytkowników uprawnionych do kojarzenia atrybutów bezpieczeństwa z informacjami; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za powiązanie atrybutów bezpieczeństwa z informacją; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające powiązanie atrybutów bezpieczeństwa użytkowników z informacją].	

AC-16(5)	**ATRYBUTY BEZPIECZEŃSTWA | *ATRYBUTY BEZPIECZEŃSTWA PREZENTOWANE NA WYŚWIETLACZACH URZĄDZEŃ WYJŚCIOWYCH***	
	CEL OCENY: *Określić, czy:*	
	AC-16(5)[1]	*organizacja określa specjalne zasady rozpowszechniania, obsługi lub dystrybucji, które mają być stosowane w odniesieniu do każdego obiektu przekazywanego przez system informacyjny do urządzeń wyjściowych;*

AC-16(5)	**ATRYBUTY BEZPIECZEŃSTWA | *ATRYBUTY BEZPIECZEŃSTWA PREZENTOWANE NA WYŚWIETLACZACH URZĄDZEŃ WYJŚCIOWYCH***	
	AC-16(5)[2]	*system informacyjny wyświetla, w postaci czytelnej dla użytkownika, specjalne instrukcje rozpowszechniania, obchodzenia się lub dystrybucji określonych przez organizację atrybutów bezpieczeństwa każdego obiektu, które dany system przesyła do urządzeń wyjściowych w celu identyfikacji; oraz*
	AC-16(5)[3]	*system informacyjny wyświetla atrybuty bezpieczeństwa w formie czytelnej dla użytkownika na każdym obiekcie, który system przekazuje do urządzeń wyjściowych w celu zidentyfikowania określonych przez organizację specjalnych instrukcji rozpowszechniania, obsługi lub dystrybucji przy użyciu określonych przez organizację, czytelnych dla użytkownika, standaryzowanych zasad nazewnictwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące wyświetlania atrybutów bezpieczeństwa w formie czytelnej dla człowieka; specjalne instrukcje dotyczące rozpowszechniania, obsługi lub dystrybucji; typy standaryzowanych zasad nazewnictwa czytelnych dla człowieka; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Systemowe urządzenia wyjściowe wyświetlające atrybuty bezpieczeństwa w formie czytelnej dla człowieka na każdym obiekcie].	

AC-16(6)	**ATRYBUTY BEZPIECZEŃSTWA | *ZARZĄDZANIE POWIĄZANYMI ATRYBUTAMI BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-16(6)[1]	*definiuje atrybuty bezpieczeństwa, które mają być powiązane z podmiotami i obiektami;*
	AC-16(6)[2]	*definiuje podmioty i obiekty, które mają być powiązane z atrybutami bezpieczeństwa zdefiniowanymi przez organizację;*

AC-16(6)	**ATRYBUTY BEZPIECZEŃSTWA | *ZARZĄDZANIE POWIĄZANYMI ATRYBUTAMI BEZPIECZEŃSTWA***	
	AC-16(6)[3]	*definiuje politykę bezpieczeństwa w celu umożliwienia personelowi kojarzenia i utrzymywania kojarzenia atrybutów bezpieczeństwa zdefiniowanych przez organizację z podmiotami i obiektami zdefiniowanymi przez organizację; oraz*
	AC-16(6)[4]	*pozwala personelowi na kojarzenie i utrzymywanie kojarzenia atrybutów bezpieczeństwa określonych przez organizację ze zdefiniowanymi przez organizację podmiotami i obiektami zgodnie z ustalonymi przez organizację politykami bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące kojarzenia atrybutów bezpieczeństwa z podmiotami i obiektami; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kojarzenie i utrzymywanie kojarzenia atrybutów bezpieczeństwa z podmiotami i obiektami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające kojarzenie atrybutów bezpieczeństwa z obiektami i podmiotami].	

AC-16(7)	**ATRYBUTY BEZPIECZEŃSTWA | *INTERPRETACJA WSPÓLNYCH ATRYBUTÓW BEZPIECZEŃSTWA***
	CEL OCENY: *Ustalenie, czy organizacja zapewnia spójną interpretację atrybutów bezpieczeństwa przesyłanych pomiędzy rozproszonymi komponentami systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące spójnej interpretacji atrybutów bezpieczeństwa przekazywanych między rozproszonymi komponentami systemu informacyjnego; procedury dotyczące egzekwowania prawa dostępu; procedury dotyczące egzekwowania zasad przepływu informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

AC-16(7)	**ATRYBUTY BEZPIECZEŃSTWA | *INTERPRETACJA WSPÓLNYCH ATRYBUTÓW BEZPIECZEŃSTWA***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za zapewnienie spójnej interpretacji atrybutów bezpieczeństwa wykorzystywanych w działaniach związanych z egzekwowaniem dostępu i przepływem informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania dostępu i przepływu informacji].

AC-16(8)	**ATRYBUTY BEZPIECZEŃSTWA | *POWIĄZANIE TECHNIKI / TECHNOLOGII Z ATRYBUTAMI BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy:*	
	AC-16(8)[1]	*organizacja określa techniki lub technologie, które należy wdrożyć w celu powiązania atrybutów bezpieczeństwa z informacją;*
	AC-16(8)[2]	*organizacja określa poziom wiarygodności, który należy zapewnić, gdy system informacyjny wdraża technologie lub techniki określone przez organizację w celu powiązania atrybutów bezpieczeństwa z informacją; oraz*
	AC-16(8)[3]	*system informacyjny wdraża techniki lub technologie o zdefiniowanym przez organizację poziomie wiarygodności powiązania atrybutów bezpieczeństwa z informacją.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące powiązania atrybutów bezpieczeństwa z informacjami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za powiązanie atrybutów bezpieczeństwa z informacją; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test:** [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania technik lub technologii kojarzących atrybuty bezpieczeństwa z informacjami].	

AC-16(9)	**ATRYBUTY BEZPIECZEŃSTWA | *PONOWNY PRZYDZIAŁ ATRYBUTU BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-16(9)[1]	*określa techniki lub procedury oceny mechanizmów ponownej klasyfikacji stosowanych do zmiany skojarzenia atrybutów bezpieczeństwa z informacjami; oraz*
	AC-16(9)[2]	*zapewnia, że atrybuty bezpieczeństwa związane z informacjami są ponownie przydzielane tylko poprzez mechanizmy przeklasyfikowania zatwierdzone przy użyciu technik lub procedur zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zmiany przypisania atrybutów bezpieczeństwa do informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Procedury dotyczące zmiany przypisania atrybutów bezpieczeństwa do informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające techniki lub procedury ponownego przypisywania atrybutów bezpieczeństwa do informacji].	

AC-16(10)	**ATRYBUTY BEZPIECZEŃSTWA | *KONFIGURACJA ATRYBUTÓW BEZPIECZEŃSTWA PRZEZ UPOWAŻNIONE OSOBY***
	CEL OCENY: *Określenie, czy system informacyjny zapewnia uprawnionym osobom możliwość definiowania lub zmiany typu i wartości atrybutów zabezpieczeń dostępnych dla kojarzenia z podmiotami i obiektami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące konfiguracji atrybutów bezpieczeństwa przez uprawnione osoby; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

AC-16(10)	**ATRYBUTY BEZPIECZEŃSTWA | *KONFIGURACJA ATRYBUTÓW BEZPIECZEŃSTWA PRZEZ UPOWAŻNIONE OSOBY***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za definiowanie lub zmianę atrybutów bezpieczeństwa związanych z informacjami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementujące możliwość definiowania lub zmiany atrybutów bezpieczeństwa].

AC-17	**ZDALNY DOSTĘP**		
	CEL OCENY: *Określić, czy organizacja:*		
	AC-17(a)	**AC-17(a)[1]**	*identyfikuje rodzaje zdalnego dostępu do systemu informacyjnego;*
		AC-17(a)[2]	*ustanawia dla każdego dozwolonego typu zdalnego dostępu:*
			AC-17(a)[2][a] *ograniczenia użytkowania;*
			AC-17(a)[2][b] *wymagania dotyczące konfiguracji/podłączenia;*
			AC-17(a)[2][c] *wskazówki dotyczące wdrożenia;*
		AC-17(a)[3]	*dokumentacja dla każdego rodzaju dozwolonego zdalnego dostępu:*
			AC-17(a)[3][a] *ograniczenia użytkowania;*
			AC-17(a)[3][b] *wymagania dotyczące konfiguracji/podłączenia;*
			AC-17(a)[3][c] *wskazówki dotyczące wdrożenia; oraz*
	AC-17(b)	*umożliwia zdalny dostęp do systemu informacyjnego przed zezwoleniem na takie połączenia.*	

AC-17	**ZDALNY DOSTĘP**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące wdrożenia i wykorzystania zdalnego dostępu (w tym ograniczenia); plan zarządzania konfiguracją; plan bezpieczeństwa; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; uprawnienia do zdalnego dostępu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie połączeniami zdalnego dostępu; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Możliwość zarządzania zdalnym dostępem do systemu informacyjnego].

AC-17(1)	**ZDALNY DOSTĘP | *ZAUTOMATYZOWANE MONITOROWANIE / KONTROLA***
	CEL OCENY: *Ustalić, czy system informacyjny monitoruje i kontroluje metody zdalnego dostępu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zdalnego dostępu do systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; zapisy z monitoringu systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy monitorowania i kontroli metod zdalnego dostępu].

AC-17(2)	**ZDALNY DOSTĘP | *OCHRONA POUFNOŚCI / INTEGRALNOŚCI Z WYKORZYSTANIEM SZYFROWANIA***
	CEL OCENY: *Ustalenie, czy system informacyjny wdraża mechanizmy kryptograficzne w celu ochrony poufności i integralności sesji zdalnego dostępu.*

AC-17(2)	**ZDALNY DOSTĘP | *OCHRONA POUFNOŚCI / INTEGRALNOŚCI Z WYKORZYSTANIEM SZYFROWANIA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zdalnego dostępu do systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; mechanizmy kryptograficzne i związana z nimi dokumentacja konfiguracyjna; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficzne zapewniające poufność i integralność sesji zdalnego dostępu].

AC-17(3)	**ZDALNY DOSTĘP | *ZARZĄDZANIE PUNKTAMI KONTROLI DOSTĘPU***	
	CEL OCENY: *Określić, czy:*	
	AC-17(3)[1]	*organizacja określa liczbę zarządzanych punktów kontroli dostępu do sieci, przez które mają być kierowane wszystkie zdalne dostępy; oraz*
	AC-17(3)[2]	*system informacyjny kieruje wszystkie zdalne dostępy przez zdefiniowaną przez organizację liczbę zarządzanych punktów kontroli dostępu do sieci.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zdalnego dostępu do systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; lista wszystkich zarządzanych punktów kontroli dostępu do sieci; ustawienia konfiguracji systemu informacyjnego i związana z nimi dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy routingu wszystkich zdalnych dostępów przez zarządzane punkty kontroli dostępu do sieci].	

AC-17(4) ZDALNY DOSTĘP | *POLECENIA UPRZYWILEJOWANE / DOSTĘP*			
	CEL OCENY: *Określić, czy organizacja:*		
	AC-17(4)(a)	**AC-17(4)(a)[1]**	*definiuje wymagania dotyczące autoryzacji wykonywania uprzywilejowanych poleceń i dostępu do informacji istotnych z punktu widzenia bezpieczeństwa poprzez zdalny dostęp;*
		AC-17(4)(a)[2]	*upoważnia do wykonywania uprzywilejowanych poleceń i dostępu do informacji mających znaczenie dla bezpieczeństwa, poprzez zdalny dostęp, tylko dla potrzeb zdefiniowanych przez organizację; oraz*
	AC-17(4)(b)	*dokumentuje uzasadnienie takiego dostępu w planie bezpieczeństwa systemu informacyjnego.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zdalnego dostępu do systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; plan bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania zarządzania zdalnym dostępem].		

AC-17(5) ZDALNY DOSTĘP | *MONITOROWANIE NIEAUTORYZOWANYCH POŁĄCZEŃ*
[Włączone do: SI-4].

AC-17(6) ZDALNY DOSTĘP | *OCHRONA MECHANIZMÓW ZDALNEGO DOSTĘPU*	
	CEL OCENY: *Ustalenie, czy organizacja zapewnia, że użytkownicy chronią informacje o mechanizmach zdalnego dostępu przed nieautoryzowanym użyciem i udostępnieniem.*

AC-17(6)	**ZDALNY DOSTĘP | *OCHRONA MECHANIZMÓW ZDALNEGO DOSTĘPU***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące zdalnego dostępu do systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za wdrażanie lub monitorowanie zdalnego dostępu do systemu informacyjnego; użytkownicy systemu informacyjnego posiadający wiedzę na temat mechanizmów zdalnego dostępu; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

AC-17(7)	**ZDALNY DOSTĘP | *DODATKOWA OCHRONA DOSTĘPU DO FUNKCJI BEZPIECZEŃSTWA***
[Włączone do: AC-3 (10)].	

AC-17(8)	**ZDALNY DOSTĘP | *DEZAKTYWACJA NIEZABEZPIECZONYCH PROTOKOŁÓW SIECIOWYCH***
[Włączone do: CM-7].	

AC-17(9)	**ZDALNY DOSTĘP | *WYŁĄCZANIE / DEZAKTYWACJA DOSTĘPU***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-17(9)[1]	*określa okres czasu, w którym można niezwłocznie wyłączyć lub dezaktywować zdalny dostęp do systemu informacyjnego; oraz*
	AC-17(9)[2]	*zapewnia możliwość szybkiego wyłączenia lub dezaktywacji zdalnego dostępu do systemu informacyjnego w określonym przez organizację okresie czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące wyłączania lub dezaktywacji zdalnego dostępu do systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; plan bezpieczeństwa, rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AC-17(9)	**ZDALNY DOSTĘP | *WYŁĄCZANIE / DEZAKTYWACJA DOSTĘPU***
	Wywiad: [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcję wyłączania lub dezaktywacji zdalnego dostępu do systemu informacyjnego].

AC-18	**DOSTĘP BEZPRZEWODOWY**	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-18(a)	*ustanawia dla dostępu bezprzewodowego:*
	AC-18(a)[1]	*ograniczenia użytkowania;*
	AC-18(a)[2]	*wymagania dotyczące konfiguracji/podłączenia;*
	AC-18(a)[3]	*wytyczne dotyczące wdrożenia; oraz*
	AC-18(b)	*zezwala na bezprzewodowy dostęp do systemu informacyjnego przed zezwoleniem na takie połączenia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące wdrożenia i wykorzystania dostępu bezprzewodowego (w tym ograniczenia); plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zezwolenia na dostęp bezprzewodowy; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie bezprzewodowymi połączeniami dostępowymi; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Możliwość zarządzania dostępem bezprzewodowym do systemu informacyjnego].	

AC-18(1)	**DOSTĘP BEZPRZEWODOWY | *UWIERZYTELNIANIE I SZYFROWANIE***
	CEL OCENY: *Ustalić, czy system informacyjny chroni dostęp bezprzewodowy do systemu za pomocą szyfrowania oraz jednego lub kilku z poniższych elementów:*

AC-18(1)	**DOSTĘP BEZPRZEWODOWY | *UWIERZYTELNIANIE I SZYFROWANIE***	
	AC-18(1)[1]	*uwierzytelnianie użytkowników; i/lub*
	AC-18(1)[2]	*uwierzytelnianie urządzeń.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące wdrażania dostępu bezprzewodowego i użytkowania (w tym ograniczenia); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające zabezpieczenia dostępu bezprzewodowego do systemu informacyjnego].	

AC-18(2)	**DOSTĘP BEZPRZEWODOWY | *MONITOROWANIE POŁĄCZEŃ NIEAUTORYZOWANYCH***
[Włączone do: SI-4].	

AC-18(3)	**DOSTĘP BEZPRZEWODOWY | *DEZAKTYWACJA SIECI BEZPRZEWODOWEJ***
	CEL OCENY: *Ustalenie, czy przed udostępnieniem i wdrożeniem organizacja wyłącza, gdy nie są przewidziane do użytku, funkcje sieci bezprzewodowej wbudowane wewnętrznie w komponenty systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące wdrażania dostępu bezprzewodowego i użytkowania (w tym ograniczenia); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zarządzające dezaktywacją funkcji sieci bezprzewodowej, wbudowanych wewnątrz komponentów systemu informacyjnego].

AC-18(4)	**DOSTĘP BEZPRZEWODOWY | *OGRANICZENIE DOKONYWANIA KONFIGURACJI PRZEZ UŻYTKOWNIKÓW***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-18(4)[1]	*identyfikuje użytkowników, którzy mogą samodzielnie konfigurować właściwości sieci bezprzewodowej; oraz*
	AC-18(4)[2]	*jednoznacznie upoważnia zidentyfikowanych użytkowników do samodzielnego konfigurowania funkcji sieci bezprzewodowej.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące wdrażania dostępu bezprzewodowego i użytkowania (w tym ograniczenia); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy pozwalające na niezależną konfigurację przez użytkownika funkcji sieci bezprzewodowej].	

AC-18(5)	**DOSTĘP BEZPRZEWODOWY | *POZIOMY MOCY ANTEN / TRANSMISJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-18(5)[1]	*selekcjonuje anteny radiowe w celu zmniejszenia prawdopodobieństwa odbioru sygnałów użytkowych poza kontrolowanymi przez organizację granicami; oraz*
	AC-18(5)[2]	*kalibruje poziomy mocy nadawania, aby zmniejszyć prawdopodobieństwo, że użyteczne sygnały mogą być odbierane poza kontrolowanymi przez organizację granicami.*

AC-18(5)	**DOSTĘP BEZPRZEWODOWY | *POZIOMY MOCY ANTEN / TRANSMISJI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące wdrażania bezprzewodowego i użytkowania (w tym ograniczenia); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Funkcja dostępu bezprzewodowego chroniąca sygnały użyteczne przed nieautoryzowanym dostępem poza granicami organizacji].

AC-19	**KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH)**	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-19(a)	*ustanawia dla urządzeń mobilnych kontrolowanych przez organizację:*
	AC-19(a)[1]	*ograniczenia użytkowania;*
	AC-19(a)[2]	*wymagania dotyczące konfiguracji/podłączenia;*
	AC-19(a)[3]	*wytyczne dotyczące wdrożenia; oraz*
	AC-19(b)	*zezwala na podłączenie urządzeń mobilnych do organizacyjnych systemów informacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące kontroli dostępu do użytkowania urządzeń przenośnych (w tym ograniczenia); plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zezwolenia na połączenia urządzeń mobilnych z systemami informacyjnymi organizacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AC-19	**KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH)**
	Wywiad: [*wybierz spośród:* Personel organizacji korzystający z urządzeń mobilnych w celu uzyskania dostępu do systemów informacyjnych organizacji; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Funkcja kontroli dostępu upoważniająca do połączeń urządzeń mobilnych z systemami informacyjnymi organizacji].

AC-19(1)	**KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH) | *KORZYSTANIE Z ZAPISYWALNYCH / PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH***
[Włączone do: MP-7].	

AC-19(2)	**KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH) | *WYKORZYSTANIE OSOBISTYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH***
[Włączone do: MP-7].	

AC-19(3)	**KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH) | *WYKORZYSTANIE OGÓLNODOSTĘPNYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH***
[Włączone do: MP-7].	

AC-19(4)	**KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH) | *OGRANICZENIA DOTYCZĄCE INFORMACJI NIEJAWNYCH*[3]**			
	CEL OCENY: *Określić, czy organizacja:*			
	AC-19(4)(a)	*zakazuje używania nieklasyfikowanych urządzeń przenośnych w obiektach, w których znajdują się systemy informacyjne przetwarzające, przechowujące lub przesyłające informacje niejawne, chyba, że organ autoryzujący wyraźnie na to zezwoli;*		
	AC-19(4)(b)	*egzekwuje następujące ograniczenia w stosunku do osób dopuszczonych przez organ autoryzujący do korzystania z jawnych urządzeń przenośnych w obiektach wyposażonych w systemy informacyjne przetwarzające, przechowujące lub przesyłające informacje niejawne:*		
		AC-19(4)(b)(1)	*podłączenie jawnych urządzeń mobilnych do systemów przetwarzających informacje niejawne jest zabronione;*	
		AC-19(4)(b)(2)	*podłączenie nieklasyfikowanych urządzeń przenośnych do systemów przetwarzających informacji niejawne wymaga zgody organu autoryzującego;*	
		AC-19(4)(b)(3)	*stosowanie wewnętrznych lub zewnętrznych modemów lub interfejsów bezprzewodowych w urządzeniach nieklasyfikowanych jest zabronione;*	
		AC-19(4)(b)(4)	**AC-19(4)(b)(4)[1]**	*określa personel ds. bezpieczeństwa odpowiedzialny za przeglądy i inspekcje nieklasyfikowanych urządzeń przenośnych oraz informacji przechowywanych na tych urządzeniach;*
			AC-19(4)(b)(4)[2]	*poddawanie wyrywkowym przeglądom/kontrolom, przez określony w organizacji personel bezpieczeństwa, nieklasyfikowanych urządzeń przenośnych oraz informacji przechowywanych na tych urządzeniach;*

AC-19(4)	**KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH) | *OGRANICZENIA DOTYCZĄCE INFORMACJI NIEJAWNYCH*[3]**			
			AC-19(4)(b)(4)[3]	*w przypadku odnalezienia informacji niejawnych postępuje się zgodnie z polityką postępowania z incydentami;*
	AC-19(4)(c)	**AC-19(4)(c)[1]**	*określa zasady bezpieczeństwa zezwalające wyłącznie na połączenie niejawnych (klasyfikowanych) urządzeń przenośnych z niejawnymi systemami informacyjnymi; oraz*	
		AC-19(4)(c)[2]	*Zezwala na podłączenie niejawnych urządzeń przenośnych do niejawnych systemów informacyjnych zgodnie z określonymi przez organizację politykami bezpieczeństwa.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; polityka postępowania z incydentami; procedury dotyczące kontroli dostępu do urządzeń przenośnych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja dowodowa na potrzeby wyrywkowych kontroli i przeglądów urządzeń przenośnych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za wyrywkowe przeglądy/kontrole urządzeń przenośnych; personel organizacji korzystający z urządzeń przenośnych w obiektach, w których znajdują się systemy informacyjne przetwarzające, przechowujące lub przekazujące informacje niejawne; personel organizacji odpowiedzialny za reagowanie na incydenty; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zakazujące korzystania z wewnętrznych lub zewnętrznych modemów lub interfejsów bezprzewodowych w urządzeniach przenośnych].			

[3] Realizowane zgodnie z przepisami ustawy o ochronie informacji niejawnych.

AC-19(5)	**KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH) | *SZYFROWANIE ZAWARTOŚCI CAŁEGO URZĄDZENIA / WYBRANYCH ZASOBÓW URZĄDZENIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-19(5)[1]	*definiuje urządzenia mobilne, dla których wymagane jest pełne szyfrowanie urządzeń lub szyfrowanie kontenerowe w celu ochrony poufności i integralności informacji na tych urządzeniach; oraz*
	AC-19(5)[2]	*stosuje pełne szyfrowanie urządzeń lub szyfrowanie kontenerowe w celu ochrony poufności i integralności informacji na urządzeniach mobilnych zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Procedury dotyczące kontroli dostępu do urządzeń przenośnych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; mechanizm szyfrowania i związana z nim dokumentacja konfiguracyjna; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu do urządzeń przenośnych; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Mechanizmy szyfrujące chroniące poufność i integralność informacji w urządzeniach przenośnych].	

AC-20	**WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW INFORMACYJNYCH**	
	CEL OCENY: *Ustalić, czy organizacja ustanawia zasady i warunki, zgodne z wszelkimi relacjami zaufania ustanowionymi z innymi organizacjami posiadającymi, obsługującymi i/lub utrzymującymi zewnętrzne systemy informacyjne, umożliwiające upoważnionym osobom korzystanie z:*	
	AC-20(a)	*dostępu do systemu informacyjnego z zewnętrznych systemów informacyjnych; oraz*
	AC-20(b)	*przetwarzania, przechowywania lub przekazywania informacji kontrolowanych przez organizację za pomocą zewnętrznych systemów informacyjnych.*

AC-20	**WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW INFORMACYJNYCH**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące korzystania z zewnętrznych systemów informacyjnych; zasady i warunki dotyczące zewnętrznych systemów informacyjnych; wykaz typów aplikacji dostępnych z zewnętrznych systemów informacyjnych; maksymalna kategoryzacja bezpieczeństwa dla informacji przetwarzanych, przechowywanych lub przekazywanych w zewnętrznych systemach informacyjnych; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określenie zasad i warunków korzystania z zewnętrznych systemów informacyjnych w celu uzyskania dostępu do systemów organizacyjnych; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania zasad i warunków korzystania z zewnętrznych systemów informacyjnych].

AC-20(1)	**WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW INFORMACYJNYCH | *OGRANICZENIA AUTORYZOWANEGO DOSTĘPU***	
	CEL OCENY: *Ustalenie, czy organizacja zezwala upoważnionym jednostkom na korzystanie z zewnętrznego systemu informacyjnego w celu uzyskania dostępu do systemu informacyjnego lub w celu przetwarzania, przechowywania lub przekazywania informacji kontrolowanych przez organizację tylko wtedy, gdy organizacja:*	
	AC-20(1)(a)	*weryfikuje wdrożenie wymaganych środków bezpieczeństwa w systemie zewnętrznym, określonych w polityce bezpieczeństwa informacji organizacji i w planie bezpieczeństwa; lub*
	AC-20(1)(b)	*posiada zatwierdzone umowy o połączeniu lub przetwarzaniu systemu informacyjnego z jednostką organizacyjną udostępniającą zewnętrzny system informacyjny.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące korzystania z zewnętrznych systemów informacyjnych; plan bezpieczeństwa; umowy dotyczące podłączenia do systemu informacyjnego lub przetwarzania danych; dokumenty dotyczące zarządzania kontem; inne odpowiednie dokumenty lub rejestry].	

AC-20(1)	**WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW INFORMACYJNYCH | *OGRANICZENIA AUTORYZOWANEGO DOSTĘPU***
	Wywiad: [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wprowadzające ograniczenia w korzystaniu z zewnętrznych systemów informacyjnych].

AC-20(2)	**WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW INFORMACYJNYCH | *PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE***
	CEL OCENY: *Ustalić, czy organizacja ogranicza lub zakazuje korzystania z kontrolowanych przez organizację przenośnych urządzeń pamięci masowej przez uprawnione osoby w zewnętrznych systemach informacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące korzystania z zewnętrznych systemów informacyjnych; plan bezpieczeństwa; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; umowy dotyczące podłączenia do systemu informacyjnego lub przetwarzania danych; dokumenty dotyczące zarządzania kontem; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ograniczenie lub zakaz korzystania z kontrolowanych przez organizację urządzeń pamięci masowej w zewnętrznych systemach informacyjnych; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wprowadzające ograniczenia w korzystaniu z przenośnych urządzeń pamięci masowej].

AC-20(3)	**WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW INFORMACYJNYCH | *KOMPONENTY / URZĄDZENIA INNYCH SYSTEMÓW***
	CEL OCENY: *Ustalić, czy organizacja ogranicza lub zakazuje korzystania z systemów informacyjnych niebędących własnością organizacji, komponentów systemu lub urządzeń, do przetwarzania, przechowywania lub przekazywania informacji organizacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące korzystania z zewnętrznych systemów informacyjnych; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; umowy dotyczące podłączenia do systemu informacyjnego lub przetwarzania danych; dokumenty dotyczące zarządzania kontem; zapisy z audytu systemu informacyjnego, inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za wprowadzanie ograniczeń lub zakazów dotyczących korzystania z systemów informacyjnych, komponentów systemów lub urządzeń niebędących własnością organizacji; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wprowadzające ograniczenia w korzystaniu z systemów/części składowych/urządzeń niebędących własnością organizacji].

AC-20(4)	**WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW INFORMACYJNYCH | *SIECIOWE URZĄDZENIA MAGAZYNUJĄCE***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-20(4)[1]	*definiuje dostępne w sieci urządzenia pamięci masowej, których stosowanie w zewnętrznych systemach informacyjnych jest zabronione; oraz*
	AC-20(4)[2]	*zakazuje stosowania w zewnętrznych systemach informacyjnych zdefiniowanych przez organizację urządzeń pamięci masowej dostępnych w sieci.*

AC-20(4)	**WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW INFORMACYJNYCH | *SIECIOWE URZĄDZENIA MAGAZYNUJĄCE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące korzystania w zewnętrznych systemach informacyjnych z dostępnych w sieci urządzeń pamięci masowej; plan bezpieczeństwa, dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; umowy dotyczące podłączenia do systemu informacyjnego lub przetwarzania danych; wykaz urządzeń pamięci masowej dostępnych w sieci, których stosowanie w zewnętrznych systemach informacyjnych jest zabronione; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za wprowadzenie zakazu korzystania z dostępnych w sieci urządzeń pamięci masowej w zewnętrznych systemach informacyjnych; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zakazujące korzystania w zewnętrznych systemach informacyjnych z dostępnych sieciowych urządzeń pamięci masowej].

AC-21	**UDOSTĘPNIANIE INFORMACJI**		
	CEL OCENY: *Określić, czy organizacja:*		
	AC-21(a)	**AC-21(a)[1]**	*określa okoliczności udostępniania informacji, w których wymagana jest zgoda użytkownika;*
		AC-21(a)[2]	*ułatwia wymianę informacji poprzez umożliwienie autoryzowanym użytkownikom określenia, czy uprawnienia dostępu przydzielone partnerowi udostępniającemu informacje odpowiadają ograniczeniom dostępu do informacji w okolicznościach zdefiniowanych przez organizację;*
	AC-21(b)	**AC-21(b)[1]**	*definiuje zautomatyzowane mechanizmy lub procesy ręczne, które mają być stosowane, aby pomóc użytkownikom w podejmowaniu decyzji dotyczących udostępniania informacji/współpracy; oraz*

AC-21	**UDOSTĘPNIANIE INFORMACJI**		
		AC-21(b)[2]	*wykorzystuje zdefiniowane przez organizację zautomatyzowane mechanizmy lub procesy ręczne, aby pomóc użytkownikom w podejmowaniu decyzji dotyczących wymiany informacji i współpracy.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące współpracy z użytkownikami i udostępniania informacji (w tym ograniczeń); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista użytkowników upoważnionych do podejmowania decyzji o udostępnianiu informacji / współpracy; lista okoliczności udostępniania informacji wymagających zgody użytkownika; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za podejmowanie decyzji dotyczących wymiany informacji i współpracy; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy lub procesy ręczne implementujące uprawnienia dostępu wspierające decyzje dotyczące udostępniania informacji/ współpracy z użytkownikami].		

AC-21(1)	**UDOSTĘPNIANIE INFORMACJI | *ZAUTOMATYZOWANE WSPARCIE DECYZJI***	
	CEL OCENY: *Ustalić, czy system informacyjny wymusza podejmowanie decyzji o udostępnianiu informacji przez uprawnionych użytkowników na podstawie decyzji:*	
	AC-21(1)[1]	*zezwalających na dostęp partnerów współpracujących; oraz*
	AC-21(1)[2]	*ograniczających dostęp do informacji, które mają być udostępniane.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące współpracy z użytkownikami i udostępniania informacji (w tym ograniczeń); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; generowana przez system lista użytkowników upoważnionych do udostępniania informacji/decyzji dotyczących współpracy; generowana przez system lista partnerów udostępniających informacje i uprawnień dostępu; generowana przez system lista ograniczeń dostępu do informacji, które mają być udostępniane; inne odpowiednie dokumenty lub rejestry].	

AC-21(1)	**UDOSTĘPNIANIE INFORMACJI | *ZAUTOMATYZOWANE WSPARCIE DECYZJI***
	Wywiad: [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące uprawnienia dostępu wspierające decyzje dotyczące udostępniania informacji/ współpracy z użytkownikami].

AC-21(2)	**UDOSTĘPNIANIE INFORMACJI | *WYSZUKIWANIE I ODZYSKIWANIE INFORMACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-21(2)[1]	*organizacja definiuje ograniczenia w zakresie udostępniania informacji, które mają być egzekwowane poprzez usługi wyszukiwania i odzyskiwania informacji; oraz*
	AC-21(2)[2]	*system informacyjny wdraża usługi wyszukiwania i odzyskiwania informacji, które wymuszają, określone przez organizację, ograniczenia w zakresie udostępniania informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące współpracy z użytkownikami i wymiany informacji (w tym ograniczeń); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z nimi dokumentacja; wygenerowany przez system wykaz ograniczeń dostępu dotyczących informacji, które mają być udostępniane; rejestry wyszukiwania i odzyskiwania informacji; zapisy z audytu systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie dostępu do usług wyszukiwania i odzyskiwania systemów informacyjnych; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test:** [*wybierz spośród:* Usługi wyszukiwania i odzyskiwania danych w systemie informacyjnym wymuszające ograniczenia w zakresie wymiany informacji].	

AC-22	**TREŚCI PUBLICZNIE DOSTĘPNE**		
	CEL OCENY: *Określić, czy organizacja:*		
	AC-22(a)	*wyznacza osoby upoważnione do wprowadzania informacji do publicznie dostępnego systemu informacyjnego;*	
	AC-22(b)	*szkoli upoważniony personel w celu zapewnienia, że informacje publicznie dostępne nie zawierają informacji niepublicznych;*	
	AC-22(c)	*dokonuje przeglądu proponowanej treści informacji przed umieszczeniem ich w publicznie dostępnym systemie informacyjnym, aby upewnić się, że nie zawierają one informacji niepublicznych;*	
	AC-22(d)	**AC-22(d)[1]**	*określa częstotliwość przeglądania treści informacji niepublicznych w publicznie dostępnym systemie informacyjnym;*
		AC-22(d)[2]	*dokonuje przeglądu treści informacji niepublicznych w publicznie dostępnym systemie informacyjnym z częstotliwością określoną przez organizację; oraz*
		AC-22(d)[3]	*usuwa informacje niepubliczne z publicznie dostępnego systemu informacyjnego, jeżeli zostaną one odkryte.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące treści publicznie dostępnych; lista użytkowników uprawnionych do umieszczania publicznie dostępnych treści w systemach informacyjnych organizacji; materiały szkoleniowe i/lub rejestry; rejestry przeglądów informacji publicznie dostępnych; rejestry odpowiedzi na informacje niepubliczne na publicznych stronach internetowych; logi audytów systemowych; rekordy przeprowadzanych szkoleń w zakresie uświadamiania bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie publicznie dostępnymi informacjami zamieszczanymi w systemach informacyjnych organizacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające zarządzanie publicznie dostępnymi treściami].		

AC-23	**OCHRONA PRZED PRZESZUKIWANIEM DANYCH**	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-23[1]	*definiuje techniki wykrywania oraz zapobiegające inwigilacji danych, które mają być stosowane w zdefiniowanych przez organizację obiektach pamięci masowej, w celu właściwego wykrywania i ochrony przed inwigilacją danych;*
	AC-23[2]	*definiuje obiekty służące do przechowywania danych, które należy chronić przed inwigilacją danych; oraz*
	AC-23[3]	*wykorzystuje zdefiniowane przez organizację techniki zapobiegania inwigilacji danych i wykrywania obiektów przechowujących dane w celu odpowiedniego rozpoznania i ochrony przed penetracją danych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące technik inwigilacji danych; procedury dotyczące ochrony obiektów przechowujących dane przed inwigilacją danych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dzienniki audytu systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za wdrażanie technik wykrywania i zapobiegania inwigilacji danych w odniesieniu do obiektów przechowywania danych; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania prewencji i wykrywania inwigilacji danych].	

AC-24	**PRZYZNAWANIE PRAW DOSTĘPU**	
	CEL OCENY: *Określić, czy organizacja:*	
	AC-24[1]	*definiuje decyzje dotyczące przyznawania praw dostępu, które mają być stosowane do każdego wniosku o dostęp przed wykonaniem kontroli dostępu; oraz*
	AC-24[2]	*ustanawia procedury zapewniające stosowanie zdefiniowanych przez organizację zasad przyznawania praw dostępu w odniesieniu do każdego wniosku o dostęp przed wykonaniem kontroli dostępu.*

AC-24	**PRZYZNAWANIE PRAW DOSTĘPU**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące przyznawanie praw dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ustanowienie procedur dotyczących przyznawania praw dostępu do systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy stosujące wdrożone procedury przyznawanie praw dostępu].

AC-24(1)	**PRZYZNAWANIE PRAW DOSTĘPU | *PRZESYŁANIE INFORMACJI O AUTORYZACJI DOSTĘPU***	
	CEL OCENY: *Określić, czy:*	
	AC-24(1)[1]	*organizacja definiuje informacje o autoryzacji dostępu, które system informacyjny przekazuje do zdefiniowanych przez organizację systemów informacyjnych, egzekwujących przyznawanie praw dostępu;*
	AC-24(1)[2]	*organizacja definiuje środki bezpieczeństwa, które mają być stosowane, gdy system informacyjny przekazuje informacje o autoryzacji dostępu do zdefiniowanych przez organizację systemów informacyjnych, wymuszających przyznawanie praw dostępu;*
	AC-24(1)[3]	*organizacja definiuje systemy informacyjne, które wymuszają przyznawanie prawa dostępu; oraz*
	AC-24(1)[4]	*system informacyjny przekazuje informacje o uprawnieniach dostępu zdefiniowanych przez organizację przy użyciu zdefiniowanych przez organizację zabezpieczeń do określonych przez organizację systemów informacyjnych wymuszających przyznawanie praw dostępu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące egzekwowania prawa dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AC-24(1)	**PRZYZNAWANIE PRAW DOSTĘPU | *PRZESYŁANIE INFORMACJI O AUTORYZACJI DOSTĘPU***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test:** [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania dostępu**].**

AC-24(2)	**PRZYZNAWANIE PRAW DOSTĘPU | *BRAK TOŻSAMOŚCI UŻYTKOWNIKA LUB PROCESU***	
	CEL OCENY: *Określić, czy:*	
	AC-24(2)[1]	*organizacja definiuje atrybuty bezpieczeństwa wspierające przyznawanie praw dostępu, które nie obejmują tożsamości użytkownika lub procesów działających w jego imieniu; oraz*
	AC-24(2)[2]	*system informacyjny wymusza przyznawanie praw dostępu w oparciu o zdefiniowany organizacyjnie atrybuty bezpieczeństwa, które nie obejmują tożsamości użytkownika lub procesu działającego w jego imieniu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące egzekwowania prawa dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test:** [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania dostępu**].**	

AC-25	**MONITOROWANIE REFERENCYJNE**	
	CEL OCENY: *Określić, czy:*	
	AC-25[1]	*organizacja określa zasady kontroli dostępu, dla których system informacyjny wdraża monitorowanie referencyjne, w celu egzekwowania tych zasad; oraz*
	AC-25[2]	*system informacyjny wdraża monitorowanie referencyjne dla zdefiniowanych przez organizację reguł kontroli dostępu, które jest odporne na manipulacje, zawsze przywoływane i na tyle ograniczone, że może być poddane analizie i testom, których kompletność można zapewnić.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące egzekwowania prawa dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za egzekwowanie praw dostępu; administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test:** [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje egzekwowania dostępu**].**	

KATEGORIA AT - UŚWIADAMIANIE I SZKOLENIA

AT-1	**ŚWIADOMOŚĆ BEZPIECZEŃSTWA, POLITYKA I PROCEDURY SZKOLENIOWE**			
	CEL OCENY: *Określić, czy organizacja:*			
	AT-1(a)(1)	**AT-1(a)(1)[1]**	*opracowuje i dokumentuje politykę uświadamiania i szkolenia w zakresie bezpieczeństwa, która dotyczy:*	
			AT-1(a)(1)[1][a]	*celu;*
			AT-1(a)(1)[1][b]	*zakresu stosowania;*
			AT-1(a)(1)[1][c]	*ról;*
			AT-1(a)(1)[1][d]	*odpowiedzialności;*
			AT-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			AT-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			AT-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		AT-1(a)(1)[2]	*określa personel lub role, którym ma być rozpowszechniana polityka świadomości i szkolenia w zakresie bezpieczeństwa;*	
		AT-1(a)(1)[3]	*rozpowszechnia politykę świadomości i szkolenia w zakresie bezpieczeństwa wśród personelu lub ról zdefiniowanych przez organizację;*	
	AT-1(a)(2)	**AT-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrożenie polityki świadomości i szkolenia w zakresie bezpieczeństwa oraz związanych z nią kontroli świadomości i szkolenia;*	
		AT-1(a)(2)[2]	*określa personel lub role, którym procedury mają być rozpowszechniane;*	
		AT-1(a)(2)[3]	*rozpowszechnia procedury wśród personelu / ról określonego przez organizację;*	

AT-1	**ŚWIADOMOŚĆ BEZPIECZEŃSTWA, POLITYKA I PROCEDURY SZKOLENIOWE**		
	AT-1(b)(1)	**AT-1(b)(1)[1]**	*określa częstotliwość przeglądu i aktualizacji obecnej polityki w zakresie świadomości i szkolenia w zakresie bezpieczeństwa;*
		AT-1(b)(1)[2]	*dokonuje przeglądu i aktualizacji aktualnej polityki świadomości i szkolenia w zakresie bezpieczeństwa z częstotliwością określoną przez organizację;*
	AT-1(b)(2)	**AT-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji aktualnej świadomości bezpieczeństwa i procedur szkoleniowych; oraz*
		AT-1(b)(2)[2]	*dokonuje przeglądu i aktualizacji aktualnej świadomości bezpieczeństwa i procedur szkoleniowych z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Świadomość bezpieczeństwa, polityka i procedury szkoleniowe; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji posiadający świadomość bezpieczeństwa i przeszkolony w zakresie odpowiedzialności za bezpieczeństwo; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

AT-2	**SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA**	
	CEL OCENY: *Określić, czy organizacja:*	
	AT-2(a)	*zapewnia podstawowe szkolenie w zakresie uświadamiania bezpieczeństwa użytkownikom systemów informacyjnych (w tym menedżerom, wyższej kadrze kierowniczej i kontrahentom) w ramach szkoleń wstępnych dla nowych użytkowników;*
	AT-2(b)	*zapewnia podstawowe szkolenie w zakresie uświadamiania bezpieczeństwa dla użytkowników systemów informacyjnych (w tym kierownikom, wyższej kadrze kierowniczej i kontrahentom), gdy wymagają tego zmiany wprowadzane w systemie informacyjnym; oraz*

AT-2	**SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA**		
	AT-2(c)	**AT-2(c)[1]**	*określa częstotliwość przeprowadzania szkoleń aktualizujących użytkownikom systemów informacyjnych (w tym kierownikom, wyższej kadrze kierowniczej i kontrahentom w zakresie uświadamiania bezpieczeństwa; oraz*
		AT-2(c)[2]	*zapewnia szkolenia aktualizujące w zakresie uświadamiania bezpieczeństwa użytkownikom informacji (w tym menedżerom, wyższej kadrze kierowniczej i kontrahentom) z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Świadomość bezpieczeństwa, polityka i procedury szkoleniowe; procedury dotyczące wdrażania szkolenia w zakresie świadomości bezpieczeństwa; odpowiednie przepisy i regulacje; program szkolenia w zakresie świadomości bezpieczeństwa; materiały szkoleniowe w zakresie świadomości bezpieczeństwa; plan bezpieczeństwa; rejestry szkoleniowe; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za szkolenie w zakresie świadomości bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji tworzący ogólną wspólnotę użytkowników systemu informacyjnego]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zarządzania szkoleniami świadomości w zakresie bezpieczeństwa].		

AT-2(1)	**SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | *ĆWICZENIA PRAKTYCZNE***
	CEL OCENY: *Ustalenie, czy organizacja prowadzi praktyczne ćwiczenia w zakresie świadomości bezpieczeństwa, które symulują rzeczywiste cyberataki.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Świadomość bezpieczeństwa, polityka i procedury szkoleniowe; procedury dotyczące wdrażania szkolenia w zakresie świadomości bezpieczeństwa; program szkolenia w zakresie świadomości bezpieczeństwa; materiały szkoleniowe w zakresie świadomości bezpieczeństwa; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry].

AT-2(1)	**SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | *ĆWICZENIA PRAKTYCZNE***
	Wywiad: [*wybierz spośród:* Personel organizacji uczestniczący w szkoleniach świadomości bezpieczeństwa; personel organizacji odpowiedzialny za szkolenia świadomości bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące symulacje cyberataków w ćwiczeniach praktycznych].

AT-2(2)	**SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | *ZAGROŻENIE WEWNĘTRZNE***
	CEL OCENY: *Ustalenie, czy organizacja prowadzi szkolenia z zakresu świadomości bezpieczeństwa w zakresie rozpoznawania i zgłaszania potencjalnych wskaźników zagrożeń wewnętrznych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Świadomość bezpieczeństwa, polityka i procedury szkoleniowe; procedury dotyczące wdrażania szkolenia w zakresie świadomości bezpieczeństwa; program szkolenia w zakresie świadomości bezpieczeństwa; materiały szkoleniowe w zakresie świadomości bezpieczeństwa; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji uczestniczący w szkoleniach świadomości bezpieczeństwa; personel organizacji odpowiedzialny za podstawowe szkolenia świadomości bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

AT-3	**SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH**	
	CEL OCENY: *Określić, czy organizacja:*	
	AT-3(a)	*prowadzi szkolenia w zakresie bezpieczeństwa opartego na rolach dla personelu, który przed autoryzowaniem dostępu do systemu informacyjnego lub wykonaniem przydzielonych mu obowiązków ma przydzielone role i obowiązki w zakresie bezpieczeństwa;*

AT-3	**SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH**		
	AT-3(b)	*zapewnia szkolenie w zakresie bezpieczeństwa opartego na rolach personelowi z przydzielonymi rolami i obowiązkami w zakresie bezpieczeństwa, gdy jest to wymagane przez zmiany w systemie informacyjnym; oraz*	
	AT-3(c)	**AT-3(c)[1]**	*określa częstotliwość przeprowadzania szkoleń aktualizujących w zakresie bezpieczeństwa opartego na rolach dla personelu, któremu przydzielono role i odpowiedzialność w zakresie bezpieczeństwa; oraz*
		AT-3(c)[2]	*zapewnia aktualizacje szkolenia w zakresie bezpieczeństwa opartego na rolach personelowi z przydzielonymi rolami i obowiązkami w zakresie bezpieczeństwa z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Świadomość bezpieczeństwa, procedury dotyczące wdrażania szkoleń z zakresu bezpieczeństwa; stosowne przepisy i regulacje; program szkolenia z zakresu bezpieczeństwa; materiały szkoleniowe z zakresu bezpieczeństwa; plan bezpieczeństwa; rejestry szkoleniowe; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za szkolenie w zakresie bezpieczeństwa w oparciu o role; personel organizacji z przydzielonymi rolami i obowiązkami w zakresie bezpieczeństwa systemów informacyjnych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zarządzania szkoleniami dotyczącymi bezpieczeństwa w oparciu o role].		

AT-3(1)	**SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | *ZABEZPIECZENIA ŚRODOWISKOWE***	
	CEL OCENY: *Określić, czy organizacja:*	
	AT-3(1)[1]	*definiuje personel lub role, które mają być zapewnione w ramach wstępnego i uaktualniającego szkolenia w zakresie wykorzystania i funkcjonowania zabezpieczeń środowiskowych;*
	AT-3(1)[2]	*określa personel lub role, które mają być zapewnione przez organizację, w tym szkolenie wstępne i dokształcające w zakresie zapewniania zatrudnienia i funkcjonowania systemu zabezpieczeń środowiskowych;*

AT-3(1)	**SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | *ZABEZPIECZENIA ŚRODOWISKOWE***	
	AT-3(1)[3]	*definiuje częstotliwość przeprowadzania szkoleń doskonalących w zakresie wykorzystania i funkcjonowania systemu zabezpieczeń środowiskowych; oraz*
	AT-3(1)[4]	*zapewnia szkolenia doskonalące w zakresie wykorzystania i funkcjonowania zabezpieczeń środowiskowych z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Świadomość bezpieczeństwa, polityka i procedury szkoleniowe; procedury dotyczące wdrażania szkolenia w zakresie bezpieczeństwa; program szkolenia w zakresie bezpieczeństwa; materiały szkoleniowe w zakresie bezpieczeństwa; plan bezpieczeństwa; rejestry szkoleniowe; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za szkolenia z zakresu bezpieczeństwa w oparciu o role; personel organizacji odpowiedzialny za wdrażanie i prowadzenie zabezpieczeń środowiskowych].	

AT-3(2)	**SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | *ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO***	
	CEL OCENY: *Określić, czy organizacja:*	
	AT-3(2)[1]	*definiuje personel lub role, którym ma być zapewnione szkolenie wstępne i doskonalące w zakresie wykorzystywania i obsługi środków bezpieczeństwa fizycznego;*
	AT-3(2)[2]	*określa personel lub role, którym ma być zapewnione przez organizację szkolenie wstępne i uzupełniające w zakresie wykorzystania i eksploatacji środków bezpieczeństwa fizycznego;*
	AT-3(2)[3]	*definiuje częstotliwość przeprowadzania szkoleń aktualizujących w zakresie wykorzystania i eksploatacji środków bezpieczeństwa fizycznego; oraz*
	AT-3(2)[4]	*zapewnia szkolenia aktualizujące w zakresie wykorzystania i obsługi środków bezpieczeństwa fizycznego z częstotliwością określoną przez organizację.*

AT-3(2)	**SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | *ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Świadomość bezpieczeństwa, polityka i procedury szkoleniowe; procedury dotyczące wdrażania szkolenia w zakresie bezpieczeństwa; program szkolenia w zakresie bezpieczeństwa; materiały szkoleniowe w zakresie bezpieczeństwa; plan bezpieczeństwa; rejestry szkoleniowe; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za szkolenie w zakresie bezpieczeństwa w oparciu o role; personel organizacji odpowiedzialny za wdrażanie i eksploatację środków bezpieczeństwa fizycznego].

AT-3(3)	**SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | *ĆWICZENIA PRAKTYCZNE***
	CEL OCENY: *Ustalić, czy organizacja włącza ćwiczenia praktyczne do szkoleń z zakresu bezpieczeństwa, które wspierają cele szkoleniowe.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Świadomość bezpieczeństwa, polityka i procedury szkoleniowe; procedury dotyczące wdrażania szkolenia w zakresie świadomości bezpieczeństwa; program szkolenia w zakresie świadomości bezpieczeństwa; materiały szkoleniowe w zakresie świadomości bezpieczeństwa; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za szkolenie w zakresie bezpieczeństwa w oparciu o role; personel organizacji uczestniczący w szkoleniach w zakresie uświadamiania bezpieczeństwa].

AT-3(4)	**SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | *PODEJRZANE TRANSMISJE I ANOMALIE ZACHOWANIA SYSTEMU***	
	CEL OCENY: *Określić, czy organizacja:*	
	AT-3(4)[1]	*definiuje wskaźniki złośliwego kodu; oraz*

AT-3(4)	**SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | *PODEJRZANE TRANSMISJE I ANOMALIE ZACHOWANIA SYSTEMU***	
	AT-3(4)[2]	*prowadzi szkolenia dla swojego personelu w zakresie zdefiniowanych przez organizację wskaźników złośliwego kodu w celu rozpoznania podejrzanej komunikacji i anomalii w systemach informacyjnych organizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Świadomość bezpieczeństwa, polityka i procedury szkoleniowe; procedury dotyczące wdrażania szkolenia w zakresie bezpieczeństwa; program szkolenia w zakresie bezpieczeństwa; materiały szkoleniowe w zakresie bezpieczeństwa; plan bezpieczeństwa; rejestry szkoleniowe; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za szkolenie w zakresie bezpieczeństwa w oparciu o role; personel organizacji uczestniczący w szkoleniach w zakresie uświadamiania bezpieczeństwa].	

AT-4	**REJESTROWANIE SZKOLEŃ Z ZAKRESU BEZPIECZEŃSTWA**			
	CEL OCENY: *Określić, czy organizacja:*			
	AT-4(a)	**AT-4(a)[1]**	*dokumentuje indywidualne działania szkoleniowe w zakresie bezpieczeństwa systemu informacyjnego, w tym:*	
			AT-4(a)[1][a]	*podstawowe szkolenia w zakresie świadomości bezpieczeństwa;*
			AT-4(a)[1][b]	*szkolenia w zakresie bezpieczeństwa systemu informacyjnego w oparciu o konkretne role;*
		AT-4(a)[2]	*monitoruje indywidualne działania szkoleniowe w zakresie bezpieczeństwa systemów informacyjnych, w tym:*	
			AT-4(a)[2][a]	*podstawowe szkolenia w zakresie świadomości bezpieczeństwa;*
			AT-4(a)[2][b]	*szkolenia w zakresie bezpieczeństwa systemu informacyjnego w oparciu o konkretne role;*

AT-4	**REJESTROWANIE SZKOLEŃ Z ZAKRESU BEZPIECZEŃSTWA**		
	AT-4(b)	**AT-4(b)[1]**	*określa okres czasu, w ciągu którego należy zachować indywidualny rejestr szkoleniowy; oraz*
		AT-4(b)[2]	*zachowuje indywidualny rejestr szkoleniowy na określony przez organizację okres czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Świadomość bezpieczeństwa, polityka i procedury szkoleniowe; procedury dotyczące rejestrowania szkoleń z zakresu bezpieczeństwa; świadomość bezpieczeństwa i rejestry szkoleniowe; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji prowadzący szkolenia z zakresu bezpieczeństwa odpowiadający za przechowywanie dokumentacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające zarządzanie dokumentacją szkoleniową w zakresie bezpieczeństwa].		

AT-5	**KONTAKTY Z GRUPAMI I STOWARZYSZENIAMI ZAJMUJĄCYMI SIĘ BEZPIECZEŃSTWEM INFORMACJI**
[Włączone do: PM-15].	

KATEGORIA AU - AUDYT I ROZLICZALNOŚĆ

AU-1	**POLITYKA ORAZ PROCEDURY W ZAKRESIE AUDYTU I ROZLICZALNOŚCI**			
	CEL OCENY: *Określić, czy organizacja:*			
	AU-1(a)(1)	**AU-1(a)(1)[1]**	*opracowuje i dokumentuje politykę w zakresie audytu i odpowiedzialności, która dotyczy:*	
			AU-1(a)(1)[1][a]	*celu;*
			AU-1(a)(1)[1][b]	*zakresu stosowania;*
			AU-1(a)(1)[1][c]	*ról;*
			AU-1(a)(1)[1][d]	*odpowiedzialności;*
			AU-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			AU-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			AU-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		AU-1(a)(1)[2]	*określa personel lub role, wśród których należy upowszechniać politykę audytu i rozliczalności;*	
		AU-1(a)(1)[3]	*rozpowszechnia politykę audytu i rozliczalności wśród personelu lub ról zdefiniowanych przez organizację;*	
	AU-1(a)(2)	**AU-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrażanie polityki w zakresie audytu i rozliczalności oraz związanych z nią zabezpieczenia w zakresie audytu i rozliczalności;*	
		AU-1(a)(2)[2]	*określa personel lub rolę, którym procedury mają być udostępniane;*	
		AU-1(a)(2)[3]	*rozpowszechnia procedury wśród zdefiniowanego przez organizację personelu lub ról;*	
	AU-1(b)(1)	**AU-1(b)(1)[1]**	*określa częstotliwość przeglądów i aktualizacji obecnej polityki w zakresie audytu i rozliczalności;*	

AU-1	**POLITYKA ORAZ PROCEDURY W ZAKRESIE AUDYTU I ROZLICZALNOŚCI**		
		AU-1(b)(1)[2]	*dokonuje przeglądu i aktualizacji aktualnej polityki w zakresie audytu i rozliczalności z częstotliwością określoną przez organizację;*
	AU-1(b)(2)	**AU-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji aktualnej polityki w zakresie audytu i rozliczalności;*
		AU-1(b)(2)[2]	*dokonuje przeglądu i aktualizacji aktualnych procedur audytu i rozliczalności zgodnie z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oraz procedury w zakresie audytu i rozliczalności; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

AU-2	**AUDYT ZDARZEŃ**		
	CEL OCENY: *Określić, czy organizacja:*		
	AU-2(a)	**AU-2(a)[1]**	*określa zdarzenia, które system informacyjny powinien być w stanie zweryfikować;*
		AU-2(a)[2]	*ustala, że system informacyjny jest zdolny do kontrolowania zdarzeń zdefiniowanych przez organizację;*
	AU-2(b)	*koordynuje funkcję audytu bezpieczeństwa z innymi jednostkami organizacyjnymi zajmującymi się informacjami związanymi z audytem w celu zwiększenia wzajemnego wsparcia i pomocy w wyborze zdarzeń podlegających audytowi;*	
	AU-2(c)	*uzasadnia konieczność przeprowadzania audytu zdarzeń celem wsparcia postępowania wyjaśniającego prowadzonego po fakcie wystąpienia zdarzenia naruszającego bezpieczeństwo;*	
	AU-2(d)	**AU-2(d)[1]**	*definiuje podzbiór zdarzeń podlegających kontroli określonych w kategorii AU-2a, które mają być kontrolowane w ramach systemu informacyjnego;*

AU-2	**AUDYT ZDARZEŃ**		
		AU-2(d)[2]	*określa, że podzbiór dających się skontrolować zdarzeń zdefiniowanych w kategorii AU-2a ma zostać skontrolowany w ramach systemu informacyjnego; oraz*
		AU-2(d)[3]	*określa częstotliwość audytu (lub sytuację wymagającą przeprowadzenia audytu) dla każdego zidentyfikowanego zdarzenia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące zdarzeń podlegających audytowi; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; zdarzenia podlegające audytowi systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące audyt systemu informacyjnego].		

AU-2(1)	**AUDYT ZDARZEŃ | *KOMPILACJA ZAPISÓW AUDYTU Z WIELU ŹRÓDEŁ***
[Włączone do: AU-12].	

AU-2(2)	**AUDYT ZDARZEŃ | *WYBÓR WYDARZEŃ AUDYTOWYCH WEDŁUG KOMPONENTÓW***
[Włączone do: AU-12].	

AU-2(3)	**AUDYT ZDARZEŃ | *OPINIE I AKTUALIZACJE***	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-2(3)[1]	*określa częstotliwość przeglądów i aktualizacji badanych zdarzeń; oraz*
	AU-2(3)[2]	*dokonuje przeglądów i aktualizacji zdarzeń podlegających audytowi z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące zdarzeń podlegających audytowi; plan bezpieczeństwa; lista zdefiniowanych przez organizację zdarzeń podlegających audytowi; przegląd zdarzeń podlegających audytowi i aktualizacja zapisów; zapisy z audytu systemu informacyjnego; raporty o incydentach w systemie informacyjnym; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające przegląd i aktualizację zdarzeń podlegających audytowi].	

AU-2(4)	**AUDYT ZDARZEŃ | *UPRZYWILEJOWANE FUNKCJE***
[Włączone do: AC-6(9)].	

AU-3	**ZAWARTOŚĆ REJESTRÓW AUDYTU**	
	CEL OCENY: *Ustalić, czy system informacyjny generuje zapisy z audytu zawierające informacje, które ustanawiają:*	
	AU-3[1]	*jaki rodzaj zdarzenia miał miejsce;*
	AU-3[2]	*kiedy zdarzenie miało miejsce;*
	AU-3[3]	*gdzie zdarzenie miało miejsce;*
	AU-3[4]	*źródło zdarzenia;*

AU-3	**ZAWARTOŚĆ REJESTRÓW AUDYTU**	
	AU-3[5]	*wynik zdarzenia; oraz*
	AU-3[6]	*tożsamość wszelkich osób lub podmiotów związanych z tym wydarzeniem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące zawartość rejestrów audytu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista zdefiniowanych przez organizację zdarzeń podlegających audytowi; zapisy z audytu systemu informacyjnego; raporty o incydentach w systemie informacyjnym; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wprowadzające audyt zdarzeń podlegających audytowi w systemie informacyjnym].	

AU-3(1)	**ZAWARTOŚĆ REJESTRÓW AUDYTU | *DODATKOWE INFORMACJE KONTROLNE***	
	CEL OCENY: *Określić, czy:*	
	AU-3(1)[1]	*organizacja definiuje dodatkowe, bardziej szczegółowe informacje, które mają być zawarte w zapisach z audytu generowanych przez system informacyjny; oraz*
	AU-3(1)[2]	*system informacyjny generuje zapisy z audytu zawierające zdefiniowane przez organizację dodatkowe, bardziej szczegółowe informacje.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące zawartości rejestrów audytu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista zdefiniowanych przez organizację zdarzeń podlegających audytowi; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zdolność audytu systemu informacyjnego].	

AU-3(2)	**ZAWARTOŚĆ REJESTRÓW AUDYTU | *CENTRALNE ZARZĄDZANIE TREŚCIĄ PLANOWANEGO REJESTRU AUDYTU***	
	CEL OCENY: *Określić, czy:*	
	AU-3(2)[1]	*organizacja definiuje składniki systemu informacyjnego, generujące zapisy z audytu, których zawartość ma być centralnie zarządzana i konfigurowana przez system informacyjny; oraz*
	AU-3(2)[2]	*system informacyjny zapewnia scentralizowane zarządzanie i konfigurację treści, które mają być rejestrowane w dokumentacji audytowej generowanej przez zdefiniowane przez organizację składniki systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące zawartości rejestrów audytu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista zdefiniowanych przez organizację zdarzeń podlegających audytowi; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Możliwości systemu informacyjnego wykorzystującego scentralizowane zarządzanie i konfigurację zawartości dokumentacji audytowej].	

AU-4	**PAMIĘĆ PRZECHOWYWANIA REKORDÓW AUDYTU**	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-4[1]	*określa wymagania dotyczące przechowywania zapisów z audytu; oraz*
	AU-4[2]	*przydziela pojemność pamięci masowej do zapisów z audytów zgodnie z wymaganiami przechowywania zapisów z audytów zdefiniowanymi przez organizację.*

AU-4	**PAMIĘĆ PRZECHOWYWANIA REKORDÓW AUDYTU**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące pojemności pamięci zapisów audytu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wymagania dotyczące przechowywania zapisów audytowych; zdolność przechowywania zapisów z audytu komponentów systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Pojemność pamięci masowej rekordu audytowego i związana z tym konfiguracja ustawień].

AU-4(1)	**PAMIĘĆ PRZECHOWYWANIA REKORDÓW AUDYTU | *TRANSFER REKORDÓW DO ALTERNATYWNYCH URZĄDZEŃ MAGAZYNUJĄCYCH***	
	CEL OCENY: *Określić, czy:*	
	AU-4(1)[1]	*organizacja określa częstotliwość przenoszenia zapisów z audytu do innego systemu lub nośnika niż system będący przedmiotem audytu; oraz*
	AU-4(1)[2]	*system informacyjny przenosi zapisy z audytu na inny system lub nośnik niż system będący przedmiotem audytu z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące pojemności pamięci zapisów audytu; procedury dotyczące przekazywania zapisów z audytu systemu informacyjnego do systemów zapasowych lub alternatywnych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dzienniki rejestrów audytów przekazywanych do systemów zapasowych lub alternatywnych; inne odpowiednie dokumenty lub rejestry].	

AU-4(1)	**PAMIĘĆ PRZECHOWYWANIA REKORDÓW AUDYTU | *TRANSFER REKORDÓW DO ALTERNATYWNYCH URZĄDZEŃ MAGAZYNUJĄCYCH***
	Wywiad: [*wybierz spośród:* Personel organizacji z odpowiedzialnością za projektowanie pojemności pamięci masowej; personel organizacji z odpowiedzialnością za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające przenoszenie zapisów z audytu do innego systemu].

AU-5	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU**		
	CEL OCENY: *Określić, czy:*		
	AU-5(a)	**AU-5(a)[1]**	*organizacja określa personel lub role, które mają być objęte powiadomieniem w przypadku awarii przetwarzania danych w ramach audytu;*
		AU-5(a)[2]	*system informacyjny alarmuje zdefiniowany przez organizację personel lub role w przypadku awarii przetwarzania danych w ramach audytu;*
	AU-5(b)	**AU-5(b)[1]**	*organizacja definiuje dodatkowe działania, które należy podjąć (np. wyłączenie systemu informacyjnego, nadpisanie najstarszych zapisów z audytu, zaprzestanie generowania zapisów z audytu) w przypadku awarii przetwarzania audytu; oraz*
		AU-5(b)[2]	*system informacyjny podejmuje dodatkowe, określone przez organizację działania w przypadku niepowodzenia przetwarzania audytu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące reakcji na błędy procesów audytu; dokumentacja projektowa systemu informacyjnego; plan bezpieczeństwa; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; wykaz personelu, który należy powiadomić w przypadku awarii przetwarzania danych w ramach audytu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].		

AU-5	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy reagowania systemu informacyjnego na awarie przetwarzania audytu].

AU-5(1)	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU | *PAMIĘĆ PRZECHOWYWANIA REKORDÓW AUDYTU***		
	CEL OCENY: *Określić, czy:*		
	AU-5(1)[1]	*organizacja określa:*	
		AU-5(1)[1][a]	*personel, który należy powiadomić, gdy przydzielona pojemność pamięci masowej zapisów audytowych osiągnie określony przez organizację procent maksymalnej pojemności pamięci masowej zapisów audytowych;*
		AU-5(1)[1][b]	*role, które należy powiadomić, gdy wielkość pamięci masowej przydzielonych zapisów z audytów osiągnie określony przez organizację procent maksymalnej pojemności pamięci masowej zapisów z audytów; i/lub*
		AU-5(1)[1][c]	*obiekty, które należy powiadomić, gdy przydzielony wolumen pamięci masowej zapisów audytowych osiągnie określony przez organizację procent maksymalnej pojemności pamięci masowej zapisów audytowych;*
	AU-5(1)[2]	*organizacja określa okres czasu, w którym system informacyjny ma przekazywać ostrzeżenie zdefiniowanemu przez organizację personelowi, rolom i/lub lokalizacjom, kiedy przydzielona pojemność pamięci masowej zapisów z audytów osiągnie określony przez organizację procent maksymalnej pojemności pamięci masowej zapisów z audytów;*	
	AU-5(1)[3]	*organizacja określa procent maksymalnej pojemności pamięci masowej zapisów z rejestrów audytów, którego osiągnięcie wymaga udzielenia ostrzeżenia; oraz*	

AU-5(1)	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU | *PAMIĘĆ PRZECHOWYWANIA REKORDÓW AUDYTU***	
	AU-5(1)[4]	*system informacyjny przekazuje ostrzeżenie zdefiniowanemu przez organizację personelowi, rolom i/lub obiektom w określonym przez organizację okresie czasu, kiedy przydzielona ilość pamięci zapisów z audytów osiągnie określony przez organizację procent maksymalnej pojemności pamięci zapisów z audytów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące reakcji na błędy procesów audytu; dokumentacja projektowa systemu informacyjnego; plan bezpieczeństwa; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wprowadzające ostrzeżenia o ograniczeniach w przechowywaniu danych audytowych].	

AU-5(2)	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU | *ALERTY CZASU RZECZYWISTEGO***		
	CEL OCENY: *Określić, czy:*		
	AU-5(2)[1]	*organizacja określa zdarzenia awarii procesów audytu wymagające powiadomień w czasie rzeczywistym;*	
	AU-5(2)[2]	*organizacja określa:*	
		AU-5(2)[2][a]	*personel, który ma być powiadamiany, gdy wystąpią określone przez organizację zdarzenia dotyczące nieprawidłowości w audycie wymagające alertów czasu rzeczywistego;*
		AU-5(2)[2][b]	*role, które należy zawiadamiać, gdy wystąpią określone przez organizację zdarzenia dotyczące nieprawidłowości w audycie wymagające alertów czasu rzeczywistego;*

AU-5(2)	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU | *ALERTY CZASU RZECZYWISTEGO***		
		AU-5(2)[2][c]	*obiekty, które mają być informowane o wystąpieniu zdefiniowanych przez organizację zdarzeń powodujących usterki procesów audytu wymagających alertów czasu rzeczywistego;*
	AU-5(2)[3]	*organizacja określa okres czasu rzeczywistego, w którym system informacyjny dostarcza ostrzeżenie do określonego przez organizację personelu, ról i/lub miejsc, w których wystąpią określone przez organizację zdarzenia dotyczące nieprawidłowości procesów audytu, powodujące wystąpienie alertów czasu rzeczywistego; oraz*	
	AU-5(2)[4]	*system informacyjny przekazuje w zdefiniowanym przez organizację okresie czasu rzeczywistego ostrzeżenie personelowi, rolom i/lub obiektom, gdy wystąpią określone przez organizację zdarzenia nieprawidłowości procesów audytu powodujące wystąpienie alertów czasu rzeczywistego.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące reakcji na błędy procesów audytu; dokumentacja projektowa systemu informacyjnego; plan bezpieczeństwa; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry powiadomień lub alerty czasu rzeczywistego, w przypadku wystąpienia błędów w przetwarzaniu danych z audytu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementujące alerty audytowe w czasie rzeczywistym w przypadku wystąpienia zdefiniowanych przez organizację zdarzeń niepowodzeń audytu].		

AU-5(3)	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU | *KONFIGUROWALNE PROGI NATĘŻENIA RUCHU***	
	CEL OCENY: *Określić, czy:*	
	AU-5(3)[1]	*system informacyjny wymusza konfigurowalne progi natężenia ruchu w komunikacji sieciowej, odzwierciedlające limity Zdolności audytowej;*

AU-5(3)	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU | *KONFIGUROWALNE PROGI NATĘŻENIA RUCHU***		
	AU-5(3)[2]	*organizacja wybiera, czy ruch w sieci ma być powyżej konfigurowalnych progów natężenia ruchu:*	
		AU-5(3)[2][a]	*odrzucony; lub*
		AU-5(3)[2][b]	*opóźniony; oraz*
	AU-5(3)[3]	*system informacyjny odrzuca lub opóźnia ruch komunikacyjny sieciowy generowany powyżej konfigurowalnych progów natężenia ruchu.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące reakcji na błędy procesów audytu; dokumentacja projektowa systemu informacyjnego; plan bezpieczeństwa; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; konfiguracja progów natężenia ruchu w komunikacji sieciowej; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Możliwości systemu informacyjnego wdrażającego konfigurowalne progi natężenia ruchu].		

AU-5(4)	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU | *WYŁĄCZENIE W PRZYPADKU AWARII***		
	CEL OCENY: *Określić, czy:*		
	AU-5(4)[1]	*organizacja wybiera jedno z następujących specyficznych działań dla systemu informacyjnego, które należy podjąć w przypadku zdefiniowanych przez organizację niepowodzeń audytu:*	
		AU-5(4)[1][a]	*pełne zamknięcie systemu;*
		AU-5(4)[1][b]	*częściowe wyłączenie systemu; lub*
		AU-5(4)[1][c]	*awaryjny tryb operacyjny z ograniczoną funkcjonalnością misyjną/biznesową;*

AU-5(4)	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU | *WYŁĄCZENIE W PRZYPADKU AWARII***	
	AU-5(4)[2]	*organizacja określa niepowodzenia audytu, które, o ile nie istnieje zdolność do alternatywnego audytu, mają spowodować uruchomienie systemu informacyjnego w celu wywołania określonego działania; oraz*
	AU-5(4)[3]	*system informacyjny uruchamia określone działanie w przypadku zdefiniowanych przez organizację niepowodzeń audytu, chyba, że istnieje zdolność do alternatywnego audytu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące reakcji na błędy procesów audytu; dokumentacja projektowa systemu informacyjnego; plan bezpieczeństwa; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zdolność systemu informacyjnego do wyłączenia systemu lub awaryjnego trybu pracy w przypadku awarii przetwarzania danych w procesie audytu].	

AU-6	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE**		
	CEL OCENY: *Określić, czy organizacja:*		
	AU-6(a)	**AU-6(a)[1]**	*definiuje rodzaje niewłaściwych lub nietypowych czynności, których należy szukać podczas przeglądania i analizy zapisów z systemu audytu informacyjnego;*
		AU-6(a)[2]	*określa częstotliwość przeglądania i analizowania zapisów z audytu systemu informacyjnego pod kątem wskazań na określone przez organizację niewłaściwe lub nietypowe czynności;*
		AU-6(a)[3]	*przegląda i analizuje zapisy z audytu systemu informacyjnego pod kątem wskazań do określonych przez organizację niewłaściwych lub nietypowych czynności z określoną przez organizację częstotliwością;*

AU-6	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE**		
	AU-6(b)	**AU-6(b)[1]**	*określa personel lub role, którym mają być zgłaszane ustalenia wynikające z przeglądów i analizy zapisów z systemu audytu informacyjnego; oraz*
		AU-6(b)[2]	*raportuje ustalenia personelowi lub rolom zdefiniowanym przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące przeglądu audytu, analiza i raportowanie; sprawozdania z wyników audytu; zapisy działań podjętych w odpowiedzi na przeglądy/analizy dokumentacji audytowej; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się przeglądem, analizą i raportowaniem audytów; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

AU-6(1)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *INTEGRACJA PROCESU***		
	CEL OCENY: *Określić, czy organizacja:*		
	AU-6(1)[1]	*stosuje zautomatyzowane mechanizmy integracji:*	
		AU-6(1)[1][a]	*przeglądu audytu;*
		AU-6(1)[1][b]	*analizy;*
		AU-6(1)[1][c]	*procesów raportowania;*
	AU-6(1)[2]	*wykorzystuje zintegrowane procesy przeglądu, analizy i raportowania audytów w celu wsparcia procesów organizacyjnych:*	
		AU-6(1)[2][a]	*dochodzenia w sprawie podejrzanych działań; oraz*
		AU-6(1)[2][b]	*reakcji na podejrzane działania.*

AU-6(1)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *INTEGRACJA PROCESU***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące przeglądu audytu, analiza i raportowanie; procedury dotyczące dochodzenia i reagowania na podejrzane działania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się przeglądem, analizą i raportowaniem audytów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy integrujące procesy przeglądu, analizy i raportowania audytów].

AU-6(2)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *AUTOMATYCZNE ALARMY BEZPIECZEŃSTWA***
[Włączone do: SI-4].	

AU-6(3)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *KORELACJA ZBIORÓW AUDYTU***
	CEL OCENY: *Ustalenie, czy organizacja analizuje i koreluje zapisy z audytów w różnych repozytoriach, aby uzyskać świadomość sytuacyjną w całej organizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące przeglądu audytu, analiza i raportowanie; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego w różnych repozytoriach; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się przeglądem, analizą i raportowaniem audytów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające analizę i korelację zapisów z audytu].

AU-6(4)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *CENTRALNE PRZEGLĄDANIE I ANALIZY***
	CEL OCENY: *Ustalenie, czy system informacyjny zapewnia możliwość centralnego przeglądu i analizy zapisów audytowych z wielu komponentów systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące przeglądu audytu, analiza i raportowanie; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; plan bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się przeglądem, analizą i raportowaniem audytów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zdolność systemu informacyjnego do scentralizowanego przeglądu i analizy dokumentacji audytowej].

AU-6(5)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *MOŻLIWOŚCI INTEGRACJI / SKANOWANIA I MONITOROWANIA***		
	CEL OCENY: *Określić, czy organizacja:*		
	AU-6(5)[1]	*definiuje dane/informację, które mają być zbierane z innych źródeł;*	
	AU-6(5)[2]	*wybiera źródła danych/systemów informacyjnych, które mają być analizowane i zintegrowane z analizą zapisów z audytu z jednego lub kilku z poniższych źródeł:*	
		AU-6(5)[2][a]	*informacje o skanowaniu podatności na zagrożenia;*
		AU-6(5)[2][b]	*dane dotyczące wydajności;*
		AU-6(5)[2][c]	*informacje dotyczące monitorowania systemu informacyjnego; i/lub*
		AU-6(5)[2][d]	*dane/informacje określone przez organizację, zebrane z innych źródeł; oraz*

AU-6(5)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *MOŻLIWOŚCI INTEGRACJI / SKANOWANIA I MONITOROWANIA***	
	AU-6(5)[3]	*integruje analizę zapisów z audytu z analizą wybranych danych/systemów informacyjnych w celu dalszego zwiększenia Zdolności do identyfikacji niewłaściwych lub nietypowych działań.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące przeglądu audytu, analiza i raportowanie; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zintegrowana analiza zapisów audytów, informacje o skanowaniu luk, dane o wydajności, informacje o monitorowaniu sieci i związana z tym dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się przeglądem, analizą i raportowaniem audytów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementujące możliwość integracji analizy zapisów audytowych z analizą danych/źródeł informacji].	

AU-6(6)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *KORELACJA AUDYTU Z MONITOROWANIEM FIZYCZNYM***
	CEL OCENY: *Ustalić, czy organizacja koreluje informacje z zapisów z audytu z informacjami uzyskanymi z monitorowania dostępu fizycznego w celu zwiększenia Zdolności do identyfikacji podejrzanych, niewłaściwych, nietypowych lub złośliwych działań.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące przeglądu audytu, analiza i raportowanie; procedury dotyczące monitorowania dostępu fizycznego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentację zawierającą udokumentowanie skorelowanych informacji uzyskanych z zapisów z audytu i zapisów dotyczących monitorowania dostępu fizycznego; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry].

AU-6(6)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *KORELACJA AUDYTU Z MONITOROWANIEM FIZYCZNYM***
	Wywiad: [*wybierz spośród:* Personel organizacji zajmujący się przeglądem, analizą i raportowaniem audytów; personel organizacji odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające możliwość korelacji informacji z zapisów audytowych z informacjami z monitorowania dostępu fizycznego].

AU-6(7)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *DOPUSZCZALNE DZIAŁANIA***	
	CEL OCENY: *Ustalić, czy organizacja określa dozwolone działania dla każdego z poniższych działań związanych z przeglądem, analizą i raportowaniem informacji dotyczących audytu:*	
	AU-6(7)[1]	*procesu systemu informacyjnego;*
	AU-6(7)[2]	*roli; i/lub*
	AU-6(7)[3]	*użytkownika.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące dozwolonego działania użytkownika i/lub roli, wynikające z przeglądu audytowego, analizy i raportowania; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się przeglądem, analizą i raportowaniem audytów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające dopuszczalne działania w zakresie przeglądu, analizy i raportowania informacji z audytu].	

AU-6(8)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *PEŁNA ANALIZA TEKSTU UPRZYWILEJOWANYCH POLECEŃ***	
	CEL OCENY: *Ustalić, czy organizacja wykonuje pełną analizę tekstową audytowanych komend uprzywilejowanych:*	
	AU-6(8)[1]	*fizycznie odrębnego składnika lub podsystemu systemu informacyjnego; lub*
	AU-6(8)[2]	*innego systemu informacyjnego, który jest dedykowany do tej analizy.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące przeglądu audytu, analiza i raportowanie; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia i techniki analizy tekstu; dokumentacja analizy tekstu kontrolowanych poleceń uprzywilejowanych ; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się przeglądem, analizą i raportowaniem audytów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wykorzystujące zdolność do wykonywania pełno tekstowej analizy audytowanych uprzywilejowanych poleceń].	

AU-6(9)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *KORELACJA Z INFORMACJAMI UZYSKANYMI ZE ŹRÓDEŁ NIETECHNICZNYCH***
	CEL OCENY: *Ustalenie, czy organizacja koreluje informacje ze źródeł nietechnicznych z informacjami o audycie, w celu zwiększenia świadomości sytuacyjnej w całej organizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące przeglądu audytu, analiza i raportowanie; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja przedstawiająca wykaz skorelowanych informacji uzyskanych z zapisów z audytu oraz ze zdefiniowanych przez organizację źródeł nietechnicznych; wykaz rodzajów informacji ze źródeł nietechnicznych umożliwiających korelację z informacjami z audytu; inne odpowiednie dokumenty lub rejestry].

AU-6(9)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *KORELACJA Z INFORMACJAMI UZYSKANYMI ZE ŹRÓDEŁ NIETECHNICZNYCH***
	Wywiad: [*wybierz spośród:* Personel organizacji zajmujący się przeglądem, analizą i raportowaniem audytów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wykorzystujące zdolność do korelowania informacji ze źródeł nietechnicznych].

AU-6(10)	**PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | *KORYGOWANIE POZIOMU AUDYTU***	
	CEL OCENY: *Ustalić, czy organizacja dostosowuje (koryguje) poziom przeglądu audytu, analizy i raportowania w ramach systemu informacyjnego, gdy następuje zmiana poziomu ryzyka na podstawie:*	
	AU-6(10)[1]	*informacji uzyskanych od organów ścigania;*
	AU-6(10)[2]	*informacji wywiadowczych; i/lub*
	AU-6(10)[3]	*innych wiarygodnych źródeł informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące przeglądu audytu, analiza i raportowanie; szacowanie ryzyka organizacyjnego; ocena środków bezpieczeństwa; ocena podatności; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się przeglądem, analizą i raportowaniem audytów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające przegląd, analizę i raportowanie informacji z audytu].	

AU-7	**REDUKCJA TREŚCI ZAPISÓW AUDYTU I GENEROWANIE RAPORTÓW**	
	CEL OCENY: *Ustalić, czy system informacyjny zapewnia ograniczanie zawartości zapisów audytu i generowania raportów, które wspomagają:*	
	AU-7(a)	**AU-7(a)[1]** *audyt na żądanie;*

AU-7	**REDUKCJA TREŚCI ZAPISÓW AUDYTU I GENEROWANIE RAPORTÓW**		
		AU-7(a)[2]	*analizę;*
		AU-7(a)[3]	*wymogi w zakresie sprawozdawczości;*
		AU-7(a)[4]	*badania po fakcie zdarzeń naruszających bezpieczeństwo; oraz*
	AU-7(b)	*nie zmieniają oryginalnej treści, ani kolejności czasowej zapisów z audytu.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące redukcja treści zapisów audytu i generowanie raportów; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia służące do redukcji, przeglądu, analizy i sprawozdawczości audytu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ograniczanie zawartości zapisów audytów i tworzenie raportów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Redukcja zawartości zapisów audytów i zdolność generowania raportów].		

AU-7(1)	**REDUKCJA TREŚCI ZAPISÓW AUDYTU I GENEROWANIE RAPORTÓW | *AUTOMATYZACJA PROCESU***	
	CEL OCENY: *Określić, czy:*	
	AU-7(1)[1]	*organizacja określa pola audytowe w dokumentacji audytowej w celu przetworzenia dokumentacji audytowej dla zdarzeń będących przedmiotem zainteresowania; oraz*
	AU-7(1)[2]	*system informacyjny zapewnia możliwość przetwarzania zapisów z audytów dla interesujących nas zdarzeń w oparciu o zdefiniowane przez organizację pola audytu w zapisach z audytów.*

AU-7(1)	**REDUKCJA TREŚCI ZAPISÓW AUDYTU I GENEROWANIE RAPORTÓW | *AUTOMATYZACJA PROCESU***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące redukcja treści zapisów audytu i generowanie raportów; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia służące do redukcji, przeglądu, analizy i sprawozdawczości audytu; kryteria zapisów z audytu (pola) określające interesujące zdarzenia; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ograniczanie zawartości zapisów audytów i tworzenie raportów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Redukcja zawartości zapisów audytów i zdolność generowania raportów].

AU-7(2)	**REDUKCJA TREŚCI ZAPISÓW AUDYTU I GENEROWANIE RAPORTÓW | *AUTOMATYCZNE SORTOWANIE I WYSZUKIWANIE***	
	CEL OCENY: *Określić, czy:*	
	AU-7(2)[1]	*organizacja określa pola audytu w dokumentacji audytowej w celu posortowania i przeszukania dokumentacji audytowej pod kątem interesujących ją zdarzeń w oparciu o zawartość takich pól audytu; oraz*
	AU-7(2)[2]	*system informacyjny zapewnia możliwość sortowania i wyszukiwania zapisów audytów dla interesujących nas zdarzeń w oparciu o zawartość zdefiniowanych przez organizację pól audytowych w zapisach audytów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące redukcji treści zapisów audytu i generowanie raportów; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia służące do redukcji, przeglądu, analizy i sprawozdawczości audytu; kryteria zapisów z audytu (pola) określające interesujące zdarzenia; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AU-7(2)	**REDUKCJA TREŚCI ZAPISÓW AUDYTU I GENEROWANIE RAPORTÓW | *AUTOMATYCZNE SORTOWANIE I WYSZUKIWANIE***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za ograniczanie zawartości zapisów audytów i tworzenie raportów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Redukcja zawartości zapisów audytów i zdolność generowania raportów].

AU-8	**ZNACZNIKI CZASU**		
	CEL OCENY: *Określić, czy:*		
	AU-8(a)	*System informacyjny wykorzystuje wewnętrzne zegary systemowe do generowania znaczników czasu na potrzeby ewidencji rekordów audytu;*	
	AU-8(b)	**AU-8(b)[1]**	*system informacyjny rejestruje znaczniki czasu dla zapisów rekordów audytu, które mogą być mapowane do uniwersalnego czasu koordynowanego (UTC) lub uniwersalnego czasu Greenwich (GMT);*
		AU-8(b)[2]	*organizacja określa ziarnistość pomiaru czasu, który należy spełnić podczas rejestracji znaczników czasu dla zapisów rekordów audytowych; oraz*
		AU-8(b)[3]	*organizacja rejestruje znaczniki czasu dla zapisów rekordów audytu, które spełniają zdefiniowaną przez organizację ziarnistość pomiaru czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące generowania znacznika czasu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące generowanie znaczników czasu].		

AU-8(1)	**ZNACZNIKI CZASU | *SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA***		
	CEL OCENY: *Określić, czy:*		
	AU-8(1)(a)	**AU-8(1)(a)[1]**	*organizacja określa autoryzowane źródło czasu, z którym porównywane są wewnętrzne zegary systemu informacyjnego;*
		AU-8(1)(a)[2]	*organizacja określa częstotliwość porównywania zegarów wewnętrznego systemu informacyjnego z określonym przez organizację autoryzowanym źródłem czasu; oraz*
		AU-8(1)(a)[3]	*system informacyjny porównuje wewnętrzne zegary systemu informacyjnego ze zdefiniowanym przez organizację autoryzowanym źródłem czasu ze zdefiniowaną przez organizację częstotliwością; oraz*
	AU-8(1)(b)	**AU-8(1)(b)[1]**	*organizacja określa okres czasu, który po przekroczeniu różnicy czasu między wewnętrznymi zegarami systemowymi, a autoryzowanym źródłem czasu spowoduje zsynchronizowanie wewnętrznych zegarów systemowych z autoryzowanym źródłem czasu; oraz*
		AU-8(1)(b)[2]	*system informacyjny synchronizuje wewnętrzne zegary systemu informacyjnego z autoryzowanym źródłem czasu, gdy różnica czasu jest większa niż okres czasu określony przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące generowania znacznika czasu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące wewnętrzną synchronizację zegarów systemu informacyjnego].		

AU-8(2)	**ZNACZNIKI CZASU | *WTÓRNE ŹRÓDŁO CZASU ODNIESIENIA***
	CEL OCENY: *Ustalić, czy system informacyjny identyfikuje wtórne źródło czasu odniesienia, które znajduje się w innym regionie geograficznym niż główne autoryzowane źródło czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące generowania znacznika czasu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementujące w systemie informacyjnym wewnętrzny zegar stanowiący autoryzowane źródło czasu].

AU-9	**OCHRONA INFORMACJI AUDYTOWYCH**		
	CEL OCENY: *Określić, czy:*		
	AU-9[1]	*system informacyjny chroni informacje z audytu przed nieupoważnionym:*	
		AU-9[1][a]	*dostępem;*
		AU-9[1][b]	*modyfikacją;*
		AU-9[1][c]	*skasowaniem;*
	AU-9[2]	*system informacyjny chroni narzędzia audytu przed nieautoryzowanym:*	
		AU-9[2][a]	*dostępem;*
		AU-9[2][b]	*modyfikacją;*
		AU-9[2][c]	*skasowaniem.*

AU-9	**OCHRONA INFORMACJI AUDYTOWYCH**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; zasady I procedury kontroli dostępu; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja, zapisy z audytu systemu informacyjnego; narzędzia audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania ochrony informacji uzyskanych w wyniku audytu].

AU-9(1)	**OCHRONA INFORMACJI AUDYTOWYCH | *NOŚNIKI JEDNOKROTNEGO ZAPISU***
	CEL OCENY: *Ustalić, czy system informacyjny zapisuje ścieżki audytu na wprowadzonym do użycia nośniku jednorazowego zapisu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; zasady I procedury kontroli dostępu; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu informacyjnego; ustawienia sprzętowe systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; nośniki danych systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Nośniki systemu informacyjnego przechowujące ścieżki audytu].

AU-9(2)	**OCHRONA INFORMACJI AUDYTOWYCH | *BACKUP AUDYTU W ODSEPAROWANYM FIZYCZNIE SYSTEMIE / KOMPONENCIE***	
	CEL OCENY: *Określić, czy:*	
	AU-9(2)[1]	*organizacja określa częstotliwość tworzenia kopii zapasowych zapisów z audytu w fizycznie odseparowanym systemie lub komponencie systemu, od systemu lub komponentu będącego przedmiotem audytu; oraz*
	AU-9(2)[2]	*system informacyjny tworzy kopię zapasową zapisów z audytu z częstotliwością określoną przez organizację, na fizycznie odseparowanym systemie lub komponencie systemu od systemu lub komponentu będącego przedmiotem audytu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja, system lub nośnik przechowujący kopie zapasowe zapisów z audytu systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące tworzenie kopii zapasowych dokumentacji audytowej].	

AU-9(3)	**OCHRONA INFORMACJI AUDYTOWYCH | *OCHRONA KRYPTOGRAFICZNA***	
	CEL OCENY: *Ustalić, czy system informacyjny:*	
	AU-9(3)[1]	*wykorzystuje mechanizmy kryptograficzne do ochrony integralności informacji z audytu; oraz*
	AU-9(3)[2]	*wykorzystuje mechanizmy kryptograficzne do ochrony integralności narzędzi audytu.*

AU-9(3)	**OCHRONA INFORMACJI AUDYTOWYCH | *OCHRONA KRYPTOGRAFICZNA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; zasady i procedury kontroli dostępu; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu informacyjnego; ustawienia sprzętowe systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja, rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficzne zapewniające integralność informacji i narzędzi audytorskich].

AU-9(4)	**OCHRONA INFORMACJI AUDYTOWYCH | *DOSTĘP DO PODZBIORU UPRAWNIONYCH UŻYTKOWNIKÓW***	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-9(4)[1]	*definiuje podzbiór uprzywilejowanych użytkowników, którzy mają być upoważnieni do zarządzania funkcjami audytu; oraz*
	AU-9(4)[2]	*autoryzuje dostęp do zarządzania funkcjonalnością audytu tylko zdefiniowanemu przez organizację podzbiorowi uprzywilejowanych użytkowników.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; zasady i procedury kontroli dostępu; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja, generowana przez system lista uprzywilejowanych użytkowników z dostępem do zarządzania funkcjami audytu; uprawnienia dostępu; lista kontroli dostępu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zarządzania dostępem do funkcji audytu].	

AU-9(5)	**OCHRONA INFORMACJI AUDYTOWYCH | *PODWÓJNA AUTORYZACJA***	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-9(5)[1]	*określa informacje dotyczące audytu, dla których podwójna autoryzacja ma być egzekwowana;*
	AU-9(5)[2]	*definiuje jeden lub więcej z następujących rodzajów operacji dotyczących informacji o audycie, dla których podwójna autoryzacja ma być egzekwowana:*
	AU-9(5)[2][a]	*przemieszczanie; i/lub*
	AU-9(5)[2][b]	*usuwanie; oraz*
	AU-9(5)[3]	*egzekwuje podwójną autoryzację do przemieszczania i/lub usuwania zdefiniowanych przez organizację informacji o audycie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; zasady i procedury kontroli dostępu; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja, zezwolenia na dostęp; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania procedur egzekwowania podwójnej autoryzacji].	

AU-9(6)	**OCHRONA INFORMACJI AUDYTOWYCH | *DOSTĘP TYLKO DO ODCZYTU***	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-9(6)[1]	*definiuje podzbiór uprzywilejowanych użytkowników, którzy mają być upoważnieni do dostępu tylko do odczytu do informacji audytowych; oraz*

AU-9(6)	**OCHRONA INFORMACJI AUDYTOWYCH | *DOSTĘP TYLKO DO ODCZYTU***	
	AU-9(6)[2]	*zezwala na dostęp tylko do odczytu do informacji o audycie do zdefiniowanego przez organizację podzbioru uprzywilejowanych użytkowników.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; zasady i procedury kontroli dostępu; procedury dotyczące ochrony informacji audytowych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja, generowana przez system lista uprzywilejowanych użytkowników z dostępem tylko do odczytu do informacji z audytu; uprawnienia dostępu; lista kontroli dostępu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt i rozliczalność; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zarządzania dostępem do informacji z audytu].	

AU-10	**NIEZAPRZECZALNOŚĆ**	
	CEL OCENY: *Określić, czy:*	
	AU-10[1]	*organizacja określa działania, które mają być objęte niezaprzeczalnością; oraz*
	AU-10[2]	*system informacyjny chroni przed fałszywym zaprzeczeniem przez użytkownika (lub proces działający w jego imieniu), że wykonała ona określone organizacyjnie czynności, które mają być objęte niezaprzeczalnością.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące niezaprzeczalności; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AU-10	**NIEZAPRZECZALNOŚĆ**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające procedury niezaprzeczalności].

AU-10(1)	**NIEZAPRZECZALNOŚĆ | *POŁĄCZENIE TOŻSAMOŚCI***		
	CEL OCENY: *Określić, czy:*		
	AU-10(1)(a)	**AU-10(1)(a)[1]**	*organizacja określa siłę wiązania między tożsamością wytwórcy informacji, a informacją;*
		AU-10(1)(a)[2]	*system informacyjny wiąże tożsamość twórcy informacji z informacją, z określoną przez organizację siłą wiążącą; oraz*
	AU-10(1)(b)	*system informacyjny zapewnia upoważnionym użytkownikom środki umożliwiające określenie tożsamości autora informacji.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące niezaprzeczalności; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające procedury niezaprzeczalności].		

AU-10(2) NIEZAPRZECZALNOŚĆ | *POWIĄZANIE INFORMACJI Z TOŻSAMOŚCIĄ TWÓRCY*			
	CEL OCENY: *Określić, czy:*		
	AU-10(2)(a)	**AU-10(2)(a)[1]**	*organizacja definiuje częstotliwość potwierdzania powiązania tożsamości autora informacji z informacjami;*
		AU-10(2)(a)[2]	*system informacyjny zatwierdza powiązanie tożsamości twórcy informacji z informacją, z częstotliwością określoną przez organizację; oraz*
	AU-10(2)(b)	**AU-10(2)(b)[1]**	*organizacja definiuje działania, które należy wykonać w przypadku sprawdzania poprawności powiązania; oraz*
		AU-10(2)(b)[2]	*system informacyjny wykonuje czynności zdefiniowane przez organizację w przypadku błędu sprawdzania poprawności powiązania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące niezaprzeczalności; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry weryfikacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające procedury niezaprzeczalności].		

AU-10(3) NIEZAPRZECZALNOŚĆ | *ŁAŃCUCH NADZORU*		
	CEL OCENY: *Ustalić, czy system informacyjny:*	
	AU-10(3)[1]	*utrzymuje tożsamość recenzenta / wydawcy w ramach ustalonego łańcucha dowodowego dla wszystkich sprawdzanych informacji;*

AU-10(3) NIEZAPRZECZALNOŚĆ | *ŁAŃCUCH NADZORU*		
	AU-10(3)[2]	*utrzymuje tożsamość recenzenta / wydawcy zlecającego w ramach ustalonego łańcucha dowodowego w odniesieniu do wszystkich udostępnionych informacji;*
	AU-10(3)[3]	*utrzymuje poświadczenia recenzenta / wydawcy w ramach ustalonego łańcucha dowodowego w odniesieniu do wszystkich kontrolowanych informacji; oraz*
	AU-10(3)[4]	*utrzymuje poświadczenia recenzenta / wydawcy w ramach ustalonego łańcucha dowodowego dla wszystkich udostępnianych informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące niezaprzeczalności; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry przeglądów informacji i komunikatów informacyjnych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające procedury niezaprzeczalności].	

AU-10(4) NIEZAPRZECZALNOŚĆ | *POTWIERDZANIE TOŻSAMOŚCI PRZEGLĄDAJĄCEGO INFORMACJE*			
	CEL OCENY: *Określić, czy:*		
	AU-10(4)(a)	**AU-10(4)(a)[1]**	*organizacja określa domeny bezpieczeństwa, dla których powiązanie tożsamości recenzenta informacji z informacją ma być zatwierdzone w punktach transferu lub udostępnienia, przed udostępnieniem/przekazaniem między tymi domenami;*

AU-10(4)	**NIEZAPRZECZALNOŚĆ | *POTWIERDZANIE TOŻSAMOŚCI PRZEGLĄDAJĄCEGO INFORMACJE***		
		AU-10(4)(a)[2]	*system informacyjny zatwierdza powiązanie tożsamości recenzenta informacji z informacjami w punktach transferu lub wydania, przed wydaniem/przekazaniem informacji pomiędzy zdefiniowanymi przez organizację domenami bezpieczeństwa;*
	AU-10(4)(b)	**AU-10(4)(b)[1]**	*organizacja określa działania, które należy wykonać w przypadku błędu sprawdzania poprawności; oraz*
		AU-10(4)(b)[2]	*system informacyjny wykonuje czynności zdefiniowane przez organizację w przypadku błędu sprawdzania poprawności.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące niezaprzeczalności; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry weryfikacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające procedury niezaprzeczalności].		

AU-10(5)	**NIEZAPRZECZALNOŚĆ | *PODPISY CYFROWE***
[Włączone do: SI-7].	

AU-11	**RETENCJA ZAPISÓW AUDYTU**	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-11[1]	*określa okres przechowywania dokumentacji audytowej, który jest zgodny z przepisami dotyczącymi przechowywania dokumentacji;*

AU-11	**RETENCJA ZAPISÓW AUDYTU**		
	AU-11[2]	*przechowuje dokumentację z audytu przez określony przez organizację okres czasu, zgodny z przepisami polityki przechowywania dokumentacji w celu:*	
		AU-11[2][a]	*zapewnienia wsparcia procesów dochodzeniowych dotyczących incydentów bezpieczeństwa; oraz*
		AU-11[2][b]	*spełnienia wymagań prawnych i organizacyjnych dotyczących przechowywania informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; polityka i procedury przechowywania dokumentacji audytowej; plan bezpieczeństwa; określony przez organizację okres przechowywania zapisów z audytu; archiwum zapisów z audytu; dzienniki audytu; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za przechowywanie dokumentacji audytowej; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci].		

AU-11(1)	**RETENCJA ZAPISÓW AUDYTU | *DŁUGOTERMINOWA ZDOLNOŚĆ DO ODZYSKU***	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-11(1)[1]	*określa środki, które należy zastosować w celu zapewnienia możliwości uzyskania długoterminowych zapisów z audytu generowanych przez system informacyjny; oraz*
	AU-11(1)[2]	*stosuje określone przez organizację środki, aby zapewnić możliwość uzyskania długoterminowych zapisów z audytu generowanych przez system informacyjny.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; polityka i procedury przechowywania dokumentacji audytowej; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; archiwum zapisów z audytów; dzienniki audytów; zapisy z audytów; inne odpowiednie dokumenty lub rejestry].	

AU-11(1)	**RETENCJA ZAPISÓW AUDYTU | *DŁUGOTERMINOWA ZDOLNOŚĆ DO ODZYSKU***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za przechowywanie dokumentacji audytowej; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy umożliwiające retencję rekordów z audytu].

AU-12	**TWORZENIE ZAPISÓW AUDYTU**		
	CEL OCENY: *Określić, czy:*		
	AU-12(a)	**AU-12(a)[1]**	*organizacja określa elementy systemu informacyjnego, które mają zapewnić możliwość generowania zapisów audytowych dla zdarzeń podlegających audytowi określonych w zabezpieczeniu AU-2a;*
		AU-12(a)[2]	*system informacyjny zapewnia zdolność do generowania zapisów audytowych dla podlegających audytowi zdarzeń zdefiniowanych w zabezpieczeniu AU-2a, przy zdefiniowanych przez organizację komponentach systemu informacyjnego;*
	AU-12(b)	**AU-12(b)[1]**	*organizacja określa personel lub role dopuszczone do wyboru, które zdarzenia podlegające audytowi mają być kontrolowane przez określone części składowe systemu informacyjnego;*
		AU-12(b)[2]	*system informacyjny umożliwia zdefiniowanemu przez organizację personelowi lub rolom dokonanie wyboru, które ze zdarzeń podlegających audytowi mają być poddane audytowi przez określone części składowe systemu; oraz*
	AU-12(c)	*system informacyjny generuje zapisy z audytu dla zdarzeń zdefiniowanych w zabezpieczeniu AU-2d o treści zdefiniowanej w zabezpieczeniu AU-3.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące generowania zapisów z audytu; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista zdarzeń podlegających audytowi; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].		

AU-12	**TWORZENIE ZAPISÓW AUDYTU**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za tworzenie dokumentacji audytowej; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy generujące zapisy z przeprowadzanych audytów].

AU-12(1)	**TWORZENIE ZAPISÓW AUDYTU | *OGÓLNOSYSTEMOWE / SKORELOWANE W CZASIE ŚCIEŻKI AUDYTU***	
	CEL OCENY: *Określić, czy:*	
	AU-12(1)[1]	*organizacja określa komponenty systemu informacyjnego, z których mają być tworzone zapisy audytowe w ramach ogólnosystemowej (logicznej lub fizycznej) ścieżki audytu;*
	AU-12(1)[2]	*organizacja określa poziom tolerancji dla relacji pomiędzy znacznikami czasu poszczególnych zapisów w ścieżce audytu; oraz*
	AU-12(1)[3]	*system informacyjny kompiluje zapisy audytowe ze zdefiniowanych w organizacji komponentów systemu informacyjnego w ogólnosystemową (logiczną lub fizyczną) ścieżkę audytu, która jest związana z określonym w organizacji poziomem tolerancji dla relacji pomiędzy znacznikami czasu poszczególnych zapisów w ścieżce audytu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące generowania zapisów z audytu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; ogólnosystemowa ścieżka audytu (logiczna lub fizyczna); rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za tworzenie dokumentacji audytowej; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy generujące zapisy z przeprowadzanych audytów].	

AU-12(2) TWORZENIE ZAPISÓW AUDYTU | *UJEDNOLICONE FORMATY*	
	CEL OCENY: *Ustalić, czy system informacyjny tworzy ogólnosystemową (logiczną lub fizyczną) ścieżkę audytu składającą się z zapisów audytowych w znormalizowanym formacie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące generowania zapisów z audytu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; ogólnosystemowa ścieżka audytu (logiczna lub fizyczna); rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za tworzenie dokumentacji audytowej; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy generujące zapisy z przeprowadzanych audytów].

AU-12(3) TWORZENIE ZAPISÓW AUDYTU | *ZMIANY DOKONYWANE PRZEZ UPRAWNIONE OSOBY*		
	CEL OCENY: *Określić, czy:*	
	AU-12(3)[1]	*organizacja określa elementy systemu informacyjnego, w oparciu o które ma być przeprowadzany audyt;*
	AU-12(3)[2]	*organizacja określa osoby lub role upoważnione do zmiany audytu, który ma być przeprowadzony na zdefiniowanych przez organizację komponentach systemu informacyjnego;*
	AU-12(3)[3]	*organizacja określa progi czasowe, w ramach których zdefiniowane przez organizację osoby lub role mogą zmienić audyt, który ma być przeprowadzony na zdefiniowanych przez organizację komponentach systemu informacyjnego;*
	AU-12(3)[4]	*organizacja określa możliwe do wyboru kryteria zdarzeń, które umożliwiają właściwym osobom lub rolom, zdefiniowanym przez organizację, zmianę audytu, który ma być przeprowadzony na zdefiniowanych przez organizację komponentach systemu informacyjnego; oraz*

AU-12(3)	**TWORZENIE ZAPISÓW AUDYTU | *ZMIANY DOKONYWANE PRZEZ UPRAWNIONE OSOBY***	
	AU-12(3)[5]	*system informacyjny zapewnia określonym przez organizację osobom lub rolom możliwość zmiany audytu, który ma być przeprowadzony na określonych przez organizację komponentach systemu informacyjnego, w oparciu o określone przez organizację kryteria wyboru zdarzeń, w ramach określonych przez organizację progów czasowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące generowania zapisów z audytu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; generowana przez system lista osób lub ról upoważnionych do zmiany audytu, który ma być przeprowadzony; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za tworzenie dokumentacji audytowej; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy generujące zapisy z przeprowadzanych audytów].	

AU-13	**MONITOROWANIE UJAWNIANIA INFORMACJI**	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-13[1]	*definiuje informacje o otwartym kodzie źródłowym (typu Open Source) i/lub witryny informacyjne, które mają być monitorowane pod kątem dowodów nieuprawnionego ujawnienia informacji organizacyjnych;*
	AU-13[2]	*definiuje częstotliwość monitorowania informacji o otwartym kodzie źródłowym i/lub witryn informacyjnych zdefiniowanych przez organizację w celu uzyskania dowodów nieautoryzowanego ujawnienia informacji organizacyjnych; oraz*
	AU-13[3]	*monitoruje zdefiniowane przez organizację informacje o otwartym kodzie źródłowym i/lub witryny informacyjne pod kątem dowodów nieautoryzowanego ujawnienia informacji organizacyjnych z określoną przez organizację częstotliwością.*

AU-13	**MONITOROWANIE UJAWNIANIA INFORMACJI**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące monitorowania ujawniania informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z monitoringu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za monitorowanie informacji z kodem źródłowym i/lub witryn informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania monitoringu w zakresie ujawniania informacji].

AU-13(1)	**MONITOROWANIE UJAWNIANIA INFORMACJI | *WYKORZYSTANIE ZAUTOMATYZOWANYCH NARZĘDZI***
	CEL OCENY: *Ustalenie, czy organizacja stosuje zautomatyzowane mechanizmy w celu ustalenia, czy informacje organizacyjne zostały ujawnione w sposób nieupoważniony.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące monitorowania ujawniania informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zautomatyzowane narzędzia monitorowania; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za monitorowanie ujawnianych informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania monitoringu w zakresie ujawniania informacji].

AU-13(2)	**MONITOROWANIE UJAWNIANIA INFORMACJI | *PRZEGLĄD MONITOROWANYCH STRON***	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-13(2)[1]	*określa częstotliwość przeglądu monitorowanych witryn informacyjnych z otwartym kodem źródłowym (typu open source); oraz*
	AU-13(2)[2]	*dokonuje przeglądu stron z informacjami typu open source, które są monitorowane z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące monitorowania ujawniania informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; przeglądu monitorowanych witryn informacyjnych z otwartym kodem źródłowym; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za monitorowanie stron internetowych zawierających informacje typu open source; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania monitoringu w zakresie ujawniania informacji].	

AU-14	**AUDYT SESJI**	
	CEL OCENY: *Ustalić, czy system informacyjny daje uprawnionym użytkownikom możliwość wyboru sesji użytkownika do:*	
	AU-14[1]	*przechwycenia/rejestracji; i/lub*
	AU-14[2]	*nagrywania lub przeglądania / utrwalania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące audytu sesji użytkownika; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

AU-14	**AUDYT SESJI**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementujące możliwości audytu sesji użytkownika].

AU-14(1)	**AUDYT SESJI | *URUCHAMIANIE SYSTEMU***
	CEL OCENY: *Ustalić, czy system informacyjny inicjuje audyty sesji przy uruchamianiu systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące audytu sesji użytkownika; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementujące możliwości audytu sesji użytkownika].

AU-14(2)	**AUDYT SESJI | *PRZECHWYTY / NAGRYWANIE I ZAWARTOŚĆ DZIENNIKÓW LOGOWANIA***	
	CEL OCENY: *Ustalić, czy system informacyjny zapewnia uprawnionym użytkownikom:*	
	AU-14(2)[1]	*przechwytywanie/nagrywanie treści związanych z sesją użytkownika; oraz*
	AU-14(2)[2]	*zawartość dziennika związanego z sesją użytkownika.*

AU-14(2)	**AUDYT SESJI | *PRZECHWYTY / NAGRYWANIE I ZAWARTOŚĆ DZIENNIKÓW LOGOWANIA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące audytu sesji użytkownika; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementujące możliwości audytu sesji użytkownika].

AU-14(3)	**AUDYT SESJI | *ZDALNE WYŚWIETLANIE / ODSŁUCHIWANIE***
	CEL OCENY: *Ustalić, czy system informacyjny umożliwia uprawnionym użytkownikom zdalne przeglądanie / odsłuchiwanie w czasie rzeczywistym wszystkich treści związanych z ustanowioną sesją użytkownika.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące audytu sesji użytkownika; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementujące możliwości audytu sesji użytkownika].

AU-15	**ZDOLNOŚĆ DO ALTERNATYWNEGO AUDYTU**	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-15[1]	*definiuje funkcję alternatywnego audytu, którą należy zapewnić w przypadku awarii podstawowej funkcji audytu; oraz*
	AU-15[2]	*zapewnia funkcję alternatywnego audytu w przypadku awarii podstawowej jednostki audytu, która zapewnia zdefiniowaną przez organizację alternatywną funkcję audytu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące Zdolności do alternatywnego audytu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy testowe dla alternatywnych możliwości audytu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zapewnienie alternatywnych Zdolności audytowych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające alternatywną zdolność audytu].	

AU-16	**AUDYT MIĘDZYORGANIZACYJNY**	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-16[1]	*definiuje informacje o audycie, które mają być koordynowane pomiędzy zewnętrznymi organizacjami, gdy informacje o audycie są przekazywane poza granice organizacji;*
	AU-16[2]	*definiuje metody koordynacji zdefiniowanych przez organizację informacji o audycie pomiędzy zewnętrznymi organizacjami, gdy informacje o audycie są przekazywane poza granice organizacyjne; oraz*
	AU-16[3]	*stosuje zdefiniowane przez organizację metody koordynacji zdefiniowanych przez organizację informacji o audycie wśród organizacji zewnętrznych, gdy informacje o audycie są przekazywane poza granice organizacji.*

AU-16	**AUDYT MIĘDZYORGANIZACYJNY**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące metod przekazywania informacji o audycie organizacjom zewnętrznym; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; metody koordynacji informacji o audycie wśród organizacji zewnętrznych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za koordynację informacji o audycie pomiędzy organizacjami zewnętrznymi; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test:** [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania audytu międzyorganizacyjnego (jeśli dotyczy)].

AU-16(1)	**AUDYT MIĘDZYORGANIZACYJNY | *OCHRONA TOŻSAMOŚCI***
	CEL OCENY: *Ustalenie, czy organizacja wymaga zachowania tożsamości osób w ścieżkach audytu między organizacjami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące międzyorganizacyjnych ścieżek audytu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za audyt międzyorganizacyjny; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test:** [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania audytu międzyorganizacyjnego (jeśli dotyczy)].

AU-16(2)	**AUDYT MIĘDZYORGANIZACYJNY | *UDOSTĘPNIANIE INFORMACJI AUDYTOWYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	AU-16(2)[1]	*definiuje organizacje, którym należy udostępniać międzyorganizacyjne informacje o audycie;*
	AU-16(2)[2]	*określa porozumienia dotyczące wymiany zapisów audytu między organizacjami, które mają być wykorzystywane przy dostarczaniu informacji dotyczących audytu międzyorganizacyjnego do określonych organizacji; oraz*
	AU-16(2)[3]	*dostarcza informacji o audycie międzyorganizacyjnym do określonych organizacji w oparciu o zdefiniowane przez organizację umowy o współpracy międzyorganizacyjnej.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka audytu i rozliczalności; procedury dotyczące międzyorganizacyjnej wymiany informacji dotyczących audytu; porozumienia między organizacjami; porozumienia o wymianie danych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za udostępnianie międzyorganizacyjnych informacji dotyczących audytu; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

KATEGORIA CA - OCENA BEZPIECZEŃSTWA I AUTORYZACJA

CA-1	**POLITYKA I PROCEDURY OCENY BEZPIECZEŃSTWA I AUTORYZACJI**			
	CEL OCENY: *Określić, czy organizacja:*			
	CA-1(a)(1)	**CA-1(a)(1)[1]**	*opracowuje i dokumentuje zasady oceny bezpieczeństwa i autoryzacji, które dotyczą:*	
			CA-1(a)(1)[1][a]	*celu;*
			CA-1(a)(1)[1][b]	*zakresu stosowania;*
			CA-1(a)(1)[1][c]	*ról;*
			CA-1(a)(1)[1][d]	*odpowiedzialności;*
			CA-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			CA-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			CA-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		CA-1(a)(1)[2]	*określa personel lub role, którym ma być rozpowszechniana polityka oceny bezpieczeństwa i autoryzacji;*	
		CA-1(a)(1)[3]	*rozpowszechnia politykę oceny bezpieczeństwa i autoryzacji wśród personelu lub ról zdefiniowanych przez organizację;*	
	CA-1(a)(2)	**CA-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrożenie polityki oceny bezpieczeństwa i autoryzacji oraz związanych z nią kontroli oceny i autoryzacji;*	
		CA-1(a)(2)[2]	*określa personel lub role, którym procedury mają być rozpowszechniane;*	
		CA-1(a)(2)[3]	*rozpowszechnia procedury wśród personelu lub ról zdefiniowanych przez organizację;*	
	CA-1(b)(1)	**CA-1(b)(1)[1]**	*definiuje częstotliwość przeglądów i aktualizacji aktualnej polityki oceny bezpieczeństwa i autoryzacji;*	

CA-1	**POLITYKA I PROCEDURY OCENY BEZPIECZEŃSTWA I AUTORYZACJI**		
		CA-1(b)(1)[2]	*dokonuje oceny i aktualizacji aktualnej polityki oceny bezpieczeństwa i autoryzacji z częstotliwością określoną przez organizację;*
	CA-1(b)(2)	**CA-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji bieżących procedur oceny bezpieczeństwa i autoryzacji; oraz*
		CA-1(b)(2)[2]	*opiniuje i aktualizuje bieżące procedury oceny bezpieczeństwa i autoryzacji z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury oceny bezpieczeństwa i autoryzacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ocenę bezpieczeństwa i autoryzację; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

CA-2	**OCENA BEZPIECZEŃSTWA**			
	CEL OCENY: *Określić, czy organizacja:*			
	CA-2(a)	*opracowuje plan oceny bezpieczeństwa, który opisuje zakres oceny, w tym:*		
		CA-2(a)(1)	*środki bezpieczeństwa (zabezpieczenia) i ulepszenia zabezpieczeń podlegające oszacowaniu;*	
		CA-2(a)(2)	*procedury oceny bezpieczeństwa stosowane w celu ustalenia skuteczności zabezpieczeń;*	
		CA-2(a)(3)	**CA-2(a)(3)[1]**	*środowisko oceniające;*
			CA-2(a)(3)[2]	*zespół oceniający;*
			CA-2(a)(3)[3]	*rola i obowiązki w zakresie oceny;*
	CA-2(b)	**CA-2(b)[1]**	*określa częstotliwość oceny środków bezpieczeństwa w systemie informacyjnymi jego środowisku działania;*	

CA-2	**OCENA BEZPIECZEŃSTWA**		
		CA-2(b)[2]	*ocenia środki bezpieczeństwa w zakresie ochrony w systemie informacyjnym z częstotliwością określoną przez organizację w celu określenia zakresu, w jakim zabezpieczenia są wdrażane prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w odniesieniu do spełniania ustalonych wymogów bezpieczeństwa;*
	CA-2(c)	*sporządza sprawozdanie z oceny bezpieczeństwa, które dokumentuje wyniki tej oceny;*	
	CA-2(d)	**CA-2(d)[1]**	*określa osoby lub role, którym mają zostać przedstawione wyniki oceny środków bezpieczeństwa; oraz*
		CA-2(d)[2]	*dostarcza wyniki oceny środków bezpieczeństwa określonym osobom lub rolom w organizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Procedury dotycząca oceny bezpieczeństwa i autoryzacji; procedury dotyczące planowania oceny bezpieczeństwa; procedury dotyczące oceny bezpieczeństwa; plan oceny bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ocenę bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające ocenę bezpieczeństwa, opracowanie planu oceny bezpieczeństwa i/lub sprawozdawczości w zakresie oceny bezpieczeństwa].		

CA-2(1)	**OCENA BEZPIECZEŃSTWA | *NIEZALEŻNI AUDYTORZY***	
	CEL OCENY: *Określić, czy organizacja:*	
	CA-2(1)[1]	*określa poziom niezależności, jaki ma być stosowany do przeprowadzania ocen środków bezpieczeństwa; oraz*
	CA-2(1)[2]	*zatrudnia oceniających lub zespoły oceniające o określonym przez organizację poziomie niezależności do przeprowadzania oceny środków bezpieczeństwa.*

CA-2(1)	**OCENA BEZPIECZEŃSTWA | *NIEZALEŻNI AUDYTORZY***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady oceny bezpieczeństwa i autoryzacji; procedury dotyczące oceny bezpieczeństwa; pakiet autoryzacji bezpieczeństwa (w tym plan bezpieczeństwa, plan oceny bezpieczeństwa, raport z oceny bezpieczeństwa, plan i etapy działania, oświadczenie o autoryzacji); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ocenę bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CA-2(2)	**OCENA BEZPIECZEŃSTWA | *OCENY SPECJALISTYCZNE***		
	CEL OCENY: *Określić, czy organizacja:*		
	CA-2(2)[1]	*wybiera jedną lub więcej z poniższych form specjalistycznej oceny bezpieczeństwa, która ma być włączona do oceny środków bezpieczeństwa:*	
		CA-2(2)[1][a]	*dogłębne monitorowanie;*
		CA-2(2)[1][b]	*skanowanie podatności;*
		CA-2(2)[1][c]	*testowanie złośliwych użytkowników;*
		CA-2(2)[1][d]	*ocenianie zagrożenia wewnętrznego;*
		CA-2(2)[1][e]	*testowanie wydajności / obciążenia; i/lub*
		CA-2(2)[1][f]	*inne formy organizacyjnie definiowanej specjalistycznej oceny bezpieczeństwa;*
	CA-2(2)[2]	*określa częstotliwość przeprowadzania wybranej formy (form) specjalistycznej oceny bezpieczeństwa;*	
	CA-2(2)[3]	*określa, czy specjalistyczna ocena bezpieczeństwa zostanie ogłoszona czy niezapowiedziana; oraz*	
	CA-2(2)[4]	*przeprowadza zapowiedziane lub niezapowiedziane formy specjalistycznej oceny bezpieczeństwa z częstotliwością określoną przez organizację w ramach oceny środków bezpieczeństwa.*	

CA-2(2)	**OCENA BEZPIECZEŃSTWA | *OCENY SPECJALISTYCZNE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny bezpieczeństwa i autoryzacji; procedury dotyczące oceny bezpieczeństwa; plan bezpieczeństwa; plan oceny bezpieczeństwa; sprawozdanie z oceny bezpieczeństwa; dokumentacja oceny bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ocenę bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające ocenę środków bezpieczeństwa].

CA-2(3)	**OCENA BEZPIECZEŃSTWA | *ORGANIZACJE ZEWNĘTRZNE***	
	CEL OCENY: *Określić, czy organizacja:*	
	CA-2(3)[1]	*definiuje system informacyjny, dla którego wyniki oceny bezpieczeństwa przeprowadzonej przez zewnętrzną organizację mają być akceptowane;*
	CA-2(3)[2]	*wyznacza zewnętrzną organizację, która przeprowadza ocenę bezpieczeństwa systemu informacyjnego zdefiniowanego przez organizację;*
	CA-2(3)[3]	*definiuje wymagania, które mają być wypełniane przy ocenie bezpieczeństwa przeprowadzanej przez zewnętrzną organizację w zdefiniowanym przez organizację systemie informacyjnym; oraz*
	CA-2(3)[4]	*akceptuje wyniki oceny systemu informacyjnego zdefiniowanego przez organizację, wykonanej przez zewnętrzną organizację zdefiniowaną przez organizację, gdy ocena spełnia zdefiniowane przez organizację wymagania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny bezpieczeństwa i autoryzacji; procedury dotyczące oceny bezpieczeństwa; plan bezpieczeństwa; wymogi oceny bezpieczeństwa; plan oceny bezpieczeństwa; sprawozdanie z oceny bezpieczeństwa; dokumentacja oceny bezpieczeństwa; plan i etapy działania; inne odpowiednie dokumenty lub rejestry].	

CA-2(3)	**OCENA BEZPIECZEŃSTWA | *ORGANIZACJE ZEWNĘTRZNE***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za ocenę bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel wykonujący ocenę bezpieczeństwa dla określonej organizacji zewnętrznej].

CA-3	**POŁĄCZENIA MIĘDZYSYSTEMOWE**		
	CEL OCENY: *Określić, czy organizacja:*		
	CA-3(a)	*zezwala na połączenia z systemu informacyjnego do innych systemów informacyjnych z wykorzystaniem;*	
	CA-3(b)	*dokumentuje, dla każdego wzajemnego połączenia umów o bezpiecznym połączeniu systemów sieciowych:*	
		CA-3(b)[1]	*charakterystyki interfejsów;*
		CA-3(b)[2]	*wymogi bezpieczeństwa;*
		CA-3(b)[3]	*charakter przekazywanych informacji;*
	CA-3(c)	**CA-3(c)[1]**	*częstotliwość przeglądów i aktualizacji umów o bezpiecznym połączeniu systemów; oraz*
		CA-3(c)[2]	*opinie i aktualizacje umów o bezpiecznym połączeniu systemów z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące połączeń systemów informacyjnych; polityka ochrony systemu i komunikacji; umowy dotyczące bezpiecznego połączenia systemów sieciowych; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za opracowywanie, wdrażanie lub zatwierdzanie umów o wzajemnym połączeniu systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel zarządzający systemem(-ami), do którego(-ych) ma zastosowanie umowa o bezpiecznym połączeniu systemów sieciowych].		

CA-3(1)	**POŁĄCZENIA MIĘDZYSYSTEMOWE | *POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW KRAJOWYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	CA-3(1)[1]	*definiuje jawny, krajowy system bezpieczeństwa, którego bezpośrednie połączenie z siecią zewnętrzną ma być zakazane bez użycia zatwierdzonych brzegowych urządzeń zabezpieczających;*
	CA-3(1)[2]	*definiuje urządzenie do ochrony granic systemu, które ma być stosowane do bezpośredniego połączenia określonego przez organizację, nieoznaczonego klauzulą tajności krajowego systemu bezpieczeństwa z siecią zewnętrzną; oraz*
	CA-3(1)[3]	*zakazuje bezpośredniego podłączenia do sieci zewnętrznej, zdefiniowanego przez organizację, jawnego krajowego systemu bezpieczeństwa, bez użycia urządzenia do ochrony brzegowej zdefiniowanego przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące połączeń systemów informacyjnych; polityka ochrony systemu i komunikacji; umowy dotyczące bezpiecznego połączenia systemów sieciowych; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; raport z oceny bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie bezpośrednimi połączeniami z sieciami zewnętrznymi; administratorzy sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel zarządzający bezpośrednio podłączonymi sieciami zewnętrznymi]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające zarządzanie zewnętrznymi połączeniami sieciowymi].	

CA-3(2)	**POŁĄCZENIA MIĘDZYSYSTEMOWE | *POŁĄCZENIA NIEJAWNYCH SYSTEMÓW KRAJOWYCH*[4]**	
	CEL OCENY: *Określić, czy organizacja:*	
	CA-3(2)[1]	*określa urządzenia do ochrony granic systemu, które mają być wykorzystywane do bezpośredniego połączenia niejawnego systemu z siecią zewnętrzną; oraz*
	CA-3(2)[2]	*zakazuje bezpośredniego podłączenia niejawnego systemu do sieci zewnętrznej bez użycia urządzeń do ochrony granic określonych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące połączeń systemów informacyjnych; polityka ochrony systemu i komunikacji; umowy dotyczące bezpiecznego połączenia systemów sieciowych; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; raport z oceny bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie bezpośrednimi połączeniami z sieciami zewnętrznymi; administratorzy sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel zarządzający bezpośrednio podłączonymi sieciami zewnętrznymi]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające zarządzanie zewnętrznymi połączeniami sieciowymi].	

[4] Zgodnie z obowiązującymi przepisami połączenie systemu niejawnego z siecią zewnętrzną odbywa się po spełnieniu wymogów określonych w przepisach wydanych na podstawie ustawy o ochronie informacji niejawnych.

CA-3(3)	**POŁĄCZENIA MIĘDZYSYSTEMOWE | *POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW TRANSGRANICZNYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	CA-3(3)[1]	*definiuje jawny bezpieczny system transgraniczny, którego bezpośrednie połączenie z siecią zewnętrzną jest zabronione bez użycia zatwierdzonych brzegowych urządzeń zabezpieczających;*
	CA-3(3)[2]	*definiuje brzegowe urządzenia zabezpieczające, które zostaną wykorzystane do ustanowienia bezpośredniego połączenia określonego przez organizację jawnego bezpiecznego systemu transgranicznego z siecią zewnętrzną; oraz*
	CA-3(3)[3]	*zakazuje bezpośredniego podłączenia określonego przez organizację jawnego bezpiecznego systemu transgranicznego do sieci zewnętrznej bez użycia określonego przez organizację brzegowego urządzenia zabezpieczającego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące połączeń systemów informacyjnych; polityka ochrony systemu i komunikacji; umowy dotyczące bezpiecznego połączenia systemów sieciowych; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; raport z oceny bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie bezpośrednimi połączeniami z sieciami zewnętrznymi; administratorzy sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel zarządzający bezpośrednio podłączonymi sieciami zewnętrznymi]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające zarządzanie zewnętrznymi połączeniami sieciowymi].	

CA-3(4)	**POŁĄCZENIA MIĘDZYSYSTEMOWE | *POŁĄCZENIA Z SIECIAMI PUBLICZNYMI***	
	CEL OCENY: *Określić, czy organizacja:*	
	CA-3(4)[1]	*określa system informacyjny, którego bezpośrednie połączenie z siecią publiczną ma być zakazane; oraz*

CA-3(4)	**POŁĄCZENIA MIĘDZYSYSTEMOWE | *POŁĄCZENIA Z SIECIAMI PUBLICZNYMI***	
	CA-3(4)[2]	*zakazuje bezpośredniego podłączenia zdefiniowanego przez organizację systemu informacyjnego do sieci publicznej.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące połączeń systemów informacyjnych; polityka ochrony systemu i komunikacji; umowy dotyczące bezpiecznego połączenia systemów sieciowych; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; raport z oceny bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające zarządzanie połączeniami sieci publicznej].	

CA-3(5)	**POŁĄCZENIA MIĘDZYSYSTEMOWE | *OGRANICZENIA DOTYCZĄCE POŁĄCZEŃ SYSTEMU ZEWNĘTRZNEGO***		
	CEL OCENY: *Określić, czy organizacja:*		
	CA-3(5)[1]	*definiuje systemy informacyjne, które mają być dopuszczone do podłączenia do zewnętrznych systemów informacyjnych;*	
	CA-3(5)[2]	*stosuje jedną z następujących zasad umożliwiających organizacyjnie zdefiniowanym systemom informacyjnym połączenie się z zewnętrznymi systemami informacyjnymi:*	
		CA-3(5)[2][a]	*polityka „zezwalaj na wszystko";*
		CA-3(5)[2][b]	*polityka „odmawiaj wszystkiego z wyjątkiem";*
		CA-3(5)[2][c]	*polityka „odmawiaj wszystkiego"; lub*
		CA-3(5)[2][d]	*polityka „zezwalaj na wszystko z wyjątkiem".*

CA-3(5)	**POŁĄCZENIA MIĘDZYSYSTEMOWE | *OGRANICZENIA DOTYCZĄCE POŁĄCZEŃ SYSTEMU ZEWNĘTRZNEGO***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące połączeń systemów informacyjnych; polityka ochrony systemu i komunikacji; porozumienia o wzajemnych połączeniach systemów informacyjnych; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; raport z oceny bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie połączeniami z zewnętrznymi systemami informacyjnymi; administratorzy sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wprowadzające ograniczenia dotyczące połączeń systemu zewnętrznego].

CA-4	**CERTYFIKACJA BEZPIECZEŃSTWA**
[Włączone do: CA-2].	

CA-5	**PLAN I ETAPY DZIAŁANIA**		
	CEL OCENY: *Określić, czy organizacja:*		
	CA-5(a)	*opracowuje plan i etapy działań dla systemu informacyjnego:*	
		CA-5(a)[1]	*dokumentujące planowane działania naprawcze organizacji w celu skorygowania słabych punktów lub braków odnotowanych podczas oceny środków bezpieczeństwa;*
		CA-5(a)[2]	*zmniejszające lub eliminujące znane słabe punkty w systemie;*
	CA-5(b)	**CA-5(b)[1]**	*określające częstotliwość aktualizacji istniejącego planu i etapów działania;*
		CA-5(b)[2]	*aktualizujące istniejący plan i etapy działania z częstotliwością określoną przez organizację, w oparciu o ustalenia wynikające z:*

CA-5	**PLAN I ETAPY DZIAŁANIA**			
			CA-5(b)[2][a]	*oceny środków bezpieczeństwa;*
			CA-5(b)[2][b]	*analizy wpływu na bezpieczeństwo; oraz*
			CA-5(b)[2][c]	*ciągłości monitorowania działań.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny bezpieczeństwa i autoryzacji; procedury dotyczące planów i etapów działania; plan bezpieczeństwa; plan oceny bezpieczeństwa; sprawozdanie z oceny bezpieczeństwa; dokumentacja oceny bezpieczeństwa; plan i etapy działania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za opracowanie planu i etapów działania i jego realizację; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test:** [*wybierz spośród:* Zautomatyzowane mechanizmy opracowywania, wdrażania i utrzymywania planu i etapów działania].			

CA-5(1)	**PLAN I ETAPY DZIAŁANIA | *AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ PLANÓW***	
	CEL OCENY: *Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy, które pozwalają zapewnić, że plan i etapy działań dla systemu informacyjnego są:*	
	CA-5(1)[1]	*szczegółowe;*
	CA-5(1)[2]	*aktualne; oraz*
	CA-5(1)[3]	*natychmiast dostępne.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny bezpieczeństwa i autoryzacji; procedury dotyczące planów i etapów działania; dokumentacja projektowa systemu informacyjnego, ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; zapisy z audytu systemu informacyjnego; plan i etapy działania; inne odpowiednie dokumenty lub rejestry].	

CA-5(1)	**PLAN I ETAPY DZIAŁANIA | *AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ PLANÓW***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za opracowanie planu i etapów działania i jego realizację; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy opracowywania, wdrażania i utrzymywania planu i etapów działania systemu informacyjnego].

CA-6	**AUTORYZACJA BEZPIECZEŃSTWA**	
	CEL OCENY: *Określić, czy organizacja:*	
	CA-6(a)	*wyznacza osobę z kadry kierowniczej, jako autoryzowaną do dopuszczenia systemu informacyjnego do przetwarzania informacji;*
	CA-6(b)	*zapewnia, że dopuszczenie systemu informacyjnego do przetwarzania informacji następuje przed rozpoczęciem przetwarzania informacji w systemie;*
	CA-6(c)	**CA-6(c)[1]** *określa częstotliwość aktualizacji autoryzacji bezpieczeństwa; oraz*
		CA-6(c)[2] *aktualizuje autoryzację bezpieczeństwa z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny bezpieczeństwa i autoryzacji; procedury dotyczące autoryzacji bezpieczeństwa; dokumentacja autoryzacji bezpieczeństwa (zawierająca plan bezpieczeństwa; raport z oceny bezpieczeństwa; plan i etapy działania; świadectwo autoryzacji); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za autoryzację bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające proces autoryzacji bezpieczeństwa i aktualizację].	

CA-7	**CIĄGŁOŚĆ MONITOROWANIA**		
	CEL OCENY: *Określić, czy organizacja:*		
	CA-7(a)	**CA-7(a)[1]**	*opracowuje strategię ciągłości monitorowania, która definiuje metryki do monitorowania;*
		CA-7(a)[2]	*opracowuje strategię ciągłości monitorowania, która obejmuje monitorowanie metryk zdefiniowanych przez organizację;*
		CA-7(a)[3]	*wdraża program ciągłości monitorowania, który obejmuje monitorowanie wskaźników zdefiniowanych w organizacji, zgodnie z organizacyjną strategią ciągłości monitorowania;*
	CA-7(b)	**CA-7(b)[1]**	*opracowuje strategię ciągłości monitorowania, która definiuje częstotliwość monitorowania;*
		CA-7(b)[2]	*definiuje częstotliwości ocen wspierających monitoring;*
		CA-7(b)[3]	*opracowuje strategię ciągłości monitorowania obejmującą wyznaczenie zdefiniowanych organizacyjnie częstotliwości monitorowania i ocen wspierających monitoring;*
		CA-7(b)[4]	*realizuje program ciągłości monitorowania, w tym ustala organizacyjną częstotliwość monitorowania i ocen wspierających monitoring, zgodnie z organizacyjną strategią ciągłości monitorowania;*
	CA-7(c)	**CA-7(c)[1]**	*opracowuje strategię ciągłości monitorowania obejmującą bieżące oceny środków bezpieczeństwa;*
		CA-7(c)[2]	*realizuje program ciągłości monitorowania obejmujący bieżące oceny środków bezpieczeństwa zgodnie z organizacyjną strategią ciągłości monitorowania;*
	CA-7(d)	**CA-7(d)[1]**	*opracowuje strategię ciągłości monitorowania obejmującą bieżące monitorowanie stanu bezpieczeństwa w zakresie wskaźników zdefiniowanych w organizacji;*
		CA-7(d)[2]	*wdraża program ciągłości monitorowania obejmujący bieżące monitorowanie stanu bezpieczeństwa w zakresie wskaźników zdefiniowanych w organizacji, zgodnie z organizacyjną strategią ciągłości monitorowania;*

CA-7	**CIĄGŁOŚĆ MONITOROWANIA**		
	CA-7(e)	**CA-7(e)[1]**	*opracowuje strategię ciągłości monitorowania obejmującą korelację i analizę informacji o bezpieczeństwie generowanych przez system oceny i monitoringu;*
		CA-7(e)[2]	*wdraża program ciągłości monitorowania obejmujący korelację i analizę informacji o bezpieczeństwie generowanych przez system oceny i monitoringu, zgodnie z organizacyjną strategią ciągłości monitorowania;*
	CA-7(f)	**CA-7(f)[1]**	*opracowuje strategię ciągłości monitorowania obejmującą działania w odpowiedzi na wyniki analizy informacji o bezpieczeństwie;*
		CA-7(f)[2]	*wdraża program ciągłości monitorowania obejmujący działania zwrotne w odpowiedzi na wyniki analizy informacji związanych z bezpieczeństwem, zgodnie z organizacyjną strategią ciągłości monitorowania;*
	CA-7(g)	**CA-7(g)[1]**	*opracowuje strategię ciągłości monitorowania, która określa personel lub role, którym ma być przedstawiany stan bezpieczeństwa organizacji i systemu informacyjnego;*
		CA-7(g)[2]	*opracowuje strategię ciągłości monitorowania, która określa częstotliwość przekazywania raportów o stanie bezpieczeństwa organizacji i systemu informacyjnego do personelu lub ról zdefiniowanych w organizacji;*
		CA-7(g)[3]	*rozwija strategię ciągłości monitorowania, która obejmuje zgłaszanie statusu bezpieczeństwa organizacji lub systemu informacyjnego do określonego przez organizację personelu lub ról z częstotliwością określoną przez organizację; oraz*
		CA-7(g)[4]	*wdraża program ciągłości monitorowania, który obejmuje informowanie o stanie bezpieczeństwa organizacji i systemu informacyjnego określonego personelu lub ról z częstotliwością określoną przez organizację, zgodnie z organizacyjną strategią ciągłości monitorowania.*

CA-7	**CIĄGŁOŚĆ MONITOROWANIA**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny bezpieczeństwa i autoryzacji; procedury dotyczące ciągłości monitorowania środków bezpieczeństwa systemu informacyjnego; procedury dotyczące zarządzania konfiguracją; plan bezpieczeństwa; raport z oceny bezpieczeństwa; plan i etapy działania; zapisy z monitoringu systemu informacyjnego; rejestry zarządzania konfiguracją, analizy wpływu na bezpieczeństwo; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ciągłość monitorowania; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Mechanizmy wdrażające ciągłość monitorowania].

CA-7(1)	**CIĄGŁOŚĆ MONITOROWANIA | *NIEZALEŻNA OCENA***	
	CEL OCENY: *Określić, czy organizacja:*	
	CA-7(1)[1]	*określa poziom niezależności, jaki ma być stosowany do bieżącego monitorowania środków bezpieczeństwa w systemie informacyjnym; oraz*
	CA-7(1)[2]	*zatrudnia audytorów lub zespoły oceniające o określonym przez organizację poziomie niezależności w celu bieżącego monitorowania środków bezpieczeństwa w systemie informacyjnym.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny bezpieczeństwa i autoryzacji; procedury dotyczące ciągłości monitorowania środków bezpieczeństwa systemu informacyjnego; plan bezpieczeństwa; raport z oceny bezpieczeństwa; plan i etapy działania; zapisy z monitoringu systemu informacyjnego; analizy wpływu na bezpieczeństwo; raporty o stanie wdrożenia; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ciągłość monitorowania; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

CA-7(2)	**CIĄGŁOŚĆ MONITOROWANIA | *RODZAJE OCEN***
[Włączone do: CA-2].	

CA-7(3)	**CIĄGŁOŚĆ MONITOROWANIA | *ANALIZY TRENDÓW***	
	CEL OCENY: *Ustalić, czy organizacja stosuje analizy trendów w celu określenia, czy poniższe elementy wymagają modyfikacji w oparciu o dane empiryczne:*	
	CA-7(3)[1]	*implementacje środków bezpieczeństwa;*
	CA-7(3)[2]	*częstotliwość przeprowadzania działań związanych z ciągłością monitorowania; i/lub*
	CA-7(3)[3]	*rodzaje działań stosowanych w procesie ciągłości monitorowania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Strategia ciągłości monitorowania; polityka oceny bezpieczeństwa i autoryzacji; procedury dotyczące ciągłości monitorowania środków bezpieczeństwa systemu informacyjnego; plan bezpieczeństwa; raport z oceny bezpieczeństwa; plan i etapy działania; zapisy z monitoringu systemu informacyjnego; analizy wpływu na bezpieczeństwo; raporty o stanie wdrożenia; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ciągłość monitorowania; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

CA-8	**TESTY PENETRACYJNE**	
	CEL OCENY: *Określić, czy organizacja:*	
	CA-8[1]	*definiuje systemy informacyjne lub elementy systemu, w oparciu o które mają być prowadzone testy penetracyjne;*
	CA-8[2]	*określa częstotliwość przeprowadzania testów penetracyjnych w odniesieniu do określonych przez organizację systemów informacyjnych lub elementów systemu; oraz*
	CA-8[3]	*prowadzi testy penetracyjne systemów informacyjnych zdefiniowanych przez organizację lub komponentów systemu, z częstotliwością określoną przez organizację.*

CA-8	**TESTY PENETRACYJNE**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny bezpieczeństwa i autoryzacji; procedury dotyczące przeprowadzania testów penetracyjnych; plan bezpieczeństwa; plan oceny bezpieczeństwa; sprawozdanie z badania penetracyjnego; raport z oceny bezpieczeństwa; dokumentacja oceny bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ocenę bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji, administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające przeprowadzanie testów penetracyjnych].

CA-8(1)	**TESTY PENETRACYJNE | *NIEZALEŻNY TESTER LUB ZESPÓŁ PENETRACYJNY***
	CEL OCENY: *Ustalenie, czy organizacja zatrudnia niezależnego testera lub zespół penetracyjny do wykonywania testów penetracyjnych systemu informacyjnego lub jego elementów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny bezpieczeństwa i autoryzacji; procedury dotyczące przeprowadzania testów penetracyjnych; plan bezpieczeństwa; plan oceny bezpieczeństwa; sprawozdanie z badania penetracyjnego; raport z oceny bezpieczeństwa; dokumentacja oceny bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ocenę bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CA-8(2)	**TESTY PENETRACYJNE | *ĆWICZENIA ZESPOŁU ATAKUJĄCEGO TYPU „RED TEAM”***	
	CEL OCENY: *Określić, czy organizacja:*	
	CA-8(2)[1]	*definiuje ćwiczenia zespołu atakującego typu "Red Team", który ma być wykorzystywany do symulacji prób naruszenia systemów informacyjnych przez przeciwników;*

CA-8(2)	**TESTY PENETRACYJNE | *ĆWICZENIA ZESPOŁU ATAKUJĄCEGO TYPU „RED TEAM”***	
	CA-8(2)[2]	*definiuje zasady działania w zakresie stosowania zdefiniowanych organizacyjnie ćwiczeń "Red Team"; oraz*
	CA-8(2)[3]	*wykorzystuje zdefiniowane przez organizację ćwiczenia zespołu atakującego typu "Red Team" do symulacji prób naruszenia systemów informacyjnych organizacji przez przeciwników, zgodnie ze zdefiniowanymi przez organizację zasadami zaangażowania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny bezpieczeństwa i autoryzacji; procedury dotyczące przeprowadzania testów penetracyjnych; procedury dotyczące ćwiczeń zespołu „Red Team”; plan bezpieczeństwa; plan oceny bezpieczeństwa; wyniki ćwiczeń zespołu „Red Team”; sprawozdanie z przeprowadzonego badania penetracyjnego; raport z oceny bezpieczeństwa; zasady zaangażowania; dokumentacja oceny bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ocenę bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające ćwiczenia zespołu „Red Team”].	

CA-9	**POŁĄCZENIA WEWNĄTRZSYSTEMOWE**		
	CEL OCENY: *Określić, czy organizacja:*		
	CA-9(a)	**CA-9(a)[1]**	*definiuje komponenty systemu informacyjnego lub klasy komponentów, które mają być autoryzowane, jako wewnętrzne połączenia z systemem informacyjnym;*
		CA-9(a)[2]	*zezwala na wewnętrzne połączenia zdefiniowanych przez organizację komponentów systemu informacyjnego lub klas komponentów z systemem informacyjnym;*
	CA-9(b)	*dokumentuje, dla każdego wewnętrznego połączenia:*	
		CA-9(b)[1]	*charakterystykę interfejsu;*
		CA-9(b)[2]	*wymogi bezpieczeństwa; oraz*

CA-9	**POŁĄCZENIA WEWNĄTRZSYSTEMOWE**		
		CA-9(b)[3]	*charakter przekazywanych informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące połączeń systemów informacyjnych; polityka ochrony systemu i komunikacji; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista komponentów lub klas komponentów zatwierdzonych, jako połączenia wewnątrzsystemowe; raport z oceny bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za opracowanie, wdrożenie lub autoryzację połączeń wewnątrzsystemowych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

CA-9(1)	**POŁĄCZENIA WEWNĄTRZSYSTEMOWE | *KONTROLE ZGODNOŚCI BEZPIECZEŃSTWA***
	CEL OCENY: *Ustalić, czy system informacyjny przeprowadza kontrole zgodności bezpieczeństwa na komponentach składowych systemu przed nawiązaniem połączenia wewnętrznego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Zasady kontroli dostępu; procedury dotyczące połączeń systemów informacyjnych; polityka ochrony systemu i komunikacji; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista komponentów lub klas komponentów zatwierdzonych, jako połączenia wewnątrzsystemowe; raport z oceny bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za opracowanie, wdrożenie lub autoryzację połączeń wewnątrzsystemowych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające kontrolę zgodności bezpieczeństwa].

KATEGORIA CM - ZARZĄDZANIE KONFIGURACJĄ

CM-1	**POLITYKA I PROCEDURY ZARZĄDZANIE KONFIGURACJĄ**			
	CEL OCENY: *Określić, czy organizacja:*			
	CM-1(a)(1)	**CM-1(a)(1)[1]**	*opracowuje i dokumentuje politykę zarządzania konfiguracją, która dotyczy:*	
			CM-1(a)(1)[1][a]	*celu;*
			CM-1(a)(1)[1][b]	*zakresu stosowania;*
			CM-1(a)(1)[1][c]	*ról;*
			CM-1(a)(1)[1][d]	*odpowiedzialności;*
			CM-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			CM-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			CM-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		CM-1(a)(1)[2]	*określa personel lub role, wśród których ma być rozpowszechniana polityka zarządzania konfiguracją;*	
		CM-1(a)(1)[3]	*rozpowszechnia politykę zarządzania konfiguracją wśród personelu lub ról zdefiniowanych przez organizację;*	
	CM-1(a)(2)	**CM-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrożenie polityki zarządzania konfiguracją i związanych z nią mechanizmów sterowania konfiguracją;*	
		CM-1(a)(2)[2]	*określa personel lub rolę, którym procedury te mają być rozpowszechniane;*	
		CM-1(a)(2)[3]	*rozpowszechnia procedury wśród zdefiniowanego przez organizację personelu lub ról;*	
	CM-1(b)(1)	**CM-1(b)(1)[1]**	*określa częstotliwość przeglądu i aktualizacji aktualnej polityki zarządzania konfiguracją;*	

CM-1	**POLITYKA I PROCEDURY ZARZĄDZANIE KONFIGURACJĄ**		
		CM-1(b)(1)[2]	*opiniuje i aktualizuje bieżącą politykę zarządzania konfiguracją ze zdefiniowaną przez organizację częstotliwością;*
	CM-1(b)(2)	**CM-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji bieżących procedur zarządzania konfiguracją; oraz*
		CM-1(b)(2)[2]	*opiniuje i aktualizuje bieżące procedury zarządzania konfiguracją z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury zarządzanie konfiguracją; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie konfiguracją; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci].		

CM-2	**KONFIGURACJA PODSTAWOWA**	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-2[1]	*opracowuje i dokumentuje bieżącą konfigurację podstawową systemu informacyjnego; oraz*
	CM-2[2]	*utrzymuje pod bieżącą kontrolą konfigurację bazową systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące konfiguracji podstawowej systemu informacyjnego; plan zarządzania konfiguracją; dokumentacja struktury organizacyjnej; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry zabezpieczeń zmian; inne odpowiednie dokumenty lub rejestry].	

CM-2	**KONFIGURACJA PODSTAWOWA**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie konfiguracją; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania konfiguracją podstawową; zautomatyzowane mechanizmy wspomagające kontrolę parametrów konfiguracji podstawowej].

CM-2(1)	**KONFIGURACJA PODSTAWOWA | *OPINIE I AKTUALIZACJE***		
	CEL OCENY: *Określić, czy organizacja:*		
	CM-2(1)(a)	**CM-2(1)(a)[1]**	*definiuje częstotliwość przeglądania i aktualizacji konfiguracji podstawowej systemu informacyjnego;*
		CM-2(1)(a)[2]	*opiniuje i aktualizuje konfigurację podstawową systemu informacyjnego z częstotliwością określoną przez organizację;*
	CM-2(1)(b)	**CM-2(1)(b)[1]**	*określa okoliczności, które wymagają przeglądu i aktualizacji konfiguracji podstawowej systemu informacyjnego;*
		CM-2(1)(b)[2]	*opiniuje i aktualizuje konfigurację podstawową systemu informacyjnego, gdy jest to wymagane ze względu na uwarunkowania organizacyjne; oraz*
	CM-2(1)(c)	*opiniuje i aktualizuje konfigurację podstawową systemu informacyjnego, jako integralną część instalacji i modernizacji komponentów systemu informacyjnego.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; plan zarządzania konfiguracją; procedury dotyczące konfiguracji podstawowej systemu informacyjnego; procedury dotyczące instalacji i modernizacji komponentów systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; instalacje/modernizacje komponentów systemu informacyjnego i związana z nimi dokumentacja; rejestry zabezpieczeń zmian; inne odpowiednie dokumenty lub rejestry].		

CM-2(1)	**KONFIGURACJA PODSTAWOWA | *OPINIE I AKTUALIZACJE***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie konfiguracją; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania konfiguracją podstawową; zautomatyzowane mechanizmy wspomagające przegląd i aktualizację konfiguracji podstawowej].

CM-2(2)	**KONFIGURACJA PODSTAWOWA | *AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ PLANÓW***	
	CEL OCENY: *Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy do utrzymania:*	
	CM-2(2)[1]	*aktualnej konfiguracji podstawowej systemu informacyjnego;*
	CM-2(2)[2]	*kompletnej konfiguracja podstawowej systemu informacyjnego;*
	CM-2(2)[3]	*dokładnej konfiguracja podstawowej systemu informacyjnego; oraz*
	CM-2(2)[4]	*łatwo dostępnej konfiguracja podstawowej systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące konfiguracji podstawowej systemu informacyjnego; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; zapisy zabezpieczeń zmiany konfiguracji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie konfiguracją; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania konfiguracją podstawową; zautomatyzowane mechanizmy implementujące obsługę konfiguracji podstawowej].	

CM-2(3)	**KONFIGURACJA PODSTAWOWA | *RETENCJA ZACHOWANYCH KONFIGURACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-2(3)[1]	*definiuje poprzednie wersje konfiguracji podstawowej systemu informacyjnego, które mają być zachowane w celu wsparcia backupu; oraz*
	CM-2(3)[2]	*zachowuje zdefiniowane organizacyjnie poprzednie wersje konfiguracji podstawowej systemu informacyjnego w celu obsługi wycofanych wersji podstawowych konfiguracji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące konfiguracji podstawowej systemu informacyjnego; plan zarządzania konfiguracją; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; kopie poprzednich wersji konfiguracji podstawowej; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie konfiguracją; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z zarządzaniem konfiguracją podstawową].	

CM-2(4)	**KONFIGURACJA PODSTAWOWA | *NIEAUTORYZOWANE OPROGRAMOWANIE***
[Włączone do: CM-7].	

CM-2(5)	**KONFIGURACJA PODSTAWOWA | *AUTORYZOWANE OPROGRAMOWANIE***
[Włączone do: CM-7].	

CM-2(6)	**KONFIGURACJA PODSTAWOWA | *ROZBUDOWA SYSTEMÓW I ŚRODOWISKA BADAWCZE***
	CEL OCENY: *Ustalić, czy organizacja utrzymuje konfigurację podstawową do rozbudowy systemów informacyjnych i środowiska testowego, które są zarządzane niezależnie od operacyjnej konfiguracji bazowej.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące konfiguracji podstawowej systemu informacyjnego; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie konfiguracją; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z zarządzaniem konfiguracją podstawową; zautomatyzowane mechanizmy implementujące wydzieloną konfigurację podstawową dla środowisk programistycznych, testowych i operacyjnych].

CM-2(7)	**KONFIGURACJA PODSTAWOWA | *KONFIGUROWANIE SYSTEMU, KOMPONENTÓW LUB URZĄDZEŃ W OBSZARACH WYSOKIEGO RYZYKA***		
	CEL OCENY: *Określić, czy organizacja:*		
	CM-2(7)(a)	**CM-2(7)(a)[1]**	*definiuje systemy informacyjne, elementy systemu lub urządzenia, które mają być udostępniane osobom podróżującym do miejsc, które organizacja uważa za miejsca o istotnym ryzyku;*
		CM-2(7)(a)[2]	*definiuje konfiguracje, które mają być stosowane w systemach informacyjnych, komponentach systemów lub urządzeniach określonych przez organizację, przekazywanych osobom podróżującym do takich miejsc;*

CM-2(7)	**KONFIGURACJA PODSTAWOWA | *KONFIGUROWANIE SYSTEMU, KOMPONENTÓW LUB URZĄDZEŃ W OBSZARACH WYSOKIEGO RYZYKA***		
		CM-2(7)(a)[3]	*wydaje zdefiniowane przez organizację systemy informacyjne, komponenty systemów lub urządzenia o zdefiniowanych przez organizację konfiguracjach dla osób podróżujących do miejsc, które organizacja uważa za miejsca o istotnym ryzyku;*
	CM-2(7)(b)	**CM-2(7)(b)[1]**	*określa środki bezpieczeństwa, które mają być stosowane w odniesieniu do zwracanych urządzeń; oraz*
		CM-2(7)(b)[2]	*stosuje określone organizacyjnie zabezpieczenia do zwracanych urządzeń.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; plan zarządzania konfiguracją; procedury dotyczące konfiguracji podstawowej systemu informacyjnego; procedury dotyczące instalacji i modernizacji komponentów systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry przeglądów i aktualizacji podstawowej konfiguracji systemu informacyjnego; instalacje/modernizacje komponentów systemu informacyjnego i związana z nimi dokumentacja; rejestry zabezpieczeń zmian; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie konfiguracją; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z zarządzaniem konfiguracją podstawową].		

CM-3	**ZABEZPIECZANIE ZMIAN KONFIGURACJI**	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-3(a)	*określa rodzaje dozwolonych zmian w zabezpieczeniach konfiguracji systemu informacyjnego;*
	CM-3(b)	*przegląda proponowane zmiany konfiguracji zabezpieczeń w systemie informacyjnymi zatwierdza lub odrzuca takie zmiany, z wyraźnym uwzględnieniem analiz wpływu na bezpieczeństwo systemu;*

CM-3	**ZABEZPIECZANIE ZMIAN KONFIGURACJI**		
	CM-3(c)	*dokumentuje decyzje o zmianie konfiguracji związanej z systemem informacyjnym;*	
	CM-3(d)	*wprowadza dozwolone zmiany w zabezpieczeniach konfiguracji systemu informacyjnego;*	
	CM-3(e)	**CM-3(e)[1]**	*definiuje okres czasu, w którym przechowywane są zapisy kontrolowanych przez konfigurację zmian w systemie informacyjnym;*
		CM-3(e)[2]	*przechowuje zapisy kontrolowanych przez konfigurację zmian w systemie informacyjnym przez określony przez organizację okres czasu;*
	CM-3(f)	*przeprowadza audyty i przeglądy dokonanych zmian w zabezpieczeniach systemu informacyjnego;*	
	CM-3(g)	**CM-3(g)[1]**	*definiuje organ zabezpieczania zmian w konfiguracji (np. komitet, zarząd) odpowiedzialny za koordynację i nadzór nad działaniami zabezpieczania zmian w konfiguracji;*
		CM-3(g)[2]	*definiuje częstotliwość, z jaką musi się spotykać organ zabezpieczeń zmian konfiguracyjnych; i/lub*
		CM-3(g)[3]	*definiuje warunki zmiany konfiguracji, które powodują zwołanie organu zabezpieczeń zmian konfiguracji; oraz*
		CM-3(g)[4]	*koordynuje i zapewnia nadzór nad czynnościami zabezpieczeń zmiany konfiguracji poprzez zdefiniowany przez organizację organ zabezpieczeń zmiany konfiguracji, który zbiera się z częstotliwością zdefiniowaną przez organizację i/lub dla wszelkich zdefiniowanych przez organizację warunków zmiany konfiguracji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian w konfiguracji systemu informacyjnego; plan zarządzania konfiguracją; architektura systemu informacyjnego i dokumentacja konfiguracyjna; plan bezpieczeństwa; rejestry zabezpieczeń zmian; zapisy z audytu systemu informacyjnego; sprawozdania z audytu zabezpieczania zmian i przeglądów; protokół z posiedzeń dotyczących nadzoru nad zabezpieczeniami zmian w konfiguracji; inne odpowiednie dokumenty lub rejestry].		

CM-3	**ZABEZPIECZANIE ZMIAN KONFIGURACJI**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczanie zmian konfiguracji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; członkowie komisji ds. zabezpieczania zmian lub podobny zespół]. **Test**: [*wybierz spośród:* Procesy organizacyjne zabezpieczeń zmian konfiguracyjnych; zautomatyzowane mechanizmy implementujące zabezpieczenia zmian konfiguracyjnych].

CM-3(1)	**ZABEZPIECZANIE ZMIAN KONFIGURACJI | *AUTOMATYCZNA DOKUMENTACJA / POWIADAMIANIE / ZAKAZ ZMIAN***		
	CEL OCENY: *Określić, czy organizacja:*		
	CM-3(1)(a)	*wykorzystuje zautomatyzowane mechanizmy do dokumentowania proponowanych zmian w systemie informacyjnym;*	
	CM-3(1)(b)	**CM-3(1)(b)[1]**	*definiuje organy zatwierdzające, które mają być powiadamiane o proponowanych zmianach w systemie informacyjnymi żądaniu zatwierdzenia zmian;*
		CM-3(1)(b)[2]	*stosuje zautomatyzowane mechanizmy powiadamiania zdefiniowanych przez organizację organów zatwierdzających o proponowanych zmianach w systemie informacyjnymi żądaniu zatwierdzenia zmian;*
	CM-3(1)(c)	**CM-3(1)(c)[1]**	*definiuje okres czasu, w którym proponowane zmiany w systemie informacyjnym, które nie zostały zatwierdzone lub odrzucone, muszą być wyszczególnione;*
		CM-3(1)(c)[2]	*stosuje zautomatyzowane mechanizmy w celu wskazania proponowanych zmian w systemie informacyjnym, które nie zostały zatwierdzone lub odrzucone przez określony przez organizację okres czasu;*
	CM-3(1)(d)	*stosuje zautomatyzowane mechanizmy uniemożliwiające wprowadzanie zmian w systemie informacyjnym do czasu otrzymania autoryzacji do wykonania tych zmian;*	

CM-3(1)	**ZABEZPIECZANIE ZMIAN KONFIGURACJI | *AUTOMATYCZNA DOKUMENTACJA / POWIADAMIANIE / ZAKAZ ZMIAN***		
	CM-3(1)(e)	*wykorzystuje zautomatyzowane mechanizmy do dokumentowania wszystkich zmian w systemie informacyjnym;*	
	CM-3(1)(f)	**CM-3(1)(f)[1]**	*określa personel, który należy powiadomić po zakończeniu wprowadzania zatwierdzonych zmian w systemie informacyjnym; oraz*
		CM-3(1)(f)[2]	*stosuje zautomatyzowane mechanizmy powiadamiania personelu zdefiniowanego przez organizację, gdy zatwierdzone zmiany w systemie informacyjnym zostaną zakończone.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian w konfiguracji systemu informacyjnego; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; mechanizmy automatycznej kontroli konfiguracji; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry zabezpieczeń zmian; zapisy z audytu systemu informacyjnego; wnioski o zatwierdzenie zmian; zatwierdzenia zmian; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczanie zmian konfiguracji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne zabezpieczające zmiany konfiguracyjne; zautomatyzowane mechanizmy realizujące działania zabezpieczeń zmian konfiguracyjnych].		

CM-3(2)	**ZABEZPIECZANIE ZMIAN KONFIGURACJI | *TESTY / WALIDACJA / ZMIANY DOKUMENTÓW***	
	CEL OCENY: *Ustalić, czy organizacja, przed wprowadzeniem zmian w systemie operacyjnym:*	
	CM-3(2)[1]	*testuje zmiany w systemie informacyjnym;*
	CM-3(2)[2]	*zatwierdza zmiany w systemie informacyjnym; oraz*
	CM-3(2)[3]	*dokumentuje zmiany w systemie informacyjnym.*

CM-3(2)	**ZABEZPIECZANIE ZMIAN KONFIGURACJI | *TESTY / WALIDACJA / ZMIANY DOKUMENTÓW***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; plan zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian w konfiguracji systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; protokoły z badań; rejestry weryfikacji; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczanie zmian konfiguracji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zabezpieczające zmiany w konfiguracji; zautomatyzowane mechanizmy wspierające i/lub wdrażające testowanie, weryfikowanie i dokumentowanie zmian w systemie informacyjnym].

CM-3(3)	**ZABEZPIECZANIE ZMIAN KONFIGURACJI | *AUTOMATYCZNE ZMIANY IMPLEMENTACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-3(3)[1]	*stosuje zautomatyzowane mechanizmy implementacji zmian w aktualnych bazach systemów informacyjnych;*
	CM-3(3)[2]	*dokonuje instalacji zaktualizowanej bazy w systemie informacyjnym.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; plan zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian w konfiguracji systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; mechanizmy automatycznej kontroli konfiguracji; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczanie zmian konfiguracji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne zabezpieczające zmiany konfiguracji; zautomatyzowane mechanizmy wprowadzające zmiany w aktualnej bazie systemu informacyjnego].	

CM-3(4)	**ZABEZPIECZANIE ZMIAN KONFIGURACJI | *PRZEDSTAWICIEL BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-3(4)[1]	*określa zespół kontroli zmian konfiguracji (zgodnie z zabezpieczeniem CM-3g), którego członkiem jest przedstawiciel ds. bezpieczeństwa informacji; oraz*
	CM-3(4)[2]	*wymaga, aby przedstawiciel ds. bezpieczeństwa informacji był członkiem określonego zespołu kontroli konfiguracji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian w konfiguracji systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczanie zmian konfiguracji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące zabezpieczania zmian w konfiguracji].	

CM-3(5)	**ZABEZPIECZANIE ZMIAN KONFIGURACJI | *AUTOMATYCZNA REAKCJA BEZPIECZEŃSTWA***	
	CEL OCENY: *Określić, czy:*	
	CM-3(5)[1]	*organizacja określa środki bezpieczeństwa, które zostaną zaimplementowane automatycznie w przypadku nieautoryzowanej zmiany konfiguracji podstawowej; oraz*
	CM-3(5)[2]	*system informacyjny automatycznie wdraża zdefiniowane organizacyjnie środki bezpieczeństwa, jeśli konfiguracja podstawowa zostanie zmieniona w sposób nieautoryzowany.*

CM-3(5)	**ZABEZPIECZANIE ZMIAN KONFIGURACJI | *AUTOMATYCZNA REAKCJA BEZPIECZEŃSTWA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian w konfiguracji systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; alarmy / powiadomienia o nieautoryzowanych zmianach konfiguracji podstawowej; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczanie zmian konfiguracji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące zabezpieczania zmian w konfiguracji; zautomatyzowane mechanizmy implementujące środki bezpieczeństwa w odpowiedzi na zmiany konfiguracji podstawowej].

CM-3(6)	**ZABEZPIECZANIE ZMIAN KONFIGURACJI | *ZARZĄDZANIE KRYPTOGRAFICZNE***	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-3(6)[1]	*definiuje środki bezpieczeństwa, zapewniane przez mechanizmy kryptograficzne, które mają być zarządzane w ramach konfiguracji; oraz*
	CM-3(6)[2]	*zapewnia, że mechanizmy kryptograficzne, stosowane w celu wprowadzenia zdefiniowanych w organizacji zabezpieczeń, są objęte zarządzaniem konfiguracją.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące zabezpieczania zmian w konfiguracji systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; inne odpowiednie dokumenty lub rejestry].	

CM-3(6)	**ZABEZPIECZANIE ZMIAN KONFIGURACJI | *ZARZĄDZANIE KRYPTOGRAFICZNE***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczanie zmian konfiguracji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące zabezpieczania zmian w konfiguracji; mechanizmy kryptograficzne wdrażające organizacyjne środki bezpieczeństwa].

CM-4	**ANALIZA ZMIAN WPŁYWAJĄCYCH NA BEZPIECZEŃSTWO**
	CEL OCENY: *Ustalić, czy organizacja analizuje zmiany w systemie informacyjnym w celu określenia potencjalnego wpływu na bezpieczeństwo przed wdrożeniem zmiany.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące analizy wpływu na bezpieczeństwo w przypadku zmian w systemie informacyjnym; plan zarządzania konfiguracją; dokumentacja analizy zmian wpływających na bezpieczeństwo; narzędzia analityczne i związane z nimi wyniki; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za przeprowadzanie analizy zmian wpływających na bezpieczeństwo; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie analizy zmian wpływających na bezpieczeństwo].

CM-4(1)	**ANALIZA ZMIAN WPŁYWAJĄCYCH NA BEZPIECZEŃSTWO | *ODDZIELNE ŚRODOWISKA BADAWCZE***	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-4(1)[1]	*analizuje zmiany w systemie informacyjnym w oddzielnym środowisku badawczym przed ich wdrożeniem w środowisku operacyjnym;*
	CM-4(1)[2]	*analizuje zmiany w systemie informacyjnym w oddzielnym środowisku badawczym, szukając wpływu na poziom bezpieczeństwa wynikający z:*

CM-4(1)	**ANALIZA ZMIAN WPŁYWAJĄCYCH NA BEZPIECZEŃSTWO | *ODDZIELNE ŚRODOWISKA BADAWCZE***		
		CM-4(1)[2][a]	*wad;*
		CM-4(1)[2][b]	*słabości;*
		CM-4(1)[2][c]	*niekompatybilności; oraz*
		CM-4(1)[2][d]	*celowej złośliwości.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące analizy wpływu na bezpieczeństwo w przypadku zmian w systemie informacyjnym; plan zarządzania konfiguracją; dokumentacja analizy zmian wpływających na bezpieczeństwo; narzędzia analityczne i związane z nimi wyniki; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; rejestry zabezpieczeń zmian; zapisy z audytu systemu informacyjnego; dokumentacja potwierdzająca istnienie odrębnych środowisk badawczych i operacyjnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za przeprowadzanie analizy zmian wpływających na bezpieczeństwo; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie analizy zmian wpływających na bezpieczeństwo; zautomatyzowane mechanizmy wspierające i/lub wdrażające analizę zamian wpływających na bezpieczeństwo].		

CM-4(2)	**ANALIZA ZMIAN WPŁYWAJĄCYCH NA BEZPIECZEŃSTWO | *WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA***	
	CEL OCENY: *Ustalić, czy organizacja, po zmianie wprowadzonej do systemu informacyjnego, sprawdza funkcje bezpieczeństwa w celu sprawdzenia, czy są to funkcje:*	
	CM-4(2)[1]	*prawidłowo wprowadzony w życie;*
	CM-4(2)[2]	*działające zgodnie z przeznaczeniem; oraz*
	CM-4(2)[3]	*dające pożądany wynik w odniesieniu do spełniania wymagań bezpieczeństwa dla systemu.*

CM-4(2)	**ANALIZA ZMIAN WPŁYWAJĄCYCH NA BEZPIECZEŃSTWO | *WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące analizy wpływu na bezpieczeństwo w przypadku zmian w systemie informacyjnym; plan zarządzania konfiguracją; dokumentacja analizy zmian wpływających na bezpieczeństwo; narzędzia analityczne i związane z nimi wyniki; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za przeprowadzanie analizy zmian wpływających na bezpieczeństwo; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie analizy zmian wpływających na bezpieczeństwo; zautomatyzowane mechanizmy wspierające i/lub wdrażające weryfikację funkcji bezpieczeństwa.

CM-5	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN**	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-5[1]	*definiuje fizyczne ograniczenia dostępu związane ze zmianami w systemie informacyjnym;*
	CM-5[2]	*dokumentuje fizyczne ograniczenia dostępu związane ze zmianami w systemie informacyjnym;*
	CM-5[3]	*zatwierdza fizyczne ograniczenia dostępu związane ze zmianami w systemie informacyjnym;*
	CM-5[4]	*egzekwuje fizyczne ograniczenia dostępu związane ze zmianami w systemie informacyjnym;*
	CM-5[5]	*definiuje logiczne ograniczenia dostępu związane ze zmianami w systemie informacyjnym;*
	CM-5[6]	*dokumentuje logiczne ograniczenia dostępu związane ze zmianami w systemie informacyjnym;*
	CM-5[7]	*zatwierdza logiczne ograniczenia dostępu związane ze zmianami w systemie informacyjnym; oraz*

CM-5	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN**	
	CM-5[8]	*egzekwuje logiczne ograniczenia dostępu związane ze zmianami w systemie informacyjnym.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące ograniczania możliwości dokonywania zmian w systemie informacyjnym; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; zatwierdzenia dostępu logicznego; zatwierdzenia dostępu fizycznego; poświadczenia dostępu; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za logiczną kontrolę dostępu; personel organizacji odpowiedzialny za fizyczną kontrolę dostępu; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania ograniczeniami dostępu do dokonywania zmian; zautomatyzowane mechanizmy wspierające/wprowadzające/wykonujące ograniczenia dostępu związane ze zmianami w systemie informacyjnym].	

CM-5(1)	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | *REALIZACJA AUTOMATYCZNEGO DOSTĘPU / AUDYTU***	
	CEL OCENY: *Ustalić, czy system informacyjny:*	
	CM-5(1)[1]	*egzekwuje ograniczenia możliwości dokonywania zmian; oraz*
	CM-5(1)[2]	*wspiera audyt działań wykonawczych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące ograniczania możliwości dokonywania zmian w systemie informacyjnym; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

CM-5(1)	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | *REALIZACJA AUTOMATYCZNEGO DOSTĘPU / AUDYTU***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania ograniczeniami dostępu do zmian; zautomatyzowane mechanizmy realizujące egzekwowanie ograniczania możliwości dokonywania zmian w systemie informacyjnym; zautomatyzowane mechanizmy wspomagające audyt działań wykonawczych].

CM-5(2)	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | *PRZEGLĄD ZMIAN SYSTEMU***	
	CEL OCENY: *Ustalić, czy organizacja, podejmując próbę ustalenia, czy nastąpiły nieautoryzowane zmiany:*	
	CM-5(2)[1]	*określa częstotliwość przeglądania zmian w systemie informacyjnym;*
	CM-5(2)[2]	*definiuje okoliczności, które uzasadniają przegląd zmian w systemie informacyjnym;*
	CM-5(2)[3]	*dokonuje przeglądu zmian w systemie informacyjnym z częstotliwością określoną przez organizację; oraz*
	CM-5(2)[4]	*analizuje zmiany w systemie informacyjnym wraz z określonymi przez organizację okolicznościami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące ograniczania możliwości dokonywania zmian w systemie informacyjnym; plan zarządzania konfiguracją; plan bezpieczeństwa; przeglądy zmian w systemie informacyjnym; sprawozdania z audytu i przeglądu; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania ograniczeniami dostępu do zmian; zautomatyzowane mechanizmy wspierające/wdrażające przeglądy systemów informacyjnych w celu ustalenia, czy wystąpiły nieautoryzowane zmiany].	

CM-5(3)	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | *PODPISANE KOMPONENTY***	
	CEL OCENY: *Określić, czy:*	
	CM-5(3)[1]	*organizacja określa składniki aplikacji i oprogramowania układowego, których zainstalowanie przez system informacyjny będzie niemożliwe bez sprawdzenia, czy składniki te zostały podpisane cyfrowo za pomocą certyfikatu, który jest uznawany i zatwierdzony przez organizację; oraz*
	CM-5(3)[2]	*system informacyjny uniemożliwia instalację komponentów aplikacji i oprogramowania układowego zdefiniowanych przez organizację bez weryfikacji, czy komponenty te zostały podpisane cyfrowo za pomocą certyfikatu, który jest uznawany i zatwierdzony przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące ograniczania możliwości dokonywania zmian w systemie informacyjnym; plan zarządzania konfiguracją; plan bezpieczeństwa; lista składników aplikacji i oprogramowania układowego, których instalacja bez uznanego i zatwierdzonego certyfikatu jest zabroniona; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Organizacyjne procesy zarządzania ograniczeniami dostępu do zmian; zautomatyzowane mechanizmy uniemożliwiające instalację komponentów aplikacji i oprogramowania układowego niepodpisanych certyfikatem uznanym i zatwierdzonym przez organizację].	

CM-5(4)	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | *PODWÓJNA AUTORYZACJA***	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-5(4)[1]	*definiuje elementy systemu informacyjnego oraz informacje na poziomie systemu, które wymagają egzekwowania podwójnej autoryzacji przy wprowadzaniu zmian; oraz*

CM-5(4)	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | *PODWÓJNA AUTORYZACJA***	
	CM-5(4)[2]	*egzekwuje podwójną autoryzację w zakresie wprowadzania zmian do zdefiniowanych przez organizację komponentów systemu informacyjnego i informacji na poziomie systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące ograniczania możliwości dokonywania zmian w systemie informacyjnym; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za wdrożenie zmian w systemie informacyjnym z wykorzystaniem podwójnej autoryzacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania ograniczeniami dostępu do zmian; zautomatyzowane mechanizmy wdrażające egzekwowanie zasady podwójnej autoryzacji].	

CM-5(5)	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | *OGRANICZENIA PRODUKTOWE / UPRAWNIENIA OPERACYJNE***		
	CEL OCENY: *Określić, czy organizacja:*		
	CM-5(5)(a)	*ogranicza uprawnienia do zmiany komponentów systemu informacyjnego i informacji związanych z systemem w środowisku produkcyjnym lub operacyjnym;*	
	CM-5(5)(b)	**CM-5(5)(b)[1]**	*określa częstotliwość przeglądów i ponownej oceny uprawnień; oraz*
		CM-5(5)(b)[2]	*dokonuje przeglądu i ponownej oceny uprawnień z częstotliwością określoną przez organizację.*

CM-5(5)	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | *OGRANICZENIA PRODUKTOWE / UPRAWNIENIA OPERACYJNE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące ograniczania możliwości dokonywania zmian w systemie informacyjnym; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; przeglądy uprawnień użytkownika; ponowna weryfikacja uprawnień użytkownika; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania ograniczeniami dostępu do zmian; zautomatyzowane mechanizmy wspierające i/lub wdrażające ograniczenia możliwości dokonywania zmian].

CM-5(6)	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | *OGRANICZENIE PRZYWILEJÓW W BIBLIOTEKACH OPROGRAMOWANIA***
	CEL OCENY: *Ustalić, czy organizacja ogranicza uprawnienia do zmiany oprogramowania w bibliotekach oprogramowania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące ograniczania możliwości dokonywania zmian w systemie informacyjnym; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania ograniczeniami dostępu do zmian; zautomatyzowane mechanizmy wspierające i/lub wdrażające ograniczenia możliwości dokonywania zmian].

CM-5(7)	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | *AUTOMATYCZNE WDRAŻANIE ŚRODKÓW BEZPIECZEŃSTWA***
[Włączone do: SI-7].	

CM-6	**USTAWIENIA KONFIGURACJI**			
	CEL OCENY: *Ustalić, czy organizacja:*			
	CM-6(a)	**CM-6(a)[1]**	*definiuje listy kontrolne konfiguracji zabezpieczeń, które mają być wykorzystywane do tworzenia i dokumentowania konfiguracji ustawień wykorzystywanych produktów informacyjnych;*	
		CM-6(a)[2]	*zapewnia, że zdefiniowane listy kontrolne konfiguracji zabezpieczeń odzwierciedlają najbardziej restrykcyjny tryb pracy zgodny z wymaganiami operacyjnymi;*	
		CM-6(a)[3]	*tworzy i dokumentuje ustawienia konfiguracji produktów informacyjnych wykorzystywanych w systemie informacyjnym, za pomocą zdefiniowanych przez organizację list kontrolnych zabezpieczeń;*	
	CM-6(b)	*implementuje ustawienia konfiguracji ustalone/dokumentowane w zabezpieczeniu CM-6(a);*		
	CM-6(c)	**CM-6(c)[1]**	*definiuje elementy systemu informacyjnego, dla których wszelkie odstępstwa od ustalonych ustawień konfiguracji muszą być:*	
			CM-6(c)[1][a]	*zidentyfikowane;*
			CM-6(c)[1][b]	*udokumentowane;*
			CM-6(c)[1][c]	*zatwierdzone;*
		CM-6(c)[2]	*definiuje wymagania operacyjne dotyczące wsparcia:*	
			CM-6(c)[2][a]	*identyfikacji wszelkich odchyleń od ustalonych ustawień konfiguracji;*
			CM-6(c)[2][b]	*dokumentacji wszelkich odchyleń od założonych ustawień konfiguracji;*

CM-6	**USTAWIENIA KONFIGURACJI**			
			CM-6(c)[2][c]	*zatwierdzania wszelkich odchyleń od założonych ustawień konfiguracji;*
		CM-6(c)[3]	*identyfikuje wszelkie odchylenia od ustalonej konfiguracji ustawień komponentów systemu informacyjnego zdefiniowanego przez organizację w oparciu o określone wymagania operacyjne;*	
		CM-6(c)[4]	*dokumentuje wszelkie odstępstwa od ustalonej konfiguracji ustawień komponentów systemu informacyjnego zdefiniowanego przez organizację w oparciu o określone organizacyjnie wymagania operacyjne;*	
		CM-6(c)[5]	*zatwierdza wszelkie odchylenia od ustalonej konfiguracji ustawień komponentów systemu informacyjnego zdefiniowanego przez organizację w oparciu o określone organizacyjnie wymagania operacyjne;*	
	CM-6(d)	**CM-6(d)[1]**	*monitoruje zmiany w konfiguracji ustawień zgodnie z zasadami i procedurami organizacyjnymi; oraz*	
		CM-6(d)[2]	*kontroluje zmiany w konfiguracji ustawień zgodnie z zasadami i procedurami organizacyjnymi.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące ustawienia konfiguracji systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; listy kontrolne konfiguracji zabezpieczeń; dokumentacja potwierdzająca zatwierdzone odstępstwa od ustalonych ustawień konfiguracji; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie konfiguracją zabezpieczeń; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania ustawieniami konfiguracji; zautomatyzowane mechanizmy implementujące, monitorujące i/lub sterujące ustawieniami konfiguracji systemu informacyjnego; zautomatyzowane mechanizmy identyfikujące i/lub dokumentujące odchylenia od ustalonych ustawień konfiguracji].			

CM-6(1)	**USTAWIENIA KONFIGURACJI | *AUTOMATYCZNE SCENTRALIZOWANE ZARZĄDZANIE / APLIKACJA / WERYFIKACJA***		
	CEL OCENY: *Określić, czy organizacja:*		
	CM-6(1)[1]	*definiuje elementy systemu informacyjnego, do których mają być zastosowane mechanizmy automatyczne:*	
		CM-6(1)[1][a]	*centralnie zarządzające ustawieniami konfiguracyjnym i komponentów system informacyjnego;*
		CM-6(1)[1][b]	*wprowadzające ustawienia konfiguracyjne w tych komponentach;*
		CM-6(1)[1][c]	*weryfikujące ustawienia konfiguracyjne tych komponentów;*
	CM-6(1)[2]	*używa automatycznych mechanizmów do:*	
		CM-6(1)[2][a]	*centralnego zarządzania konfiguracją ustawień zdefiniowanych przez organizację komponentów systemu informacyjnego;*
		CM-6(1)[2][b]	*ustawiania konfiguracji w zdefiniowanych przez organizację składnikach systemu informacyjnego; oraz*
		CM-6(1)[2][c]	*weryfikacji ustawień konfiguracji w zdefiniowanych przez organizację komponentach systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące ustawienia konfiguracji systemu informacyjnego; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; listy kontrolne konfiguracji zabezpieczeń; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie konfiguracją zabezpieczeń; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów].		

CM-6(1)	**USTAWIENIA KONFIGURACJI | *AUTOMATYCZNE SCENTRALIZOWANE ZARZĄDZANIE / APLIKACJA / WERYFIKACJA***
	Test: [*wybierz spośród:* Procesy organizacyjne zarządzania ustawieniami konfiguracyjnymi; zautomatyzowane mechanizmy wdrożone w celu centralnego zarządzania, stosowania i weryfikacji ustawień konfiguracyjnych systemu informacyjnego.].

CM-6(2)	**USTAWIENIA KONFIGURACJI | *ODPOWIEDŹ NA NIEAUTORYZOWANE ZMIANY***	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-6(2)[1]	*definiuje ustawienia konfiguracji, które w przypadku nieautoryzowanych zmian skutkują zastosowaniem zabezpieczeń organizacyjnych w odpowiedzi na takie zmiany;*
	CM-6(2)[2]	*definiuje zabezpieczenia, które mają być zastosowane, w odpowiedzi na nieautoryzowane zmiany, w ustawieniach konfiguracji; oraz*
	CM-6(2)[3]	*stosuje zdefiniowane organizacyjnie środki bezpieczeństwa w odpowiedzi na nieautoryzowane zmiany w ustawieniach konfiguracji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące ustawienia konfiguracji systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; alarmy/ powiadomienia o nieautoryzowanych zmianach w ustawieniach konfiguracji systemu informacyjnego; udokumentowane odpowiedzi na nieautoryzowane zmiany ustawień konfiguracji w systemie informacyjnym; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie konfiguracją zabezpieczeń; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Reakcje na nieautoryzowane zmiany ustawień konfiguracji systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub implementujące zabezpieczenia przed nieautoryzowanymi zmianami konfiguracji].	

CM-6(3)	**USTAWIENIA KONFIGURACJI | *WYKRYWANIE NIEAUTORYZOWANYCH ZMIAN***
[Włączone do: SI-7].	

CM-6(4)	**USTAWIENIA KONFIGURACJI | *PREZENTACJA ZGODNOŚCI***
[Włączone do: CM-4].	

CM-7	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI**			
	CEL OCENY: *Określić, czy organizacja:*			
	CM-7(a)	*konfiguruje system informacyjny tak, aby zapewniał tylko niezbędne wymagane funkcje;*		
	CM-7(b)	**CM-7(b)[1]**	*definiuje zakaz lub ograniczenie:*	
			CM-7(b)[1][a]	*funkcji;*
			CM-7(b)[1][b]	*portów;*
			CM-7(b)[1][c]	*protokołów; i/lub*
			CM-7(b)[1][d]	*usług;*
		CM-7(b)[2]	*zakazuje lub ogranicza stosowanie zdefiniowanych przez organizację:*	
			CM-7(b)[2][a]	*funkcji;*
			CM-7(b)[2][b]	*portów;*
			CM-7(b)[2][c]	*protokołów; i/lub*
			CM-7(b)[2][d]	*usług.*

CM-7	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; listy kontrolne konfiguracji zabezpieczeń; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie konfiguracją zabezpieczeń; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne blokujące lub ograniczające funkcje, porty, protokoły i/lub usługi; zautomatyzowane mechanizmy wprowadzające ograniczenia lub blokady funkcji, portów, protokołów i/lub usług].

CM-7(1)	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI | *OKRESOWE PRZEGLĄDY***			
	CEL OCENY: *Określić, czy organizacja:*			
	CM-7(1)(a)	**CM-7(1)(a)[1]**	*określa częstotliwość przeglądów systemu informacyjnego w celu identyfikacji niepożądanych i/lub niezabezpieczonych:*	
			CM-7(1)(a)[1][a]	*funkcji;*
			CM-7(1)(a)[1][b]	*portów;*
			CM-7(1)(a)[1][c]	*protokołów; i/lub*
			CM-7(1)(a)[1][d]	*usług;*
		CM-7(1)(a)[2]	*dokonuje przeglądu systemu informacyjnego z częstotliwością określoną przez organizację, w celu identyfikacji niepożądanych i/lub niezabezpieczonych:*	
			CM-7(1)(a)[2][a]	*funkcji;*
			CM-7(1)(a)[2][b]	*portów;*
			CM-7(1)(a)[2][c]	*protokołów; i/lub*

<table>
<tr><th colspan="5">CM-7(1) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | OKRESOWE PRZEGLĄDY</th></tr>
<tr><td></td><td></td><td></td><td>CM-7(1)(a)[2][d]</td><td>usług;</td></tr>
<tr><td></td><td>CM-7(1)(b)</td><td>CM-7(1)(b)[1]</td><td colspan="2">definiuje, w ramach systemu informacyjnego, niepożądane i/lub niezabezpieczone:</td></tr>
<tr><td></td><td></td><td></td><td>CM-7(1)(b)[1][a]</td><td>funkcje;</td></tr>
<tr><td></td><td></td><td></td><td>CM-7(1)(b)[1][b]</td><td>porty;</td></tr>
<tr><td></td><td></td><td></td><td>CM-7(1)(b)[1][c]</td><td>protokoły; i/lub</td></tr>
<tr><td></td><td></td><td></td><td>CM-7(1)(b)[1][d]</td><td>usługi;</td></tr>
<tr><td></td><td></td><td>CM-7(1)(b)[2]</td><td colspan="2">dezaktywuje organizacyjnie zdefiniowane, jako niepożądane i/lub niezabezpieczone:</td></tr>
<tr><td></td><td></td><td></td><td>CM-7(1)(b)[2][a]</td><td>funkcje;</td></tr>
<tr><td></td><td></td><td></td><td>CM-7(1)(b)[2][b]</td><td>porty;</td></tr>
<tr><td></td><td></td><td></td><td>CM-7(1)(b)[2][c]</td><td>protokoły; i/lub</td></tr>
<tr><td></td><td></td><td></td><td>CM-7(1)(b)[2][d]</td><td>usługi;</td></tr>
<tr><td></td><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:

Sprawdź: [wybierz spośród: Polityka zarządzania konfiguracją; procedury zapewniające zasadę minimalnej funkcjonalności w systemie informacyjnym; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; listy kontrolne konfiguracji zabezpieczeń; udokumentowane przeglądy funkcji, portów, protokołów i/lub usług; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za przegląd funkcji, portów, protokołów i usług w systemie informacyjnym; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci].

Test: [wybierz spośród: Procesy organizacyjne służące do przeglądania/dezaktywacji funkcji, portów, protokołów i/lub usług niezabezpieczonych; zautomatyzowane mechanizmy wdrażające przegląd i dezaktywację funkcji, portów, protokołów i/lub usług niezabezpieczonych].</td></tr>
</table>

CM-7(2)	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI | *ZAPOBIEGANIE WYKONYWANIU PROGRAMU***		
	CEL OCENY: *Określić, czy:*		
	CM-7(2)[1]	*organizacja określa zasady dotyczące korzystania z oprogramowania i ograniczeń jego użytkowania;*	
	CM-7(2)[2]	*system informacyjny uniemożliwia wykonanie programu zgodnie z jedną lub obiema z poniższych zasad:*	
		CM-7(2)[2][a]	*zdefiniowane przez organizację zasady dotyczące korzystania z programu i stosowania ograniczeń; i/lub*
		CM-7(2)[2][b]	*zasady autoryzujące warunki korzystania z oprogramowania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury zapewniające zasadę minimalnej funkcjonalności w systemie informacyjnym; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; specyfikacje dotyczące zabezpieczenia przed wykonaniem programu; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test:** [*wybierz spośród:* Procesy organizacyjne uniemożliwiające wykonanie programu w systemie informacyjnym; procesy organizacyjne związane z użytkowaniem i ograniczeniami w użytkowaniu oprogramowania; zautomatyzowane mechanizmy uniemożliwiające wykonanie programu w systemie informacyjnym; zautomatyzowane mechanizmy wspierające i/lub wdrażające użytkowanie i ograniczenia w użytkowaniu oprogramowania].		

CM-7(3)	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI | *STOSOWANIE REJESTRACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-7(3)[1]	*określa wymogi rejestracyjne dla:*

CM-7(3)	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI | *STOSOWANIE REJESTRACJI***		
		CM-7(3)[1][a]	*funkcji;*
		CM-7(3)[1][b]	*portów;*
		CM-7(3)[1][c]	*protokołów; i/lub*
		CM-7(3)[1][d]	*usług;*
	CM-7(3)[2]	*zapewnia zgodność z określonymi przez organizację wymogami rejestracyjnymi:*	
		CM-7(3)[2][a]	*funkcji;*
		CM-7(3)[2][b]	*portów;*
		CM-7(3)[2][c]	*protokołów; i/lub*
		CM-7(3)[2][d]	*usług.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury zapewniające zasadę minimalnej funkcjonalności w systemie informacyjnym; plan zarządzania konfiguracją; plan bezpieczeństwa; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; audyt i kontrole zgodności; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zapewniające zgodność z wymogami rejestracyjnymi dotyczącymi funkcji, portów, protokołów i/lub usług; zautomatyzowane mechanizmy wdrażające zgodność z wymogami rejestracyjnymi dotyczącymi funkcji, portów, protokołów i/lub usług].		

CM-7(4)	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI | *NIEAUTORYZOWANE OPROGRAMOWANIE („CZARNA LISTA”)***	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-7(4)(a)	*identyfikuje/definiuje programy, które nie są uprawnione do rezydowania w systemie informacyjnym;*

CM-7(4)	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI | *NIEAUTORYZOWANE OPROGRAMOWANIE („CZARNA LISTA”)***		
	CM-7(4)(b)	*stosuje politykę " zezwalaj na wszystko z wyjątkiem" w celu zakazania wykonywania nieautoryzowanego oprogramowania w systemie informacyjnym;*	
	CM-7(4)(c)	**CM-7(4)(c)[1]**	*określa częstotliwość przeglądania i aktualizacji listy oprogramowania nieautoryzowanego w systemie informacyjnym; oraz*
		CM-7(4)(c)[2]	*opiniuje i aktualizuje listy oprogramowania nieautoryzowanego z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury zapewniające zasadę minimalnej funkcjonalności w systemie informacyjnym; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista programów nieautoryzowanych do wykonywania w systemie informacyjnym; listy kontrolne konfiguracji zabezpieczeń; przegląd i aktualizacja zapisów listy nieautoryzowanego oprogramowania; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za identyfikację oprogramowania nieautoryzowanego do wykonywania w systemie informacyjnym; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Organizacyjny proces identyfikacji, przeglądania i aktualizacji programów nieautoryzowanych do wykonywania w systemie informacyjnym; organizacyjny proces wdrażania *czarnych list*; zautomatyzowane mechanizmy wspierające i/lub wdrażające *czarne listy*].		

CM-7(5)	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI | *AUTORYZOWANE OPROGRAMOWANIE („BIAŁA LISTA”)***	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-7(5)(a)	*identyfikuje/definiuje oprogramowanie autoryzowane do wykonywania w systemie informacyjnym;*

CM-7(5)	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI | *AUTORYZOWANE OPROGRAMOWANIE („BIAŁA LISTA")***		
	CM-7(5)(b)	*stosuje politykę „odmawiaj wszystkiego z wyjątkiem", aby umożliwić wykonywanie autoryzowanego oprogramowania w systemie informacyjnym;*	
	CM-7(5)(c)	**CM-7(5)(c)[1]**	*określa częstotliwość przeglądania i aktualizacji listy autoryzowanego oprogramowania w systemie informacyjnym; oraz*
		CM-7(5)(c)[2]	*opiniuje i aktualizuje listy autoryzowanego oprogramowania z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury zapewniające zasadę minimalnej funkcjonalności w systemie informacyjnym; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista autoryzowanych programów dopuszczonych do uruchamiania w systemie informacyjnym; listy kontrolne konfiguracji zabezpieczeń; przegląd i aktualizacja zapisów listy autoryzowanego oprogramowania; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za identyfikację autoryzowanego oprogramowania, dopuszczonego do wykonywania w systemie informacyjnym; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Proces organizacyjny identyfikacji, przeglądania i aktualizacji autoryzowanych programów, dopuszczonych do uruchamiania w systemie informacyjnym; proces organizacyjny wdrażania białej listy; zautomatyzowane mechanizmy wdrażania białej listy].		

CM-8	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO**		
	CEL OCENY: *Określić, czy organizacja:*		
	CM-8(a)	**CM-8(a)(1)**	*opracowuje i dokumentuje spis komponentów systemu informacyjnego, który dokładnie odzwierciedla architekturę eksploatowanego systemu informacyjnego;*

<table>
<tr><th colspan="5">CM-8 INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO</th></tr>
<tr><td rowspan="6"></td><td rowspan="5"></td><td>CM-8(a)(2)</td><td colspan="2">opracowuje i dokumentuje spis komponentów systemu informacyjnego, który obejmuje wszystkie składniki znajdujące się w granicach autoryzacji systemu informacyjnego;</td></tr>
<tr><td>CM-8(a)(3)</td><td colspan="2">opracowuje i dokumentuje wykaz elementów systemu informacyjnego, który jest na poziomie szczegółowości uznanym za niezbędny do śledzenia i raportowania;</td></tr>
<tr><td rowspan="2">CM-8(a)(4)</td><td>CM-8(a)(4)[1]</td><td>określa informacje uważane za niezbędne do osiągnięcia skutecznej odpowiedzialności za elementy systemu informacyjnego;</td></tr>
<tr><td>CM-8(a)(4)[2]</td><td>opracowuje i dokumentuje wykaz składników systemu informacyjnego, który zawiera informacje określone przez organizację, uznane za niezbędne do osiągnięcia skutecznej rozliczalności komponentów systemu informacyjnego;</td></tr>
<tr><td rowspan="2">CM-8(b)</td><td>CM-8(b)[1]</td><td colspan="2">określa częstotliwość przeglądów i aktualizacji wykazu składników systemu informacyjnego; oraz</td></tr>
<tr><td>CM-8(b)[2]</td><td colspan="2">dokonuje przeglądu i aktualizacji spisów składników systemu informacyjnego z częstotliwością określoną przez organizację.</td></tr>
<tr><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:

Sprawdź: [wybierz spośród: Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; rejestry inwentaryzacji systemu informacyjnego; przeglądy inwentaryzacyjne i aktualizacja rejestrów; inne odpowiednie dokumenty lub rejestry].

Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za inwentaryzację elementów systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci].

Test: [wybierz spośród: Procesy organizacyjne związane z opracowaniem i dokumentacją inwentaryzacji elementów systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające inwentaryzację elementów systemu informacyjnego].</td></tr>
</table>

CM-8(1)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *AKTUALIZACJE INSTALACJI / USUWANIA KOMPONENTÓW***	
	CEL OCENY: *Ustalić, czy organizacja aktualizuje spis komponentów systemu informacyjnego, jako integralną część:*	
	CM-8(1)[1]	*instalacji komponentów;*
	CM-8(1)[2]	*usuwania komponentów; oraz*
	CM-8(1)[3]	*aktualizacji systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; rejestry inwentaryzacji systemu informacyjnego; przeglądy inwentaryzacyjne i aktualizacja rejestrów; dokumentacja zainstalowanych komponentów; dokumentacja demontażu komponentów; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aktualizację spisu komponentów systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące aktualizacji inwentaryzacji komponentów systemu informacyjnego; zautomatyzowane mechanizmy realizujące inwentaryzację komponentów systemu informacyjnego].	

CM-8(2)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNE UTRZYMANIE***	
	CEL OCENY: *Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy do prowadzenia ewidencji składników systemu informacyjnego, który jest:*	
	CM-8(2)[1]	*aktualny;*
	CM-8(2)[2]	*kompletny;*
	CM-8(2)[3]	*dokładny; oraz*
	CM-8(2)[4]	*łatwo dostępny.*

CM-8(2)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNE UTRZYMANIE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; plan zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry inwentaryzacji systemu informacyjnego; rejestry zabezpieczeń zmian; zapisy dotyczące konserwacji systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie zautomatyzowanymi mechanizmami wdrażania inwentaryzacji komponentów systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z prowadzeniem inwentaryzacji komponentów systemu informacyjnego; zautomatyzowane mechanizmy wdrażania inwentaryzacji komponentów systemu informacyjnego].

CM-8(3)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNE WYKRYWANIE KOMPONENTÓW NIEAUTORYZOWANYCH***			
	CEL OCENY: *Określić, czy organizacja:*			
	CM-8(3)(a)	**CM-8(3)(a)[1]**	*określa częstotliwość stosowania mechanizmów automatycznych w celu wykrycia nieautoryzowanych obecności:*	
			CM-8(3)(a)[1][a]	*komponentów sprzętowych w systemie informacyjnym;*
			CM-8(3)(a)[1][b]	*komponentów oprogramowania w systemie informacyjnym;*
			CM-8(3)(a)[1][c]	*komponentów oprogramowania sprzętowego w systemie informacyjnym;*
		CM-8(3)(a)[2]	*wykorzystuje ze zdefiniowaną przez organizację częstotliwością, automatyczne mechanizmy wykrywania obecności nieautoryzowanych:*	

<table>
<tr><th colspan="5">CM-8(3) INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | AUTOMATYCZNE WYKRYWANIE KOMPONENTÓW NIEAUTORYZOWANYCH</th></tr>
<tr><td rowspan="8"></td><td rowspan="3"></td><td rowspan="3"></td><td>CM-8(3)(a)[2][a]</td><td>komponentów sprzętowych w systemie informacyjnym;</td></tr>
<tr><td>CM-8(3)(a)[2][b]</td><td>komponentów oprogramowania w systemie informacyjnym;</td></tr>
<tr><td>CM-8(3)(a)[2][c]</td><td>komponentów oprogramowania sprzętowego w systemie informacyjnym;</td></tr>
<tr><td rowspan="4">CM-8(3)(b)</td><td>CM-8(3)(b)[1]</td><td colspan="2">definiuje personel lub role, które należy powiadomić w przypadku wykrycia nieautoryzowanych komponentów;</td></tr>
<tr><td rowspan="3">CM-8(3)(b)[2]</td><td colspan="2">wykonuje jedną lub więcej z poniższych czynności w przypadku wykrycia nieautoryzowanych komponentów:</td></tr>
<tr><td>CM-8(3)(b)[2][a]</td><td>dezaktywuje dostęp do sieci przez takie komponenty;</td></tr>
<tr><td>CM-8(3)(b)[2][b]</td><td>izoluje te komponenty; i/lub</td></tr>
<tr><td colspan="3">CM-8(3)(b)[2][c]</td><td>powiadamia personel lub role określone przez organizację.</td></tr>
<tr><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:

Sprawdź: [wybierz spośród: Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry inwentaryzacji systemu informacyjnego; ostrzeżenia/zawiadomienia o nieautoryzowanych komponentach w systemie informacyjnym; zapisy z monitoringu systemu informacyjnego; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za zarządzanie zautomatyzowanymi mechanizmami wdrażania mechanizmów wykrywania nieautoryzowanych elementów w systemie informacyjnym; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów].</td></tr>
</table>

CM-8(3)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNE WYKRYWANIE KOMPONENTÓW NIEAUTORYZOWANYCH***
	Test: [*wybierz spośród:* Procesy organizacyjne wykrywania nieautoryzowanych komponentów systemu informacyjnego; zautomatyzowane mechanizmy detekcji nieautoryzowanych komponentów systemu informacyjnego].

CM-8(4)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *INFORMACJE O ODPOWIEDZIALNOŚCI I ROZLICZALNOŚCI***	
	CEL OCENY: *Ustalenie, czy organizacja zawiera w wykazie informacji o komponentach systemu informacyjnego sposób identyfikacji osób odpowiedzialnych i rozliczanych za administrowanie tymi komponentami poprzez podanie:*	
	CM-8(4)[1]	*nazwiska;*
	CM-8(4)[2]	*stanowiska; i/lub*
	CM-8(4)[3]	*roli.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; rejestry inwentaryzacji systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie Inwentaryzacją komponentów systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z prowadzeniem inwentaryzacji komponentów systemu informacyjnego; zautomatyzowane mechanizmy wdrażania inwentaryzacji komponentów systemu informacyjnego].	

CM-8(5)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *BRAK DUPLIKACJI KOMPONENTÓW***
	CEL OCENY: *Ustalenie, czy organizacja sprawdza, czy żaden komponent autoryzowanego systemu informacyjnego nie jest duplikowany w wykazach komponentów innych systemów informacyjnych.*

CM-8(5)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *BRAK DUPLIKACJI KOMPONENTÓW***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; rejestry inwentaryzacji systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za inwentaryzację systemu informacyjnego; personel organizacji odpowiedzialny za definiowanie elementów składowych w autoryzowanym systemie informacyjnym; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z prowadzeniem inwentaryzacji komponentów systemu informacyjnego; zautomatyzowane mechanizmy wdrażania inwentaryzacji komponentów systemu informacyjnego].

CM-8(6)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *OCENA KONFIGURACJI / ZATWIERDZONE ODSTĘPSTWA***	
	CEL OCENY: *Ustalić, czy organizacja uwzględnia w inwentaryzacji komponentów systemu informacyjnego wszelkie:*	
	CM-8(6)[1]	*dokonane konfiguracje komponentów; oraz*
	CM-8(6)[2]	*zatwierdzone odchylenia od obecnie stosowanych konfiguracji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry inwentaryzacji systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie inwentaryzacją i oceną elementów systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z prowadzeniem inwentaryzacji komponentów systemu informacyjnego; zautomatyzowane mechanizmy wdrażania inwentaryzacji komponentów systemu informacyjnego].	

CM-8(7)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *SCENTRALIZOWANE REPOZYTORIUM***
	CEL OCENY: *Ustalić, czy organizacja zapewnia scentralizowane repozytorium na potrzeby inwentaryzacji elementów systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu informacyjnego; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; repozytorium inwentaryzacji systemu informacyjnego; rejestry inwentaryzacji systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie inwentaryzacją elementów systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące inwentaryzację komponentów systemu informacyjnego w scentralizowanym repozytorium].

CM-8(8)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNE MONITOROWANIE LOKALIZACJI***
	CEL OCENY: *Ustalenie, czy organizacja stosuje zautomatyzowane mechanizmy wspomagające monitorowanie elementów systemu informacyjnego według lokalizacji geograficznej.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu informacyjnego; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry inwentaryzacji systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie inwentaryzacją elementów systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów].

CM-8(8)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNE MONITOROWANIE LOKALIZACJI***
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażania inwentaryzacji komponentów systemu informacyjnego; zautomatyzowane mechanizmy wspomagające monitorowanie komponentów systemu informacyjnego według lokalizacji geograficznej].

CM-8(9)	**INWENTARYZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW***		
	CEL OCENY: *Określić, czy organizacja:*		
	CM-8(9)(a)	**CM-8(9)(a)[1]**	*definiuje pozyskane komponenty systemu informacyjnego, które mają być przypisane do systemu informacyjnego; oraz*
		CM-8(9)(a)[2]	*przypisuje zdefiniowane przez organizację pozyskane komponenty systemu informacyjnego do systemu informacyjnego organizacji; oraz*
	CM-8(9)(b)	*otrzymuje potwierdzenie od właściciela systemu informacyjnego o wykonaniu zlecenia.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące inwentaryzacji komponentów systemu informacyjnego; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; potwierdzenia przydziału elementów systemu informacyjnego; rejestry inwentaryzacji systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie inwentaryzacją elementów systemu informacyjnego; właściciel systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne przydzielania komponentów do systemów; procesy organizacyjne zatwierdzające przypisanie komponentów do systemów; zautomatyzowane mechanizmy realizujące przydzielanie nabytych komponentów do systemu informacyjnego; zautomatyzowane mechanizmy realizujące zatwierdzanie przydzielania nabytych komponentów do systemu informacyjnego].		

CM-9	**PLAN ZARZĄDZANIA KONFIGURACJĄ**		
	CEL OCENY: *Ustalić, czy organizacja opracowuje, dokumentuje i wdraża plan zarządzania konfiguracją systemu informacyjnego, który:*		
	CM-9(a)	**CM-9(a)[1]**	*definiuje role;*
		CM-9(a)[2]	*opisuje odpowiedzialności;*
		CM-9(a)[3]	*uwzględnia procesy i procedury zarządzania konfiguracją;*
	CM-9(b)	*ustanawia procesy:*	
		CM-9(b)[1]	*identyfikacji elementów konfiguracji w całym cyklu życia systemu (SDLC);*
		CM-9(b)[2]	*zarządzania konfiguracją elementów konfiguracyjnych;*
	CM-9(c)	**CM-9(c)[1]**	*definiujące pozycje konfiguracyjne systemu informacyjnego;*
		CM-9(c)[2]	*umieszczające elementy konfiguracyjne w zarządzaniu konfiguracją;*
	CM-9(d)	*chroni plan zarządzania konfiguracją przed nieuprawnionym:*	
		CM-9(d)[1]	*ujawnieniem; oraz*
		CM-9(d)[2]	*modyfikacją.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące planu zarządzania konfiguracją; plan zarządzania konfiguracją; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za opracowywanie planu zarządzania konfiguracją; personel organizacji odpowiedzialny za realizację i zarządzanie procesami określonymi w planie zarządzania konfiguracją; personel organizacji odpowiedzialny za ochronę planu zarządzania konfiguracją; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci].		

CM-9	**PLAN ZARZĄDZANIA KONFIGURACJĄ**
	Test: [*wybierz spośród:* Procesy organizacyjne związane z opracowaniem i dokumentacją planu zarządzania konfiguracją; procesy organizacyjne związane z identyfikacją i zarządzaniem elementami konfiguracji; procesy organizacyjne związane z ochroną planu zarządzania konfiguracją; zautomatyzowane mechanizmy wdrażania planu zarządzania konfiguracją; zautomatyzowane mechanizmy zarządzania elementami konfiguracji; zautomatyzowane mechanizmy ochrony planu zarządzania konfiguracją].

CM-9(1)	**PLAN ZARZĄDZANIA KONFIGURACJĄ | *PRZYPISANIE ODPOWIEDZIALNOŚCI***
	CEL OCENY: *Ustalić, czy organizacja przypisuje odpowiedzialność za opracowanie procesu zarządzania konfiguracją personelowi organizacji, który nie jest bezpośrednio zaangażowany w rozwój systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące odpowiedzialności za tworzenie procesu zarządzania konfiguracją; plan zarządzania konfiguracją; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za rozwój procesu zarządzania konfiguracją; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CM-10	**OGRANICZENIA W UŻYCIU OPROGRAMOWANIA**	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-10(a)	*korzysta z oprogramowania i związanej z nim dokumentacji zgodnie z umowami i prawami autorskimi;*
	CM-10(b)	*śledzi korzystanie z oprogramowania i związanej z nim dokumentacji chronionej licencjami ilościowymi, w celu kontroli kopiowania i rozpowszechniania; oraz*
	CM-10(c)	*kontroluje i dokumentuje korzystanie z technologii wymiany plików w systemie peer-to-peer w celu zapewnienia, że możliwość ta nie jest wykorzystywana do nieautoryzowanego rozpowszechniania, wyświetlania, wykonywania lub reprodukcji utworów chronionych prawem autorskim.*

CM-10	**OGRANICZENIA W UŻYCIU OPROGRAMOWANIA**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury dotyczące ograniczeń w użyciu oprogramowania; plan zarządzania konfiguracją; plan bezpieczeństwa; umowy licencyjne na oprogramowanie i prawa autorskie; dokumentacja licencyjna witryny; lista ograniczeń w użyciu oprogramowania; raporty z monitorowania licencji na oprogramowanie; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacji obsługujący, używający i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za zarządzanie licencjami na oprogramowanie]. **Test**: [*wybierz spośród:* Proces organizacyjny monitorowania korzystania z oprogramowania chronionego licencjami ilościowymi; proces organizacyjny kontroli/dokumentacji korzystania z technologii wymiany plików w systemie peer-to-peer; zautomatyzowane mechanizmy wdrażania monitorowania licencji na oprogramowanie; zautomatyzowane mechanizmy wdrażania i kontroli korzystania z technologii wymiany plików w systemie peer-to-peer].

CM-10(1)	**OGRANICZENIA W UŻYCIU OPROGRAMOWANIA | *OPROGRAMOWANIE OTWARTE (OPEN SOURCE)***	
	CEL OCENY: *Określić, czy organizacja:*	
	CM-10(1)[1]	*określa ograniczenia w korzystaniu z oprogramowania otwartego (open source); oraz*
	CM-10(1)[2]	*ustanawia organizacyjnie zdefiniowane ograniczenia w zakresie korzystania z oprogramowania otwartego (open source).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedura dotycząca ograniczeń w korzystaniu z oprogramowania otwartego (open source); plan zarządzania konfiguracją; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ustanawianie i egzekwowanie ograniczeń w korzystaniu z oprogramowania otwarte (open source); personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci].	

CM-10(1)	**OGRANICZENIA W UŻYCIU OPROGRAMOWANIA | *OPROGRAMOWANIE OTWARTE (OPEN SOURCE)***
	Test: [*wybierz spośród:* Proces organizacyjny ograniczania korzystania z oprogramowania otwartego (open source); zautomatyzowane mechanizmy wprowadzające ograniczenia w korzystaniu z oprogramowania otwartego (open source)].

CM-11	**OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA**		
	CEL OCENY: *Określić, czy organizacja:*		
	CM-11(a)	**CM-11(a)[1]**	*definiuje zasady regulujące instalację oprogramowania przez użytkowników;*
		CM-11(a)[2]	*wprowadza zdefiniowane przez organizację zasady regulujące instalację oprogramowania przez użytkowników;*
	CM-11(b)	**CM-11(b)[1]**	*definiuje metody egzekwowania zasad instalacji oprogramowania;*
		CM-11(b)[2]	*egzekwuje zasady instalacji oprogramowania za pomocą metod zdefiniowanych przez organizację;*
	CM-11(c)	**CM-11(c)[1]**	*definiuje częstotliwość monitorowania przestrzegania zasad i zgodności z przepisami; oraz*
		CM-11(c)[2]	*monitoruje przestrzeganie polityki z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury związane z oprogramowaniem zainstalowanym przez użytkownika; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista zasad dotyczących oprogramowania instalowanego przez użytkownika; zapisy z monitoringu systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry; strategia ciągłości monitorowania].		

CM-11	**OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie oprogramowaniem zainstalowanym przez użytkownika; personel organizacji obsługujący, korzystający i/lub utrzymujący system informacyjny; personel organizacji monitorujący zgodność z polityką w zakresie oprogramowania zainstalowanego przez użytkownika; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące oprogramowania instalowanego przez użytkownika w systemie informacyjnym; zautomatyzowane mechanizmy egzekwujące zasady/metody dotyczące instalacji oprogramowania przez użytkowników; zautomatyzowane mechanizmy monitorujące zgodność z polityką].

CM-11(1)	**OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA | *OSTRZEGANIE O NIEAUTORYZOWANYCH INSTALACJACH***	
	CEL OCENY: *Określić, czy:*	
	CM-11(1)[1]	*organizacja określa personel lub role, które mają być ostrzegane w przypadku wykrycia nieautoryzowanej instalacji oprogramowania; oraz*
	CM-11(1)[2]	*system informacyjny alarmuje zdefiniowany przez organizację personel lub role w przypadku wykrycia nieautoryzowanej instalacji oprogramowania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury związane z oprogramowaniem zainstalowanym przez użytkownika; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie oprogramowaniem zainstalowanym przez użytkownika; personel organizacji obsługujący, korzystający i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów].	

CM-11(1)	**OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA | *OSTRZEGANIE O NIEAUTORYZOWANYCH INSTALACJACH***
	Test: [*wybierz spośród:* Procesy organizacyjne dotyczące oprogramowania instalowanego przez użytkownika w systemie informacyjnym; zautomatyzowane mechanizmy ostrzegania personelu/roli w przypadku wykrycia nieautoryzowanej instalacji oprogramowania].

CM-11(2)	**OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA | *ZABRONIONA INSTALACJA BEZ POSIADANIA STOSOWNYCH UPRAWNIEŃ***
	CEL OCENY: *Ustalić, czy system informacyjny zabrania instalowania oprogramowania przez użytkownika nieposiadającego statusu użytkownika uprzywilejowanego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka zarządzania konfiguracją; procedury związane z oprogramowaniem zainstalowanym przez użytkownika; plan zarządzania konfiguracją; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; alarmy/zgłoszenia dotyczące instalacji nieautoryzowanego oprogramowania; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie oprogramowaniem zainstalowanym przez użytkownika; personel organizacji obsługujący, korzystający i/lub utrzymujący system informacyjny]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące oprogramowania instalowanego przez użytkownika w systemie informacyjnym; zautomatyzowane mechanizmy zabraniające instalowania oprogramowania przez użytkownika nieposiadającego statusu użytkownika uprzywilejowanego (np. kontrola dostępu)].

KATEGORIA CP - PLANOWANIE AWARYJNE / CIĄGŁOŚĆ DZIAŁANIA

CP-1	**POLITYKA I PROCEDURY PLANOWANIA CIĄGŁOŚCI DZIAŁANIA**			
	CEL OCENY: *Określić, czy organizacja:*			
	CP-1(a)(1)	**CP-1(a)(1)[1]**	*opracowuje i dokumentuje politykę planowania awaryjnego, w odniesieniu do:*	
			CP-1(a)(1)[1][a]	*celu*
			CP-1(a)(1)[1][b]	*zakresu stosowania;*
			CP-1(a)(1)[1][c]	*ról;*
			CP-1(a)(1)[1][d]	*odpowiedzialności;*
			CP-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			CP-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			CP-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		CP-1(a)(1)[2]	*określa personel lub role, wśród których ma być rozpowszechniana polityka planowania awaryjnego;*	
		CP-1(a)(1)[3]	*rozpowszechnia politykę planowania awaryjnego wśród personelu lub ról zdefiniowanych przez organizację;*	
	CP-1(a)(2)	**CP-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrożenie polityki planowania awaryjnego i związanych z nią środków bezpieczeństwa w zakresie planowania awaryjnego;*	
		CP-1(a)(2)[2]	*określa personel lub role, wśród których procedury te mają być rozpowszechniane;*	
		CP-1(a)(2)[3]	*rozpowszechnia te procedury wśród określonego przez organizację personelu lub na określonych stanowiskach;*	
	CP-1(b)(1)	**CP-1(b)(1)[1]**	*organizacja określa częstotliwość przeglądów i aktualizacji aktualnej polityki w zakresie planowania awaryjnego;*	

CP-1	**POLITYKA I PROCEDURY PLANOWANIA CIĄGŁOŚCI DZIAŁANIA**		
		CP-1(b)(1)[2]	*dokonuje przeglądu i aktualizacji aktualnej polityki planowania awaryjnego z częstotliwością określoną przez organizację;*
	CP-1(b)(2)	**CP-1(b)(2)[1]**	*określa częstotliwość przeglądów i aktualizacji bieżących procedur planowania awaryjnego; oraz*
		CP-1(b)(2)[2]	*dokonuje przeglądu i aktualizacji bieżących procedur planowania awaryjnego z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury planowania ciągłości działania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie awaryjne; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

CP-2	**PLAN CIĄGŁOŚCI DZIAŁANIA**			
	CEL OCENY: *Określić, czy organizacja:*			
	CP-2(a)	*opracowuje i dokumentuje plan ciągłości działania dotyczący systemu informacyjnego, który:*		
		CP-2(a)(1)	*określa istotne misje i funkcje biznesowe oraz związane z nimi działania w sytuacjach awaryjnych;*	
		CP-2(a)(2)	**CP-2(a)(2)[1]**	*zapewnia cele w zakresie odzyskiwania środków;*
			CP-2(a)(2)[2]	*zapewnia priorytety w zakresie odbudowy;*
			CP-2(a)(2)[3]	*zapewnia metryki;*
		CP-2(a)(3)	**CP-2(a)(3)[1]**	*adresuje role awaryjne;*
			CP-2(a)(3)[2]	*wskazuje rolę odpowiedzialności w sytuacjach awaryjnych;*
			CP-2(a)(3)[3]	*wskazuje osoby, z przydzielonymi danymi kontaktowymi;*

CP-2	**PLAN CIĄGŁOŚCI DZIAŁANIA**			
		CP-2(a)(4)	*dotyczy utrzymania istotnych misji i funkcji biznesowych pomimo zakłóceń w systemie informacyjnym, naruszenia lub awarii;*	
		CP-2(a)(5)	*dotyczy ewentualnego, pełnego przywrócenia systemu informacyjnego bez pogorszenia pierwotnie zaplanowanych i wdrożonych zabezpieczeń;*	
		CP-2(a)(6)	**CP-2(a)(6)[1]**	*definiuje personel lub role do przeglądu i zatwierdzenia planu ciągłości działań systemu informacyjnego;*
			CP-2(a)(6)[2]	*jest poddawany przeglądowi i zatwierdzany przez personel określony przez organizację lub rolę;*
	CP-2(b)	**CP-2(b)[1]**	*definiuje kluczowy personel awaryjny (identyfikowany po nazwisku i/lub roli) oraz elementy organizacyjne, do których mają być dystrybuowane kopie planu ciągłości działania;*	
		CP-2(b)[2]	*dystrybuuje kopie planu ciągłości działania do zdefiniowanego przez organizację kluczowego personelu i struktur organizacyjnych;*	
	CP-2(c)	*koordynuje działania związane z planowaniem ciągłości działania z czynnościami związanymi z obsługą incydentów;*		
	CP-2(d)	**CP-2(d)[1]**	*określa częstotliwość przeglądów planu ciągłości działania systemu informacyjnego;*	
		CP-2(d)[2]	*dokonuje przeglądu planu ciągłości działania z częstotliwością określoną przez organizację;*	
	CP-2(e)	*aktualizuje plan ciągłości działania w celu:*		
		CP-2(e)[1]	*uwzględnienia zmian w systemie informacyjnym lub środowisku działania;*	
		CP-2(e)[2]	*uwzględnienia problemów napotkanych podczas wdrażania, realizacji i testowania planu;*	
	CP-2(f)	**CP-2(f)[1]**	*definiowania kluczowego personelu awaryjnego (identyfikowanego na podstawie nazwy i/lub roli) oraz elementów organizacyjnych, którym mają być przekazywane informacje o zmianach w planie ciągłości działania;*	

CP-2	**PLAN CIĄGŁOŚCI DZIAŁANIA**		
		CP-2(f)[2]	*uzgadniania zmiany w planie ciągłości działania ze zdefiniowanym w organizacji kluczowym personelem i elementami organizacyjnymi w sytuacjach awaryjnych; oraz*
	CP-2(g)	*ochrony planu ciągłości działania przed nieautoryzowanym ujawnieniem i modyfikacją.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące planu ciągłości działania systemu informacyjnego; plan ciągłości działania; plan bezpieczeństwa; potwierdzenia przeglądów i aktualizacji planu ciągłości działania systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania i realizację planów; personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z opracowywaniem, przeglądem, aktualizacją i ochroną planu ciągłości działania; zautomatyzowane mechanizmy opracowywania, przeglądu, aktualizacji i/lub ochrony plan ciągłości działania].		

CP-2(1)	**PLAN CIĄGŁOŚCI DZIAŁANIA | *KOORDYNACJA Z POWIĄZANYMI PLANAMI***
	CEL OCENY: *Ustalić, czy organizacja koordynuje rozwój planu ciągłości działania z jednostkami organizacyjnymi odpowiedzialnymi za związane z nim plany.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące planu ciągłości działania systemu informacyjnego; plan ciągłości działania; plan awaryjny; plan odzyskiwania po awarii; plan ciągłości operacji; plan komunikacji kryzysowej; plan ochrony infrastruktury krytycznej; plany reagowania na incydenty komputerowe; plan przeciwdziałania zagrożeniom wewnętrznym; plan ewakuacji; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania i realizację planów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel odpowiedzialny za powiązane plany].

CP-2(2)	**PLAN CIĄGŁOŚCI DZIAŁANIA | *PLANOWANIE ZDOLNOŚCI FUNKCJONOWANIA***	
	CEL OCENY: *Określić, czy organizacja prowadzi planowanie Zdolności funkcjonowania, a także, czy podczas operacji awaryjnych istnieją niezbędne zdolności:*	
	CP-2(2)[1]	*przetwarzanie informacji;*
	CP-2(2)[2]	*komunikacji; oraz*
	CP-2(2)[3]	*wsparcia środowiskowego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące planu ciągłości działania systemu informacyjnego; plan ciągłości działania; dokumenty planowania Zdolności funkcjonowania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania i realizację planów; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

CP-2(3)	**PLAN CIĄGŁOŚCI DZIAŁANIA | *WZNAWIANIE PODSTAWOWYCH DZIAŁAŃ / FUNKCJI BIZNESOWYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-2(3)[1]	*określa okres czasu, w którym należy zaplanować wznowienie podstawowych misji i funkcji biznesowych po aktywowaniu planu ciągłości działania; oraz*
	CP-2(3)[2]	*planuje wznowienia istotnych misji i funkcji biznesowych w określonym przez organizację okresie czasu aktywacji planu ciągłości działania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące planu ciągłości działania systemu informacyjnego; plan ciągłości działania; plan bezpieczeństwa; ocena wpływu na działalność gospodarczą; inne powiązane plany; inne odpowiednie dokumenty lub rejestry].	

CP-2(3)	**PLAN CIĄGŁOŚCI DZIAŁANIA | *WZNAWIANIE PODSTAWOWYCH DZIAŁAŃ / FUNKCJI BIZNESOWYCH***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania i realizację planów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące wznowieniu misji i funkcji biznesowych].

CP-2(4)	**PLAN CIĄGŁOŚCI DZIAŁANIA | *PRZYWRÓCENIE DZIAŁANIA WSZYSTKICH FUNKCJI BIZNESOWYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-2(4)[1]	*określa okres czasu, w którym należy zaplanować wznowienie wszystkich misji i funkcji biznesowych w wyniku aktywacji planu ciągłości działania; oraz*
	CP-2(4)[2]	*planuje wznowienie wszystkich misji i funkcji biznesowych w określonym przez organizację okresie czasu od momentu aktywacji planu ciągłości działania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące planu ciągłości działania systemu informacyjnego; plan ciągłości działania; plan bezpieczeństwa; ocena wpływu na działalność gospodarczą; inne powiązane plany; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania i realizację planów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące wznowieniu misji i funkcji biznesowych].	

CP-2(5)	**PLAN CIĄGŁOŚCI DZIAŁANIA | *KONTYNUACJA NIEZBĘDNYCH DZIAŁAŃ / FUNKCJI BIZNESOWYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-2(5)[1]	*planuje kontynuację podstawowych misji i funkcji biznesowych z minimalną ciągłością operacyjną lub bez jej utraty; oraz*
	CP-2(5)[2]	*utrzymuje tę ciągłość operacyjną do czasu pełnego przywrócenia systemu informacyjnego w miejscach pierwotnego przetwarzania i/lub składowania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące planu ciągłości działania systemu informacyjnego; plan ciągłości działania; ocena wpływu na działalność gospodarczą; umowy w sprawie pierwotnego miejsca przetwarzania; umowy w sprawie pierwotnego miejsca składowania; umowy w sprawie zapasowego miejsca przetwarzania; umowy w sprawie zapasowego miejsca przechowywania kopii; dokumentacja przeprowadzonych testów planu ciągłości działania; wyniki testów planu ciągłości działania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania i realizację planów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z kontynuacją misji i funkcjami biznesowymi].	

CP-2(6)	**PLAN CIĄGŁOŚCI DZIAŁANIA | *PROCESY ALTERNATYWNE / ZAPASOWE MIEJSCA PRZETWARZANIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-2(6)[1]	*planuje przeniesienie niezbędnych procesów funkcjonowania i funkcji biznesowych do alternatywnych miejsc przetwarzania i / lub przechowywania z minimalną ciągłością operacyjną lub bez jej utraty; oraz*
	CP-2(6)[2]	*utrzymuje tę ciągłość operacyjną do momentu przywrócenia systemu informacyjnego do pierwotnych miejsc przetwarzania i/lub składowania.*

CP-2(6)	**PLAN CIĄGŁOŚCI DZIAŁANIA | *PROCESY ALTERNATYWNE / ZAPASOWE MIEJSCA PRZETWARZANIA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące planu ciągłości działania systemu informacyjnego; plan ciągłości działania; ocena wpływu na działalność gospodarczą; Umowy w sprawie zapasowego miejsca przetwarzania; umowy w sprawie zapasowego miejsca przechowywania kopii; dokumentacja przeprowadzonych testów planu ciągłości działania; dokumentacja przeprowadzonych testów planu ciągłości działania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania i realizację planów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z przeniesieniem istotnych misji i funkcji biznesowych do alternatywnych miejsc przetwarzania/składowania].

CP-2(7)	**PLAN CIĄGŁOŚCI DZIAŁANIA | *KOORDYNACJA Z USŁUGODAWCAMI ZEWNĘTRZNYMI***
	CEL OCENY: *Ustalić, czy organizacja koordynuje własny plan ciągłości działań z planem ciągłości działań usługodawców zewnętrznych, aby zapewnić możliwość spełnienia wymagań dotyczących ciągłości działań w sytuacjach awaryjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące planu ciągłości działania systemu informacyjnego; plan ciągłości działania; plan ciągłości działania z zewnętrznymi usługodawcami; umowa gwarancji świadczenia usług (SLA); plan bezpieczeństwa; wymagania dotyczące planu ciągłości działania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania i realizację planów; usługodawcy zewnętrzni; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CP-2(8)	**PLAN CIĄGŁOŚCI DZIAŁANIA | *IDENTYFIKACJA ZASOBÓW KRYTYCZNYCH***
	CEL OCENY: *Ustalenie, czy organizacja identyfikuje krytyczne aktywa systemu informacyjnego wspomagające istotne misje i funkcje biznesowe.*

CP-2(8)	**PLAN CIĄGŁOŚCI DZIAŁANIA | *IDENTYFIKACJA ZASOBÓW KRYTYCZNYCH***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące planu ciągłości działania systemu informacyjnego; plan ciągłości działania; ocena wpływu na działalność gospodarczą; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania i realizację planów; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CP-3	**SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA**		
	CEL OCENY: *Określić, czy organizacja:*		
	CP-3(a)	**CP-3(a)[1]**	*ustala okres czasu, w którym szkolenie w zakresie planowania ciągłości działania na wypadek awarii ma być przeprowadzone dla użytkowników systemu informacyjnego, którzy przyjmują na siebie rolę lub odpowiedzialność w sytuacjach awaryjnych;*
		CP-3(a)[2]	*zapewnia szkolenie w zakresie planowania ciągłości działań na wypadek awarii dla użytkowników systemu informacyjnego zgodnie z przypisanymi rolami i obowiązkami w określonym przez organizację okresie czasu, w którym przyjmują rolę lub odpowiedzialność w sytuacjach awaryjnych;*
	CP-3(b)	*prowadzi szkolenia w zakresie planowania ciągłości działań na wypadek awarii dla użytkowników systemu informacyjnego zgodnie z przypisanymi rolami i obowiązkami, gdy wymagają tego zmiany w systemie informacyjnym;*	
	CP-3(c)	**CP-3(c)[1]**	*określa częstotliwość przeprowadzania szkoleń w sytuacjach awaryjnych po wystąpieniu takich zdarzeń; oraz*
		CP-3(c)[2]	*zapewnia użytkownikom systemów informacyjnych szkolenia w sytuacjach awaryjnych zgodne z przydzielonymi rolami i obowiązkami z częstotliwością określoną przez organizację.*

CP-3	**SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* polityka planowania awaryjnego; procedury dotyczące szkolenia w zakresie planowania ciągłości działania; plan ciągłości działania; program szkolenia w zakresie planowania ciągłości działania; dokumentacja szkoleniowa w zakresie planowania ciągłości działania; plan bezpieczeństwa; rejestry przeprowadzenia szkolenia w zakresie planowania ciągłości działania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem awaryjnym, realizacją planów i szkoleniami; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące szkoleń w sytuacjach awaryjnych].

CP-3(1)	**SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA | *WYDARZENIA SYMULOWANE***
	CEL OCENY: *Ustalenie, czy organizacja wprowadza symulowane zdarzenia do szkolenia w zakresie planowania ciągłości działania, celem ułatwienia skutecznego reagowania personelu w sytuacjach kryzysowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące szkolenia w zakresie planowania ciągłości działania; plan ciągłości działania; program szkolenia w zakresie planowania ciągłości działania; dokumentacja szkoleniowa w zakresie planowania ciągłości działania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem awaryjnym, realizacją planów i szkoleniami; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące szkoleń w sytuacjach awaryjnych; zautomatyzowane mechanizmy symulacji zdarzeń awaryjnych].

CP-3(2)	**SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA | *ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE***
	CEL OCENY: *Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy zapewniające dokładniejsze i bardziej realistyczne środowisko szkolenie w zakresie planowania ciągłości działania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące szkolenia w zakresie planowania ciągłości działania; plan ciągłości działania; program szkolenia w zakresie planowania ciągłości działania; dokumentacja szkoleniowa w zakresie planowania ciągłości działania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem awaryjnym, realizacją planów i szkoleniami; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące szkoleń w sytuacjach awaryjnych; zautomatyzowane mechanizmy dostarczania środowisk szkoleniowych w zakresie planowania ciągłości działania].

CP-4	**TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA**		
	CEL OCENY: *Określić, czy organizacja:*		
	CP-4(a)	**CP-4(a)[1]**	*definiuje testy w celu określenia skuteczności planu ciągłości działania i gotowości organizacyjnej do jego realizacji;*
		CP-4(a)[2]	*definiuje częstotliwość testowania planu ciągłości działania systemu informacyjnego;*
		CP-4(a)[3]	*testuje plan ciągłości działań systemu informacyjnego z określoną przez organizację częstotliwością, wykorzystując określone przez organizację testy w celu określenia skuteczności planu i gotowości organizacyjnej do wykonania planu;*
	CP-4(b)	*dokonuje przeglądu wyników testów planu awaryjnego; oraz*	
	CP-4(c)	*w razie potrzeby inicjuje działania naprawcze.*	

CP-4	**TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące testowania planu ciągłości działania; plan ciągłości działania; plan bezpieczeństwa; dokumentacja dotycząca testów planu ciągłości działania; dokumentacja przeprowadzonych testów planu ciągłości działania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za testowanie planów awaryjnych, przegląd lub reagowanie na testy planów awaryjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z testowaniem planów awaryjnych; zautomatyzowane mechanizmy wspierające plany awaryjne i/lub testowanie planów awaryjnych].

CP-4(1)	**TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | *KOORDYNACJA Z POWIĄZANYMI PLANAMI***
	CEL OCENY: *Ustalić, czy organizacja koordynuje testowanie planu ciągłości działania z jednostkami organizacyjnymi odpowiedzialnymi za powiązane plany.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; polityka reagowania na incydenty; procedury dotyczące testowania planu ciągłości działania; dokumentacja przeprowadzonych testów planu ciągłości działania; plan ciągłości działania; plan awaryjny; plan odzyskiwania po awarii; plan ciągłości operacji; plan komunikacji kryzysowej; plan ochrony infrastruktury krytycznej; plany reagowania na incydenty komputerowe; plan ewakuacji; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za testowanie planów awaryjnych; personel organizacji; personel odpowiedzialny za powiązane plany; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CP-4(2)	**TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | *ZAPASOWE MIEJSCE PRZETWARZANIA***	
	CEL OCENY: *Ustalić, czy organizacja testuje plan awaryjny w zapasowym miejscu przetwarzania oraz:*	
	CP-4(2)(a)	*zapoznaje personel odpowiedzialny za ciągłość działania z obiektem i dostępnymi zasobami; oraz*
	CP-4(2)(b)	*ocenia możliwości zapasowego miejsca przetwarzania w celu wsparcia operacji awaryjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące testowania planu ciągłości działania; plan ciągłości działania; dokumentacja dotycząca testów planu ciągłości działania; dokumentacja przeprowadzonych testów planu ciągłości działania; umowy w sprawie zapasowego miejsca przetwarzania; umowa gwarancji świadczenia usług (SLA); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania i realizację planów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z testowaniem planów awaryjnych; zautomatyzowane mechanizmy wspierające plany awaryjne i/lub testowanie planów awaryjnych].	

CP-4(3)	**TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | *TESTOWANIE AUTOMATYCZNE***
	CEL OCENY: *Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy wszechstronnego i skutecznego testowania planu awaryjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące testowania planu ciągłości działania; plan ciągłości działania; zautomatyzowane mechanizmy wspomagające testowanie planu ciągłości działania; dokumentacja dotycząca testów planu ciągłości działania; dokumentacja przeprowadzonych testów planu ciągłości działania; inne odpowiednie dokumenty lub rejestry].

CP-4(3)	**TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | *TESTOWANIE AUTOMATYCZNE***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za testowanie planu ciągłości działania; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z testowaniem planów awaryjnych; zautomatyzowane mechanizmy wspomagające testowanie planów awaryjnych].

CP-4(4)	**TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | *PEŁNE ODZYSKIWANIE / ODTWARZANIE***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-4(4)[1]	*przeprowadza pełne przywrócenie systemu informacyjnego do pierwotnego stanu w ramach testowania planu awaryjnego; oraz*
	CP-4(4)[2]	*przeprowadza pełne odtworzenie systemu informacyjnego do pierwotnego stanu w ramach testowanie planu ciągłości działania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące odzyskiwania i odtwarzania systemu; plan ciągłości działania; dokumentacja dotycząca testów planu ciągłości działania; dokumentacja przeprowadzonych testów planu ciągłości działania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za testowanie planu ciągłości działania; personel organizacji odpowiedzialny za odzyskiwanie i odtwarzanie systemu; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z testowaniem planów awaryjnych; zautomatyzowane mechanizmy wspomagające testowanie planów awaryjnych; zautomatyzowane mechanizmy wspomagające odzyskiwanie i odtwarzanie systemu informacyjnego].	

CP-5	**AKTUALIZACJA PLANU CIĄGŁOŚCI DZIAŁANIA**
[Włączone do: CP-2].	

CP-6	**ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII**	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-6[1]	*ustanawia zapasowe miejsce przechowywania kopii wraz z niezbędnymi umowami umożliwiającymi przechowywanie i pobieranie informacji o kopii zapasowej; oraz*
	CP-6[2]	*zapewnia, że zapasowe miejsce przechowywania kopii zapewnia bezpieczeństwo informacji równoważne z tym, które zapewnia miejsce główne (podstawowe).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapasowego miejsce przechowywania kopii; plan ciągłości działania; umowy w sprawie zapasowego miejsca przechowywania kopii; umowy dotyczące głównego miejsca przechowywania kopii; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za plan ciągłości działania zapasowego miejsca przechowywania kopii; personel organizacji odpowiedzialny za odzyskiwanie systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie przechowywania i odzyskiwania informacji dotyczących kopii zapasowych systemów informacyjnych w zapasowym miejscu przechowywania kopii; zautomatyzowane mechanizmy wspomagające lub wdrażające przechowywanie i odzyskiwanie informacji dotyczących kopii zapasowych systemów informacyjnych w zapasowym miejscu przechowywania kopii].	

CP-6(1)	**ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | *ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ***
	CEL OCENY: *Ustalić, czy organizacja identyfikuje zapasowe miejsce przechowywania kopii, które jest odseparowane od głównego miejsca przechowywania w celu zmniejszenia podatności na tego samego rodzaju zagrożenia.*

CP-6(1)	**ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | *ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapasowego miejsce przechowywania kopii; plan ciągłości działania; zapasowe miejsce przechowywania kopii; umowy w sprawie zapasowego miejsca przechowywania kopii; umowy dotyczące głównego miejsca przechowywania kopii; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za plan ciągłości działania zapasowego miejsca przechowywania kopii; personel organizacji odpowiedzialny za odzyskiwanie systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CP-6(2)	**ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | *CZAS ODZYSKIWANIA / CELE PUNKTOWE***
	CEL OCENY: *Ustalić, czy organizacja konfiguruje zapasowe miejsce przechowywania kopii w celu ułatwienia operacji odzyskiwania zgodnie z czasami odzyskiwania oraz punktami odtwarzania danych (jak określono w planie awaryjnym systemu informacyjnego).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapasowego miejsce przechowywania kopii; plan ciągłości działania; zapasowe miejsce przechowywania kopii; umowy w sprawie zapasowego miejsca przechowywania kopii; konfiguracje zapasowego miejsca przechowywania kopii; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za testowanie planu ciągłości działania; personel organizacji odpowiedzialny za realizację planów związanych z testowaniem; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne testowania planu ciągłości działania; zautomatyzowane mechanizmy wspomagające realizację celów czasowych odzyskiwania / punktów odtworzenia].

CP-6(3)	**ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | *DOSTĘPNOŚĆ***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-6(3)[1]	*identyfikuje potencjalne problemy związane z dostępnością do zapasowego miejsca przechowywania kopii w przypadku zakłóceń lub katastrofy na całym obszarze; oraz*
	CP-6(3)[2]	*nakreśla wyraźne działania łagodzące dla takich potencjalnych problemów z dostępnością do zapasowego miejsca przechowywania kopii w przypadku zakłóceń lub katastrofy na całym obszarze.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapasowego miejsce przechowywania kopii; plan ciągłości działania; zapasowe miejsce przechowywania kopii; wykaz potencjalnych problemów z dostępnością do zapasowego miejsce przechowywania kopii; działania minimalizujące problemy związane z dostępnością do zapasowego miejsca przechowywania kopii; szacowanie ryzyka organizacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za plan ciągłości działania zapasowego miejsca przechowywania kopii; personel organizacji odpowiedzialny za odzyskiwanie systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

CP-7	**ZAPASOWE MIEJSCE PRZETWARZANIA**	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-7(a)	**CP-7(a)[1]** *definiuje procesy systemu informacyjnego wymagające ustanowienia zapasowego miejsca przetwarzania w celu umożliwienia przeniesienia i wznowienia tych procesów;*
		CP-7(a)[2] *definiuje okres czasu zgodny z czasami odzyskiwania i punktami odtworzenia danych (określonymi w planie awaryjnym systemu informacyjnego) na przekazanie/wznowienie operacji systemu informacyjnego zdefiniowanego przez organizację dla podstawowych misji/funkcji biznesowych;*

CP-7	**ZAPASOWE MIEJSCE PRZETWARZANIA**		
		CP-7(a)[3]	*ustanawia zapasowe miejsce przetwarzania wraz z niezbędnymi umowami umożliwiającymi przeniesienie i wznowienie operacji systemu informacyjnego zdefiniowanego przez organizację dla podstawowych misji/funkcji biznesowych, w określonym przez organizację okresie czasu, jeżeli podstawowe funkcje przetwarzania są niedostępne;*
	CP-7(b)	**CP-7(b)[1]**	*zapewnia dostępność sprzętu i materiałów niezbędnych do przeniesienia i wznowienia operacji w zapasowym miejscu przetwarzania; lub*
		CP-7(b)[2]	*zapewnia, że istnieją umowy wspierające dostawę do obiektu w określonym przez organizację okresie czasu na przeniesienie/wznowienie; oraz*
	CP-7(c)	*zapewnia, że zapasowe miejsce przetwarzania gwarantuje bezpieczeństwo informacji równoważne z tym, które zapewnia miejsce główne.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapasowego miejsca przetwarzania; plan ciągłości działania; umowy w sprawie zapasowego miejsca przetwarzania; umowy w sprawie głównego miejsca przetwarzania; zapasy sprzętu i materiałów eksploatacyjnych w zapasowym miejscu przetwarzania; umowy na wyposażenie i dostawy; umowa gwarancji świadczenia usług (SLA); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania i/lub organizację zapasowych miejsc pracy; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne odzyskiwania w zapasowym miejscu przetwarzania; zautomatyzowane mechanizmy wspierające i/lub wdrażające odzyskiwanie w zapasowym miejscu przetwarzania].		

CP-7(1)	**ZAPASOWE MIEJSCE PRZETWARZANIA | *ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ***
	CEL OCENY: *Ustalić, czy organizacja określiła zapasowe miejsce przetwarzania, które jest oddzielone od głównego miejsca przechowywania w celu zmniejszenia podatności na tego samego rodzaju zagrożenia.*

CP-7(1)	**ZAPASOWE MIEJSCE PRZETWARZANIA | *ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapasowego miejsca przetwarzania; plan ciągłości działania; zapasowe miejsce przetwarzania; umowy w sprawie zapasowego miejsca przetwarzania; umowy w sprawie głównego miejsca przetwarzania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania w zapasowym miejscu przetwarzania; personel organizacji odpowiedzialny za odzyskiwanie systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CP-7(2)	**ZAPASOWE MIEJSCE PRZETWARZANIA | *DOSTĘPNOŚĆ***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-7(2)[1]	*identyfikuje potencjalne problemy związane z dostępnością do zapasowego miejsca przetwarzania w przypadku zakłóceń lub katastrofy na całym obszarze; oraz*
	CP-7(2)[2]	*nakreśla wyraźne działania minimalizujące potencjalne problemy z dostępnością do zapasowego miejsca przetwarzania w przypadku zakłóceń lub katastrofy na całym obszarze.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapasowego miejsca przetwarzania; plan ciągłości działania; zapasowe miejsce przetwarzania; umowy w sprawie zapasowego miejsca przetwarzania; umowy w sprawie głównego miejsca przetwarzania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania w zapasowym miejscu przetwarzania; personel organizacji odpowiedzialny za odzyskiwanie systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

CP-7(3)	**ZAPASOWE MIEJSCE PRZETWARZANIA | *PRIORYTET USŁUG***
	CEL OCENY: *Ustalić, czy organizacja wdraża umowy w sprawie zapasowego miejsca przetwarzania, które zawierają postanowienia o pierwszeństwie usług zgodnie z wymaganiami dostępności organizacji (w tym czasów odzyskiwania określonych w planie awaryjnym systemu informacyjnego).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapasowego miejsca przetwarzania; plan ciągłości działania; umowy w sprawie zapasowego miejsca przetwarzania; umowa gwarancji świadczenia usług (SLA); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania w zapasowym miejscu przetwarzania; personel organizacji odpowiedzialny za odzyskiwanie systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za realizację transakcji nabycia / zawarcia umów].

CP-7(4)	**ZAPASOWE MIEJSCE PRZETWARZANIA | *GOTOWOŚĆ DO UŻYCIA***
	CEL OCENY: *Ustalić, czy organizacja przygotowuje zapasowe miejsce przetwarzania tak, aby było gotowe do użycia, jako miejsce operacyjne wspomagające istotne misje i funkcje biznesowe.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapasowego miejsca przetwarzania; plan ciągłości działania; zapasowe miejsce przetwarzania; umowy w sprawie zapasowego miejsca przetwarzania; konfiguracje zapasowego miejsce przetwarzania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania w zapasowym miejscu przetwarzania; personel organizacji odpowiedzialny za odzyskiwanie systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające odzyskiwanie w zapasowym miejscu przetwarzania].

CP-7(5)	**ZAPASOWE MIEJSCE PRZETWARZANIA | *RÓWNOWAŻNE ŚRODKI BEZPIECZEŃSTWA***
[Włączone do: CP-7].	

CP-7(6)	**ZAPASOWE MIEJSCE PRZETWARZANIA | *BRAK MOŻLIWOŚCI POWROTU DO LOKALIZACJI PODSTAWOWEJ***
	CEL OCENY: *Ustalić, czy organizacja planuje i przygotowuje się na okoliczności, które uniemożliwiają powrót do podstawowego miejsca przetwarzania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapasowego miejsca przetwarzania; plan ciągłości działania; zapasowe miejsce przetwarzania; umowy w sprawie zapasowego miejsca przetwarzania; konfiguracje zapasowego miejsce przetwarzania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za odtworzenie systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CP-8	**USŁUGI TELEKOMUNIKACYJNE**	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-8[1]	*definiuje operacje systemu informacyjnego wymagające ustanowienia alternatywnych usług telekomunikacyjnych w celu umożliwienia wznowienia takich operacji;*
	CP-8[2]	*definiuje okres czasu pozwalający na wznowienie operacji systemu informacyjnego zdefiniowanego przez organizację dla podstawowych misji i funkcji biznesowych; oraz*
	CP-8[3]	*ustanawia alternatywne usługi telekomunikacyjne, łącznie z niezbędnymi umowami pozwalającymi na wznowienie funkcjonowania zdefiniowanego przez organizację systemu informacyjnego dla podstawowych misji i funkcji biznesowych, w określonym przez organizację okresie czasu, w przypadku, gdy podstawowe funkcje telekomunikacyjne są niedostępne w podstawowym lub alternatywnym miejscu przetwarzania lub przechowywania.*

CP-8	**USŁUGI TELEKOMUNIKACYJNE**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące alternatywnych usług telekomunikacyjnych; plan ciągłości działania; umowy o świadczenie usług telekomunikacyjnych w podstawowym i alternatywnym miejscu przetwarzania i przechowywania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania usług telekomunikacyjnych; personel organizacji odpowiedzialny za odzyskiwanie systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za realizację transakcji nabycia / zawarcia umów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające usługi telekomunikacyjne].

CP-8(1)	**USŁUGI TELEKOMUNIKACYJNE | *PRIORYTETY ŚWIADCZENIA USŁUG***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-8(1)[1]	*wdraża umowy o świadczenie usług telekomunikacyjnych w podstawowym i alternatywnym miejscu przetwarzania i przechowywania, które zawierają postanowienia o pierwszeństwie usług zgodnie z wymogami dostępności organizacyjnej (w tym czas odzyskiwania określony w planie awaryjnym systemu informacyjnego); oraz*
	CP-8(1)[2]	*żąda zapewnienia pierwszeństwa usługi telekomunikacyjnej dla wszystkich usług telekomunikacyjnych wykorzystywanych w celu zapewnienia, w przypadku wystąpienia awarii, wykonywania obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w sytuacji, gdy podstawowe i / lub alternatywne usługi telekomunikacyjne są świadczone przez wspólnego operatora.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapewnienia podstawowych i alternatywnych usług telekomunikacyjnych; plan ciągłości działania; umowy o świadczenie usług telekomunikacyjnych w podstawowym i alternatywnym miejscu przetwarzania i przechowywania; dokumentacja dotycząca priorytetów świadczenia usług telekomunikacyjnych; inne odpowiednie dokumenty lub rejestry].	

CP-8(1)	**USŁUGI TELEKOMUNIKACYJNE | *PRIORYTETY ŚWIADCZENIA USŁUG***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania usług telekomunikacyjnych; personel organizacji odpowiedzialny za odzyskiwanie systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za realizację transakcji nabycia / zawarcia umów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające usługi telekomunikacyjne].

CP-8(2)	**USŁUGI TELEKOMUNIKACYJNE | *POJEDYNCZE PUNKTY AWARII***
	CEL OCENY: *Ustalenie, czy organizacja nabywa zastępcze usługi telekomunikacyjne w celu zmniejszenia prawdopodobieństwa wpływu jednostkowej awarii na świadczenie podstawowych usług telekomunikacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapewnienia podstawowych i alternatywnych usług telekomunikacyjnych; plan ciągłości działania; umowy o świadczenie usług telekomunikacyjnych w podstawowym i alternatywnym miejscu przetwarzania i przechowywania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania usług telekomunikacyjnych; personel organizacji odpowiedzialny za odzyskiwanie systemów informacyjnych; główny i alternatywni dostawcy usług telekomunikacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CP-8(3)	**USŁUGI TELEKOMUNIKACYJNE | *ROZDZIELENIE DOSTAWCÓW PODSTAWOWYCH / ALTERNATYWNYCH***
	CEL OCENY: *Ustalenie, czy organizacja uzyskuje alternatywne usługi telekomunikacyjne od dostawców, którzy są odseparowani od dostawców usług głównych, w celu zmniejszenia podatności na te same zagrożenia.*

CP-8(3)	**USŁUGI TELEKOMUNIKACYJNE | *ROZDZIELENIE DOSTAWCÓW PODSTAWOWYCH / ALTERNATYWNYCH***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące głównych i alternatywnych usług telekomunikacyjnych; plan ciągłości działania; umowy o świadczenie usług telekomunikacyjnych w podstawowym i alternatywnym miejscu przetwarzania i przechowywania; alternatywny dostawca usług telekomunikacyjnych; główny dostawca usług telekomunikacyjnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie ciągłości działania usług telekomunikacyjnych; personel organizacji odpowiedzialny za odzyskiwanie systemów informacyjnych; główny i alternatywni dostawcy usług telekomunikacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CP-8(4)	**USŁUGI TELEKOMUNIKACYJNE | *PLAN AWARYJNY DOSTAWCY***		
	CEL OCENY: *Określić, czy organizacja:*		
	CP-8(4)(a)	**CP-8(4)(a)[1]**	*wymaga od głównego dostawcy usług telekomunikacyjnych posiadania planu ciągłości działania;*
		CP-8(4)(a)[2]	*wymaga, aby alternatywny dostawca usług telekomunikacyjnych posiada plan ciągłości działania;*
	CP-8(4)(b)	*dokonuje przeglądów planów awaryjnych dostawców, aby upewnić się, że plany spełniają organizacyjne wymagania awaryjne;*	
	CP-8(4)(c)	**CP-8(4)(c)[1]**	*określa częstotliwość uzyskiwania potwierdzenia przeprowadzenia testu/szkolenia w sytuacjach awaryjnych przez usługodawców; oraz*
		CP-8(4)(c)[2]	*uzyskuje dowody przeprowadzania przez dostawców testów / szkoleń planowania ciągłości działania na wypadek awarii z częstotliwością określoną przez organizację.*

CP-8(4)	**USŁUGI TELEKOMUNIKACYJNE | *PLAN AWARYJNY DOSTAWCY***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące zapewnienia podstawowych i alternatywnych usług telekomunikacyjnych; plan ciągłości działania; plan awaryjny dostawcy; potwierdzenie przeprowadzenia przez usługodawców testów/szkoleń w sytuacjach awaryjnych; umowy o świadczenie usług telekomunikacyjnych w podstawowym i alternatywnym miejscu przetwarzania i przechowywania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem awaryjnym, realizacją planów i testowaniem; główny i alternatywni dostawcy usług telekomunikacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za realizację transakcji nabycia / zawarcia umów].

CP-8(5)	**USŁUGI TELEKOMUNIKACYJNE | *ALTERNATYWNE TESTOWANIE USŁUG TELEKOMUNIKACYJNYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-8(5)[1]	*określa częstotliwość testowania alternatywnych usług telekomunikacyjnych; oraz*
	CP-8(5)[2]	*testuje alternatywne usługi telekomunikacyjne z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące alternatywnych usług telekomunikacyjnych; plan ciągłości działania; ewidencja przeprowadzenia testów alternatywnych usług telekomunikacyjnych; umowy o świadczenie alternatywnych usług telekomunikacyjnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem awaryjnym, realizacją planów i testowaniem; alternatywni dostawcy usług telekomunikacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające testowanie alternatywnych usług telekomunikacyjnych].	

CP-9	**KOPIA ZAPASOWA**		
	CEL OCENY: *Określić, czy organizacja:*		
	CP-9(a)	**CP-9(a)[1]**	*definiuje częstotliwość, zgodną z celami dotyczącymi czasów odzyskiwania (RTO) i celami punktów odtworzenia danych (RPO) określonymi w planie awaryjnym systemu informacyjnego, do wykonywania kopii zapasowych informacji na poziomie użytkownika, przetwarzanych w systemie informacyjnym;*
		CP-9(a)[2]	*wykonuje kopie zapasowe informacji na poziomie użytkownika zawartych w systemie informacyjnym z częstotliwością określoną przez organizację;*
	CP-9(b)	**CP-9(b)[1]**	*definiuje częstotliwość, zgodną z celami dotyczącymi czasów odzyskiwania (RTO) i celami punktów odtworzenia danych (RPO) określonymi w planie awaryjnym systemu informacyjnego, do wykonywania kopii zapasowych informacji na poziomie systemu, przetwarzanych w systemie informacyjnym;*
		CP-9(b)[2]	*wykonuje kopie zapasowe informacji na poziomie systemu zawartych w systemie informacyjnym, z częstotliwością określoną przez organizację;*
	CP-9(c)	**CP-9(c)[1]**	*definiuje częstotliwość, zgodną z celami dotyczącymi czasów odzyskiwania (RTO) i celami punktów odtworzenia danych (RPO) określonymi w planie awaryjnym systemu informacyjnego, do wykonywania kopii zapasowych dokumentacji systemu informacyjnego, w tym dokumentacji związanej z bezpieczeństwem;*
		CP-9(c)[2]	*wykonuje kopie zapasowe dokumentacji, w tym dokumentacji związanej z bezpieczeństwem, z częstotliwością określoną przez organizację; oraz*
	CP-9(d)	*zapewnia poufność, integralność i dostępność kopii zapasowych w miejscach przechowywania.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu informacyjnego; plan awaryjny; lokalizacje przechowywania kopii zapasowych; dzienniki lub rejestry kopii zapasowych systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].		

CP-9	**KOPIA ZAPASOWA**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za tworzenie kopii zapasowych systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne do przeprowadzania kopii zapasowych systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające kopie zapasowe systemu informacyjnego].

CP-9(1)	**KOPIA ZAPASOWA | *BADANIE NIEZAWODNOŚCI NOŚNIKÓW / INTEGRALNOŚCI INFORMACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-9(1)[1]	*określa częstotliwość testowania kopii zapasowych informacji w celu weryfikacji niezawodności nośnika i integralności informacji; oraz*
	CP-9(1)[2]	*testuje kopie zapasowe informacji z częstotliwością określoną przez organizację w celu sprawdzenia niezawodności nośnika i integralności informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu informacyjnego; plan awaryjny; lokalizacje przechowywania kopii zapasowych; dzienniki lub rejestry kopii zapasowych systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za tworzenie kopii zapasowych systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne do przeprowadzania kopii zapasowych systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające kopie zapasowe systemu informacyjnego].	

CP-9(2)	**KOPIA ZAPASOWA | *TESTY ODTWORZENIOWE Z WYKORZYSTANIEM PRÓBEK DANYCH***
	CEL OCENY: *Ustalić, czy organizacja wykorzystuje próbkę informacji zapasowych w celu odtworzenia wybranych funkcji systemu informacyjnego w ramach testowania planu ciągłości działania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu informacyjnego; plan awaryjny; lokalizacje przechowywania kopii zapasowych; dzienniki lub rejestry kopii zapasowych systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za tworzenie kopii zapasowych systemu informacyjnego; personel organizacji odpowiedzialny za plan ciągłości działania / testowanie planu ciągłości działania; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne do przeprowadzania kopii zapasowych systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające kopie zapasowe systemu informacyjnego].

CP-9(3)	**KOPIA ZAPASOWA | *SEPARACJA PRZECHOWYWANIA INFORMACJI KRYTYCZNYCH***		
	CEL OCENY: *Określić, czy organizacja:*		
	CP-9(3)[1]	**CP-9(3)[1][a]**	*definiuje oprogramowanie krytyczne systemu informacyjnego i inne informacje związane z bezpieczeństwem wymagające przechowywania kopii zapasowych w oddzielnym obiekcie; lub*
		CP-9(3)[1][b]	*definiuje oprogramowanie krytyczne systemu informacyjnego oraz inne informacje związane z bezpieczeństwem wymagające przechowywania kopii zapasowych w ognioodpornym kontenerze, który nie jest umieszczony z bieżącym systemem operacyjnym; oraz*
	CP-9(3)[2]	*przechowuje kopie zapasowe zdefiniowanego przez organizację oprogramowania krytycznego systemu informacyjnego oraz innych informacji związanych z bezpieczeństwem w oddzielnym obiekcie lub w kontenerze ognioodpornym, który nie jest umieszczany z bieżącym systemem operacyjnym.*	

CP-9(3)	**KOPIA ZAPASOWA | *SEPARACJA PRZECHOWYWANIA INFORMACJI KRYTYCZNYCH***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu informacyjnego; plan awaryjny; lokalizacje przechowywania kopii zapasowych; dzienniki lub rejestry kopii zapasowych systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie awaryjne i wdrażanie planów; personel organizacji odpowiedzialny za tworzenie kopii zapasowych systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

CP-9(4)	**KOPIA ZAPASOWA | *OCHRONA PRZED NIEAUTORYZOWANĄ MODYFIKACJĄ***
[Włączone do: CP-9].	

CP-9(5)	**KOPIA ZAPASOWA | *PRZEKAZANIE KOPII DO ALTERNATYWNEJ LOKALIZACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-9(5)[1]	*definiuje okres czasu, zgodny z czasem odzyskiwania i punktami odtworzenia danych określonymi w planie awaryjnym systemu informacyjnego, na przekazanie kopii zapasowej do zapasowego miejsca przechowywania kopii;*
	CP-9(5)[2]	*definiuje szybkość transferu, zgodną z okresami odzyskiwania i punktami odtworzenia danych określonymi w planie awaryjnym systemu informacyjnego, kopii zapasowej do zapasowego miejsca przechowywania kopii; oraz*
	CP-9(5)[3]	*przekazuje kopie zapasowe do zapasowego miejsca przechowywania kopii w ustalonym przez organizację okresie czasu i zdefiniowaną szybkością transferu.*

CP-9(5)	**KOPIA ZAPASOWA | *PRZEKAZANIE KOPII DO ALTERNATYWNEJ LOKALIZACJI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu informacyjnego; plan ciągłości działania; dzienniki lub rejestry kopii zapasowych systemu informacyjnego; ewidencja przekazania kopii zapasowej systemu do alternatywnego miejsca przechowywania kopii; umowy w sprawie zapasowego miejsca przechowywania kopii; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za tworzenie kopii zapasowych systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące przekazywania kopii zapasowych systemów informacyjnych do alternatywnego miejsca składowania; zautomatyzowane mechanizmy wspierające i/lub wdrażające kopie zapasowe systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające przekazywanie informacji do zapasowego miejsca przechowywania kopii].

CP-9(6)	**KOPIA ZAPASOWA | *REDUNDANCJA (NADMIAROWOŚĆ) SYSTEMU***	
	CEL OCENY: *Ustalić, czy organizacja wykonuje kopię zapasową systemu informacyjnego, utrzymując redundantny system wtórny, który:*	
	CP-9(6)[1]	*nie jest kolokowany z systemem podstawowym, oraz;*
	CP-9(6)[2]	*może być aktywowany bez utraty informacji lub zakłócenia operacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu informacyjnego; plan ciągłości działania; wyniki testów kopii zapasowej; dokumentacja przeprowadzonych testów planu ciągłości działania; dokumentacja dotycząca testów planu ciągłości działania; redundancja (nadmiarowość) systemu kopii zapasowej; lokalizacja(-e) redundantnego(-ych) systemu(-ów) rezerwowego(-ych); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za tworzenie kopii zapasowych systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za redundancję (nadmiarowość) systemu].	

CP-9(6)	**KOPIA ZAPASOWA | *REDUNDANCJA (NADMIAROWOŚĆ) SYSTEMU***
	Test: [*wybierz spośród:* Procesy organizacyjne związane z utrzymaniem redundancji (nadmiarowości) systemu; zautomatyzowane mechanizmy wspierające i/lub wdrażające kopie zapasowe systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające przekazywanie informacji do systemu redundantnego (nadmiarowego)].

CP-9(7)	**KOPIA ZAPASOWA | *PODWÓJNA AUTORYZACJA***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-9(7)[1]	*definiuje informacje zapasowe, które wymagają egzekwowania podwójnej autoryzacji w celu usunięcia lub zniszczenia takich informacji; oraz*
	CP-9(7)[2]	*wymusza podwójną autoryzację do usuwania lub niszczenia informacji zapasowych zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu informacyjnego; plan ciągłości działania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; generowana przez system lista referencji lub zasad podwójnej autoryzacji; dzienniki lub zapisy dotyczące usuwania lub niszczenia informacji zapasowych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za tworzenie kopii zapasowych systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające podwójną autoryzację; zautomatyzowane mechanizmy wspierające i/lub wdrażające usuwanie/niszczenie kopii zapasowych].	

CP-10	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU**	
	CEL OCENY: *Ustalić, czy organizacja zapewnia:*	
	CP-10[1]	*odzyskanie systemu informacyjnego do znanego stanu po zakończeniu:*

CP-10	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU**		
		CP-10[1][a]	*zakłócenia;*
		CP-10[1][b]	*naruszenia; lub*
		CP-10[1][c]	*awarii;*
	CP-10[2]	*odtworzenie systemu informacyjnego do znanego stanu po zakończeniu:*	
		CP-10[2][a]	*zakłócenia;*
		CP-10[2][b]	*naruszenia; lub*
		CP-10[2][c]	*awarii.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu informacyjnego; plan ciągłości działania; wyniki testów kopii zapasowej; dokumentacja przeprowadzonych testów planu ciągłości działania; dokumentacja dotycząca testów planu ciągłości działania; redundancja (nadmiarowość) systemu dla kopii zapasowej; lokalizacja(-e) redundantnego(-ych) systemu(-ów) rezerwowego(-ych); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie awaryjne, odzyskanie i/lub odtworzenie zasobów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne wdrażające operacje odzyskiwania i odtworzenia systemów informacyjnych; zautomatyzowane mechanizmy wspierające i/lub wdrażające operacje odzyskiwania i odtworzenia systemów informacyjnych].		

CP-10(1)	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU | *TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA***
[Włączone do: CP-4].	

CP-10(2)	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU | *ODTWARZANIE TRANSAKCJI***
	CEL OCENY: *Ustalić, czy system informacyjny posiada zdolność odtwarzania transakcji w systemach opartych na transakcjach.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące odzyskiwania i odtwarzania systemu; plan ciągłości działania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja dotycząca testów planu ciągłości działania; dokumentacja przeprowadzonych testów planu ciągłości działania; zapisy dotyczące odtwarzania transakcji w systemie informacyjnym; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za odtwarzanie transakcji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwość odtwarzania transakcji].

CP-10(3)	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU | *KOMPENSACYJNE ŚRODKI BEZPIECZEŃSTWA***
[Wycofane: Uwzględnione w procedurach dostosowywania (procedurach oceny CA)].	

CP-10(4)	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU | *PRZYWRACANIE W OKREŚLONYM PRZEDZIALE CZASOWYM***	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-10(4)[1]	*definiuje okres czasu na przywracanie komponentów systemu informacyjnego z informacji kontrolowanych przez konfigurację i chronionych pod kątem integralności, reprezentujących znany stan operacyjny komponentów; oraz*
	CP-10(4)[2]	*zapewnia możliwość przywracania składników systemu informacyjnego w określonym przez organizację okresie czasu z informacji kontrolowanych przez konfigurację i chronionych pod kątem integralności, reprezentujących znany stan operacyjny komponentów.*

CP-10(4)	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU | *PRZYWRACANIE W OKREŚLONYM PRZEDZIALE CZASOWYM***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące odzyskiwania i odtwarzania systemu; plan ciągłości działania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja dotycząca testów planu ciągłości działania; dokumentacja przeprowadzonych testów planu ciągłości działania; ewidencja operacji odzyskiwania i odtwarzania systemu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za odzyskiwanie i odtwarzanie systemu; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające odzyskiwanie/ odtwarzanie informacji z systemu informacyjnego].

CP-10(5)	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU | *PRACE AWARYJNE***
[Włączone do: SI-13].	

CP-10(6)	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU | *OCHRONA KOMPONENTÓW***	
	CEL OCENY: *Ustalić, czy organizacja chroni kopie zapasowe i przywracanie:*	
	CP-10(6)[1]	*sprzętu;*
	CP-10(6)[2]	*oprogramowania układowego; oraz*
	CP-10(6)[3]	*oprogramowanie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące odzyskiwania i odtwarzania systemu; plan ciągłości działania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; poświadczenia dostępu logicznego; poświadczenia dostępu fizycznego; zapisy autoryzacji dostępu logicznego; zapisy autoryzacji dostępu fizycznego; inne odpowiednie dokumenty lub rejestry].	

CP-10(6)	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU | *OCHRONA KOMPONENTÓW***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za odzyskiwanie i odtwarzanie systemu; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące ochrony kopii i przywracania sprzętu, oprogramowania układowego i oprogramowania; zautomatyzowane mechanizmy wspierające i/lub wdrażające ochronę sprzętu, oprogramowania układowego i oprogramowania do wykonywania kopii zapasowych].

CP-11	**ALTERNATYWNE PROTOKOŁY KOMUNIKACJI**	
	CEL OCENY: *Określić, czy:*	
	CP-11[1]	*organizacja określa alternatywne protokoły łączności, które mają być stosowane w celu utrzymania ciągłości operacji; oraz*
	CP-11[2]	*system informacyjny zapewnia możliwość stosowania zdefiniowanych przez organizację alternatywnych protokołów komunikacyjnych w celu utrzymania ciągłości operacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące wykorzystania alternatywnych protokołów komunikacyjnych; plan ciągłości działania; plan ciągłości działania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz alternatywnych protokołów komunikacyjnych wspomagających ciągłość operacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji z odpowiedzialnością za planowanie awaryjne i realizację planów; personel organizacji z odpowiedzialnością za planowanie operacyjne i realizację planów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wykorzystujące alternatywne protokoły komunikacyjne].	

CP-12	**TRYB BEZPIECZNY**	
	CEL OCENY: *Określić, czy:*	
	CP-12[1]	*organizacja określa warunki, wykrycie których wymaga wejścia systemu informacyjnego w bezpieczny tryb pracy;*
	CP-12[2]	*organizacja określa ograniczenia działania bezpiecznego trybu pracy; oraz*
	CP-12[3]	*system informacyjny, w przypadku wykrycia warunków zdefiniowanych przez organizację, przechodzi do bezpiecznego trybu pracy ze zdefiniowanymi przez organizację ograniczeniami trybu pracy.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące działania system informacyjnego w trybie bezpiecznym; plan ciągłości działania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; podręczniki administrowania systemem informacyjnym; instrukcje obsługi systemu informacyjnego; instrukcje instalacji systemu informacyjnego; dokumentacja dotycząca planowania ciągłości działania; dokumentacja dotycząca obsługi incydentów; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające tryb bezpieczny].	

CP-13	**ALTERNATYWNE MECHANIZMY BEZPIECZEŃSTWA**	
	CEL OCENY: *Określić, czy organizacja:*	
	CP-13[1]	*określa alternatywne lub uzupełniające mechanizmy bezpieczeństwa, które mają być stosowane w przypadku, gdy podstawowe środki realizacji funkcji bezpieczeństwa są niedostępne lub zagrożone;*
	CP-13[2]	*definiuje funkcje bezpieczeństwa, które mają być spełnione przy zastosowaniu alternatywnych lub dodatkowych mechanizmów bezpieczeństwa określonych przez organizację w przypadku, gdy podstawowy środek wdrażania funkcji bezpieczeństwa jest niedostępny lub zagrożony; oraz*

CP-13	**ALTERNATYWNE MECHANIZMY BEZPIECZEŃSTWA**	
	CP-13[3]	*wykorzystuje zdefiniowane przez organizację alternatywne lub uzupełniające mechanizmy bezpieczeństwa spełniające funkcje bezpieczeństwa zdefiniowane przez organizację, gdy podstawowe środki realizacji funkcji bezpieczeństwa są niedostępne lub zagrożone.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania awaryjnego; procedury dotyczące stosowania alternatywnych mechanizmów bezpieczeństwa; plan ciągłości działania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rekordy testowania planu ciągłości działania; dokumentacja przeprowadzonych testów planu ciągłości działania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zdolność systemu informacyjnego do wdrażania alternatywnych mechanizmów bezpieczeństwa].	

KATEGORIA IA - IDENTYFIKACJA I UWIERZYTELNIANIE

IA-1	**POLITYKA I PROCEDURY IDENTYFIKACJI I UWIERZYTELNIANIA**			
	CEL OCENY: *Określić, czy organizacja:*			
	IA-1(a)(1)	**IA-1(a)(1)[1]**	*opracowuje i dokumentuje politykę identyfikacji i uwierzytelniania, która dotyczy:*	
			IA-1(a)(1)[1][a]	*celu;*
			IA-1(a)(1)[1][b]	*zakresu stosowania;*
			IA-1(a)(1)[1][c]	*ról;*
			IA-1(a)(1)[1][d]	*odpowiedzialności;*
			IA-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			IA-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			IA-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		IA-1(a)(1)[2]	*określa personel lub role, wśród których ma być rozpowszechniana polityka identyfikacji i uwierzytelniania; oraz*	
		IA-1(a)(1)[3]	*rozpowszechnia politykę identyfikacji i uwierzytelniania wśród personelu lub ról zdefiniowanych przez organizację;*	
	IA-1(a)(2)	**IA-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrożenie polityki identyfikacji i uwierzytelniania oraz związanych z nią zabezpieczeń identyfikacji i uwierzytelniania;*	
		IA-1(a)(2)[2]	*definiuje personel lub role, wśród których mają być rozpowszechniane procedury;*	
		IA-1(a)(2)[3]	*rozpowszechnia procedury wśród personelu lub ról zdefiniowanych przez organizację;*	
	IA-1(b)(1)	**IA-1(b)(1)[1]**	*definiuje częstotliwość przeglądu i aktualizacji bieżącej polityki identyfikacji i uwierzytelniania;*	

IA-1	**POLITYKA I PROCEDURY IDENTYFIKACJI I UWIERZYTELNIANIA**		
		IA-1(b)(1)[2]	*dokonuje przeglądu i aktualizacji aktualnej polityki identyfikacji i uwierzytelniania z częstotliwością określoną przez organizację; oraz*
	IA-1(b)(2)	**IA-1(b)(2)[1]**	*określa częstotliwość przeglądów i aktualizacji bieżących procedur identyfikacji i uwierzytelniania; oraz*
		IA-1(b)(2)[2]	*dokonuje przeglądu i aktualizacji bieżących procedur identyfikacji i uwierzytelniania z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury identyfikacji i uwierzytelniania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za identyfikację i uwierzytelnianie; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

IA-2	**IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)**
	CEL OCENY: *Ustalić, czy system informacyjny jednoznacznie identyfikuje i uwierzytelnia użytkowników organizacyjnych (lub procesy działające w imieniu użytkowników organizacyjnych).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacji odpowiedzialny za zarządzanie kontami; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące do jednoznacznej identyfikacji i uwierzytelniania użytkowników; zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcję identyfikacji i uwierzytelniania].

IA-2(1)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *DOSTĘP SIECIOWY Z KONT UPRZYWILEJOWANYCH***
	CEL OCENY: *Ustalić, czy system informacyjny stosuje implementuje uwierzytelnianie wieloskładnikowe w celu uzyskania dostępu sieciowego z kont uprzywilejowanych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające uwierzytelnianie wieloskładnikowe].

IA-2(2)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *DOSTĘP SIECIOWY Z KONT NIEUPRZYWILEJOWANYCH***
	CEL OCENY: *Ustalić, czy system informacyjny implementuje uwierzytelnianie wieloskładnikowe w celu uzyskania dostępu sieciowego z kont nieuprzywilejowanych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające uwierzytelnianie wieloskładnikowe].

IA-2(3)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *DOSTĘP LOKALNY Z KONT UPRZYWILEJOWANYCH***
	CEL OCENY: *Ustalić, czy system informacyjny implementuje uwierzytelnianie wieloskładnikowe w celu uzyskania dostępu lokalnego z kont uprzywilejowanych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające uwierzytelnianie wieloskładnikowe].

IA-2(4)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *DOSTĘP LOKALNY Z KONT NIEUPRZYWILEJOWANYCH***
	CEL OCENY: *Ustalić, czy system informacyjny implementuje uwierzytelnianie wieloskładnikowe w celu uzyskania dostępu lokalnego z kont nieuprzywilejowanych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów].

IA-2(4)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *DOSTĘP LOKALNY Z KONT NIEUPRZYWILEJOWANYCH***
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające uwierzytelnianie wieloskładnikowe].

IA-2(5)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *AUTORYZACJA GRUPY***
	CEL OCENY: *Ustalić, czy organizacja wymaga uwierzytelniania indywidualnych użytkowników logujących się do zasobów współużytkowanych przez grupę użytkowników, za pomocą indywidualnego identyfikatora przydzielonego tej osobie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwość uwierzytelniania kont grupowych].

IA-2(6)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *DOSTĘP SIECIOWY Z KONT UPRZYWILEJOWANYCH – ODSEPAROWANE URZĄDZENIE***	
	CEL OCENY: *Określić, czy:*	
	IA-2(6)[1]	*system informacyjny realizuje uwierzytelnianie wieloskładnikowe dla dostępu sieciowego z kont uprzywilejowanych w taki sposób, że urządzenie uwierzytelniające dostęp do systemu jest odseparowane od systemu udzielającego dostępu;*
	IA-2(6)[2]	*organizacja określa wymagania dotyczące mechanizmu uwierzytelniania, które mają być egzekwowane przez urządzenie niezależne od systemu uzyskującego dostęp sieciowy z kont uprzywilejowanych; oraz*

IA-2(6)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *DOSTĘP SIECIOWY Z KONT UPRZYWILEJOWANYCH – ODSEPAROWANE URZĄDZENIE***	
	IA-2(6)[3]	*system informacyjny realizuje uwierzytelnianie wieloskładnikowe do dostępu sieciowego z kont uprzywilejowanych w taki sposób, że urządzenie, oddzielone od systemu uzyskującego dostęp, spełnia określone organizacyjnie wymagania dotyczące mechanizmu uwierzytelniania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające uwierzytelnianie wieloskładnikowe].	

IA-2(7)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *DOSTĘP SIECIOWY Z KONT NIEUPRZYWILEJOWANYCH – ODSEPAROWANE URZĄDZENIE***	
	CEL OCENY: *Określić, czy:*	
	IA-2(7)[1]	*system informacyjny realizuje uwierzytelnianie wieloskładnikowe dla dostępu sieciowego z kont nieuprzywilejowanych w taki sposób, że urządzenie uwierzytelniające dostęp do systemu jest odseparowane od systemu udzielającego dostępu;*
	IA-2(7)[2]	*organizacja określa wymagania dotyczące mechanizmu uwierzytelniania, które mają być egzekwowane przez urządzenie niezależne od systemu uzyskującego dostęp sieciowy z kont nieuprzywilejowanych; oraz*
	IA-2(7)[3]	*system informacyjny realizuje uwierzytelnianie wieloskładnikowe do dostępu sieciowego z kont nieuprzywilejowanych w taki sposób, że urządzenie, oddzielone od systemu uzyskującego dostęp, spełnia określone organizacyjnie wymagania dotyczące mechanizmu uwierzytelniania.*

IA-2(7)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *DOSTĘP SIECIOWY Z KONT NIEUPRZYWILEJOWANYCH – ODSEPAROWANE URZĄDZENIE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające uwierzytelnianie wieloskładnikowe].

IA-2(8)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *DOSTĘP SIECIOWY Z KONT UPRZYWILEJOWANYCH – ODPORNOŚĆ NA POWTARZANIE***
	CEL OCENY: *Ustalić, czy system informacyjny implementuje odporne na powtarzanie mechanizmy uwierzytelniania dostępu sieciowego z kont uprzywilejowanych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont uprzywilejowanych systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające lub wdrażające funkcję identyfikacji i uwierzytelniania; zautomatyzowane mechanizmy wspierające lub wdrażające mechanizmy uwierzytelniania odporne na powtórne powtarzanie].

IA-2(9)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *DOSTĘP SIECIOWY Z KONT NIEUPRZYWILEJOWANYCH – ODPORNOŚĆ NA POWTARZANIE***
	CEL OCENY: *Ustalić, czy system informacyjny implementuje odporne na powtarzanie mechanizmy uwierzytelniania dostępu sieciowego z kont nieuprzywilejowanych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont nieuprzywilejowanych systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające lub wdrażające funkcję identyfikacji i uwierzytelniania; zautomatyzowane mechanizmy wspierające lub wdrażające mechanizmy uwierzytelniania odporne na powtórne powtarzanie].

IA-2(10)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *LOGOWANIE POJEDYNCZE***	
	CEL OCENY: *Określić, czy:*	
	IA-2(10)[1]	*organizacja określa wykaz kont systemu informacyjnego i usług, dla których musi być zapewnione możliwość logowania pojedynczego; oraz*
	IA-2(10)[2]	*system informacyjny zapewnia możliwość logowania pojedynczego dla kont i usług systemu informacyjnego zdefiniowanego przez organizację.*

IA-2(10)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *LOGOWANIE POJEDYNCZE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące możliwości pojedynczego logowania w odniesieniu do kont i usług systemu informacyjnego; procedury dotyczące identyfikacji i uwierzytelniania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; zapisy z audytu systemu informacyjnego; wykaz kont i usług systemu informacyjnego wymagających pojedynczego logowania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcję identyfikacji i uwierzytelniania; zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcję logowania pojedynczego dla kont i usług systemu informacyjnego].

IA-2(11)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *ZDALNY DOSTĘP - ODSEPAROWANE URZĄDZENIE***	
	CEL OCENY: *Określić, czy:*	
	IA-2(11)[1]	*system informacyjny realizuje uwierzytelnianie wieloskładnikowe dla dostępu zdalnego z kont uprzywilejowanych w taki sposób, że urządzenie uwierzytelniające dostęp do systemu jest odseparowane od systemu udzielającego dostępu;*
	IA-2(11)[2]	*system informacyjny realizuje uwierzytelnianie wieloskładnikowe dla dostępu zdalnego z kont nieuprzywilejowanych w taki sposób, że urządzenie uwierzytelniające dostęp do systemu jest odseparowane od systemu udzielającego dostępu;*
	IA-2(11)[3]	*organizacja określa wymagania dotyczące mechanizmu uwierzytelniania, które mają być egzekwowane przez urządzenie niezależne od systemu uzyskującego dostęp zdalny z kont uprzywilejowanych;*

IA-2(11)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *ZDALNY DOSTĘP - ODSEPAROWANE URZĄDZENIE***	
	IA-2(11)[4]	*organizacja określa wymagania dotyczące mechanizmu uwierzytelniania, które mają być egzekwowane przez urządzenie niezależne od systemu uzyskującego dostęp zdalny z kont nieuprzywilejowanych;*
	IA-2(11)[5]	*system informacyjny realizuje uwierzytelnianie wieloskładnikowe do dostępu zdalnego z kont uprzywilejowanych w taki sposób, że urządzenie, oddzielone od systemu uzyskującego dostęp, spełnia określone organizacyjnie wymagania dotyczące mechanizmu uwierzytelniania; oraz*
	IA-2(11)[6]	*system informacyjny realizuje uwierzytelnianie wieloskładnikowe do dostępu zdalnego z kont nieuprzywilejowanych w taki sposób, że urządzenie, oddzielone od systemu uzyskującego dostęp, spełnia określone organizacyjnie wymagania dotyczące mechanizmu uwierzytelniania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont uprzywilejowanych i nieuprzywilejowanych w systemie informacyjnym; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcję identyfikacji i uwierzytelniania].	

IA-2(12)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *AUTORYZACJA DANYCH DOSTĘPOWYCH***	
	CEL OCENY: *Ustalić, czy system informacyjny:*	
	IA-2(12)[1]	*akceptuje dane identyfikacyjne karty dostępowej; oraz*
	IA-2(12)[2]	*elektronicznie weryfikuje dane identyfikacyjne karty dostępowej.*

IA-2(12)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *AUTORYZACJA DANYCH DOSTĘPOWYCH***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; zapisy z weryfikacji karty dostępowej; ewidencja kart dostępowych; autoryzacje kart dostępowych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające akceptację i weryfikację kart dostępowych].

IA-2(13)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *UWIERZYTELNIANIE "POZA PASMEM" (Z WYKORZYSTANIEM DWÓCH ODDZIELNYCH ŚCIEŻEK)***	
	CEL OCENY: *Określić, czy:*	
	IA-2(13)[1]	*organizacja określa uwierzytelnianie pozapasmowe, które ma być wdrożone przez system informacyjny;*
	IA-2(13)[2]	*organizacja definiuje warunki, na jakich system informacyjny wdraża uwierzytelnianie pozapasmowe zdefiniowane przez organizację; oraz*
	IA-2(13)[3]	*system informacyjny wdraża uwierzytelnianie pozapasmowe zdefiniowane przez organizację w warunkach zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; generowana przez system lista pozapasmowych ścieżek uwierzytelniania; inne odpowiednie dokumenty lub rejestry].	

IA-2(13)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *UWIERZYTELNIANIE "POZA PASMEM" (Z WYKORZYSTANIEM DWÓCH ODDZIELNYCH ŚCIEŻEK)***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwość uwierzytelniania pozapasmowego].

IA-3	**IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA**	
	CEL OCENY: *Określić, czy:*	
	IA-3[1]	*organizacja określa specyfikacje i/lub rodzaje urządzeń, które system informacyjny jednoznacznie identyfikuje i uwierzytelnia przed ustanowieniem jednego lub więcej z poniższych dostępów:*
	IA-3[1][a]	*lokalnego;*
	IA-3[1][b]	*zdalnego; oraz/lub*
	IA-3[1][c]	*sieciowego; oraz*
	IA-3[2]	*system informacyjny jednoznacznie identyfikuje i uwierzytelnia urządzenia określone przez organizację przed ustanowieniem jednego lub więcej z poniższych dostępów:*
	IA-3[2][a]	*lokalnego;*
	IA-3[2][b]	*zdalnego; oraz/lub*
	IA-3[2][c]	*sieciowego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania urządzenia; dokumentacja projektowa systemu informacyjnego; lista urządzeń wymagających jednoznacznej identyfikacji i uwierzytelnienia; raporty dotyczące połączenia z urządzeniem; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; inne odpowiednie dokumenty lub rejestry].	

IA-3	**IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za identyfikację i uwierzytelnianie urządzeń; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające lub wdrażające identyfikację urządzeń i zdolność uwierzytelniania].

IA-3(1)	**IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | *DWUKIERUNKOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE***		
	CEL OCENY: *Określić, czy:*		
	IA-3(1)[1]	*organizacja określa specyfikacje lub rodzaje urządzeń wymagających stosowania dwukierunkowego uwierzytelniania kryptograficznego w celu uwierzytelnienia przed ustanowieniem jednego lub kilku z poniższych dostępów:*	
		IA-3(1)[1][a]	*lokalnego;*
		IA-3(1)[1][b]	*zdalnego; oraz/lub*
		IA-3(1)[1][c]	*sieciowego;*
	IA-3(1)[2]	*system informacyjny wykorzystuje dwukierunkowe uwierzytelnianie kryptograficzne do autoryzacji urządzeń zdefiniowanych przez organizację przed ustanowieniem jednego lub więcej z poniższych:*	
		IA-3(1)[2][a]	*lokalnego;*
		IA-3(1)[2][b]	*zdalnego; oraz/lub*
		IA-3(1)[2][c]	*sieciowego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania urządzenia; dokumentacja projektowa systemu informacyjnego; lista urządzeń wymagających jednoznacznej identyfikacji i uwierzytelnienia; raporty dotyczące połączenia z urządzeniem; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; inne odpowiednie dokumenty lub rejestry].		

IA-3(1)	**IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | *DWUKIERUNKOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za identyfikację i uwierzytelnianie urządzeń; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające lub implementujące możliwość uwierzytelniania kryptograficznego urządzeń; mechanizmy dwukierunkowego uwierzytelniania kryptograficznego].

IA-3(2)	**IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | *DWUKIERUNKOWE SIECIOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE***
[Włączone do: IA-3(1)].	

IA-3(3)	**IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | *ALOKACJA ADRESU DYNAMICZNEGO***		
	CEL OCENY: *Określić, czy organizacja:*		
	IA-3(3)(a)	**IA-3(3)(a)[1]**	*standaryzuje informacje przydziału adresów dynamicznych, które mają być wykorzystane do alokacji adresu dynamicznego urządzeń;*
		IA-3(3)(a)[2]	*definiuje czas trwania umowy przydziału adresów dynamicznych wykorzystywanych do alokacji adresu dynamicznego urządzeń;*
		IA-3(3)(a)[3]	*standaryzuje alokację adresu dynamicznego w zakresie przydziału adresów dynamicznych przypisanych do urządzeń zgodnie ze zdefiniowanymi przez organizację informacjami o dzierżawie;*
		IA-3(3)(a)[4]	*standaryzuje czas trwania dzierżawy alokowanych adresów dynamicznych zgodnie ze zdefiniowanym organizacyjnie czasem trwania dzierżawy; oraz*
	IA-3(3)(b)	*audytuje informacje o dzierżawie adresów dynamicznych, przypisanych do urządzenia.*	

IA-3(3)	**IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | *ALOKACJA ADRESU DYNAMICZNEGO***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania urządzenia; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykazanie historii czasu trwania dzierżawy adresów przypisanych do urządzeń; raporty dotyczące podłączania urządzeń; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za identyfikację i uwierzytelnianie urządzeń; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające lub wdrażające identyfikację urządzeń i zdolność uwierzytelniania; zautomatyzowane mechanizmy wspomagające i/lub wdrażające alokację adresu dynamicznego; zautomatyzowane mechanizmy wspomagające i/lub wprowadzające audyt informacji dotyczących dzierżawy adresów.].

IA-3(4)	**IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | *ATESTACJA URZĄDZENIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	IA-3(4)[1]	*definiuje proces zarządzania konfiguracją, który ma być zastosowany do obsługi identyfikacji i uwierzytelniania urządzenia na podstawie atestacji; oraz*
	IA-3(4)[2]	*zapewnia, że identyfikacja i uwierzytelnianie urządzenia na podstawie atestu jest realizowane przez zdefiniowany przez organizację proces zarządzania konfiguracją.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania urządzenia; procedury zarządzania konfiguracją urządzeń; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry zarządzania konfiguracją; rejestry zabezpieczeń zmian; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

IA-3(4)	**IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | *ATESTACJA URZĄDZENIA***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za identyfikację i uwierzytelnianie urządzeń; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające lub wdrażające identyfikację urządzeń i zdolność uwierzytelniania; zautomatyzowane mechanizmy wspomagające i/lub wdrażające zarządzanie konfiguracją; mechanizmy kryptograficzne wspomagające atestację urządzenia].

IA-4	**ZARZĄDZANIE IDENTYFIKATOREM**			
	CEL OCENY: *Ustalić, czy organizacja zarządza identyfikatorami systemu informacyjnego poprzez:*			
	IA-4(a)	**IA-4(a)[1]**	*określenie personelu lub ról, którzy udzielają autoryzacji do przydzielania unikalnego identyfikatora:*	
			IA-4(a)[1][a]	*osobie;*
			IA-4(a)[1][b]	*grupie;*
			IA-4(a)[1][c]	*roli; oraz/lub*
			IA-4(a)[1][d]	*urządzeniu;*
		IA-4(a)[2]	*otrzymanie upoważnienia od określonego przez organizację personelu lub ról do przydzielenia:*	
			IA-4(a)[2][a]	*osobie;*
			IA-4(a)[2][b]	*grupie;*
			IA-4(a)[2][c]	*roli; oraz/lub*
			IA-4(a)[2][d]	*urządzeniu;*
	IA-4(b)	*wybór identyfikatora, który identyfikuje:*		
		IA-4(b)[1]	*osobę;*	
		IA-4(b)[2]	*grupę;*	
		IA-4(b)[3]	*rolę; oraz/lub*	

IA-4	**ZARZĄDZANIE IDENTYFIKATOREM**		
		IA-4(b)[4]	*urządzenie;*
	IA-4(c)	*przypisanie identyfikatora do konkretnej:*	
		IA-4(c)[1]	*osoby;*
		IA-4(c)[2]	*grupy;*
		IA-4(c)[3]	*roli; oraz/lub*
		IA-4(c)[4]	*urządzenia;*
	IA-4(d)	**IA-4(d)[1]**	*określenie okresu czasu, w którym należy zapobiec ponownemu użyciu identyfikatorów;*
		IA-4(d)[2]	*zapobieganie ponownemu użyciu identyfikatorów przez okres czasu określony przez organizację;*
	IA-4(e)	**IA-4(e)[1]**	*zdefiniowanie okresu braku aktywności w celu dezaktywacji identyfikatora; oraz*
		IA-4(e)[2]	*wyłączenie identyfikatora po upływie określonego przez organizację okresu braku aktywności.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące zarządzania identyfikatorem; procedury dotyczące zarządzania kontami; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz kont systemu informacyjnego; wykaz identyfikatorów generowanych przez urządzenia kontroli dostępu fizycznego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie identyfikatorem; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie identyfikatorem].		

IA-4(1)	**ZARZĄDZANIE IDENTYFIKATOREM | *ZAKAZ UŻYWANIA IDENTYFIKATORÓW KONT JAKO IDENTYFIKATORÓW PUBLICZNYCH***
	CEL OCENY: *Ustalić, czy organizacja zakazuje stosowania w systemie informacyjnym identyfikatorów kont, które są takie same jak identyfikatory publiczne stosowane w indywidualnych kontach poczty elektronicznej.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące zarządzania identyfikatorem; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie identyfikatorem; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie identyfikatorem].

IA-4(2)	**ZARZĄDZANIE IDENTYFIKATOREM | *AUTORYZACJA PRZEŁOŻONEGO***
	CEL OCENY: *Ustalić, czy organizacja wymaga, aby proces rejestracji w celu otrzymania indywidualnego identyfikatora obejmował autoryzację przełożonego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące zarządzania identyfikatorem; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie identyfikatorem; organy nadzorcze odpowiedzialne za zatwierdzanie rejestracji identyfikatorów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie identyfikatorem].

IA-4(3)	**ZARZĄDZANIE IDENTYFIKATOREM | *WIELE FORM CERTYFIKACJI***
	CEL OCENY: *określić, czy organizacja wymaga stosowania wielu form weryfikacji identyfikacji indywidualnej, takich jak dokumenty dowodowe lub połączenie dokumentów i danych biometrycznych, które należy przedstawić organowi rejestrującemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące zarządzania identyfikatorem; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie identyfikatorem; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie identyfikatorem].

IA-4(4)	**ZARZĄDZANIE IDENTYFIKATOREM | *IDENTYFIKACJA STATUSU UŻYTKOWNIKA***	
	CEL OCENY: *Określić, czy organizacja:*	
	IA-4(4)[1]	*definiuje cechę identyfikującą, która ma być używana do określenia indywidualnego statusu; oraz*
	IA-4(4)[2]	*zarządza indywidualnymi identyfikatorami poprzez jednoznaczną identyfikację każdej osoby jako zdefiniowanej przez organizację cechy identyfikującej indywidualny status.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące zarządzania identyfikatorem; procedury dotyczące zarządzania kontami; wykaz cech określających indywidualny status; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie identyfikatorem; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci].	

IA-4(4)	**ZARZĄDZANIE IDENTYFIKATOREM | *IDENTYFIKACJA STATUSU UŻYTKOWNIKA***
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie identyfikatorem].

IA-4(5)	**ZARZĄDZANIE IDENTYFIKATOREM | *ZARZĄDZANIE DYNAMICZNE***
	CEL OCENY: *Ustalić, czy system informacyjny zarządza dynamicznie identyfikatorami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące zarządzania identyfikatorem; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie identyfikatorem; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające dynamiczne zarządzanie identyfikatorami].

IA-4(6)	**ZARZĄDZANIE IDENTYFIKATOREM | *ZARZĄDZANIE MIĘDZYORGANIZACYJNE***	
	CEL OCENY: *Określić, czy organizacja:*	
	IA-4(6)[1]	*definiuje organizacje zewnętrzne, z którymi należy koordynować zarządzanie międzyorganizacyjne identyfikatorami; oraz*
	IA-4(6)[2]	*koordynuje z organizacją zewnętrzną zarządzanie międzyorganizacyjne identyfikatorami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące zarządzania identyfikatorem; procedury dotyczące zarządzania kontami; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry].	

IA-4(6)	**ZARZĄDZANIE IDENTYFIKATOREM | *ZARZĄDZANIE MIĘDZYORGANIZACYJNE***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie identyfikatorem; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie identyfikatorem].

IA-4(7)	**ZARZĄDZANIE IDENTYFIKATOREM | *REJESTRACJA OSOBISTA***
	CEL OCENY: *Ustalenie, czy organizacja wymaga, aby proces rejestracji w celu otrzymania indywidualnego identyfikatora został przeprowadzony osobiście przez wyznaczony organ rejestrujący.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące zarządzania identyfikatorem; procedury dotyczące zarządzania kontami; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie identyfikatorem; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

IA-5	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA**	
	CEL OCENY: *Ustalić, czy organizacja zarządza autoryzacją systemów informacyjnych poprzez:*	
	IA-5(a)	*weryfikację, w ramach początkowego procesu uwierzytelnienia tożsamości, uczestniczących w procesie uwierzytelnienia:*
	IA-5(a)[1]	*osób;*
	IA-5(a)[2]	*grup;*
	IA-5(a)[3]	*ról; i/lub*
	IA-5(a)[4]	*urządzeń;*

IA-5	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA**		
	IA-5(b)	*ustanowienie wstępnej treści uwierzytelniającej odnoszącej się do osób uwierzytelnianych określonych przez organizację;*	
	IA-5(c)	*zapewnienie, że mechanizmy uwierzytelnienia mają wystarczającą siłę, która umożliwia ich wykorzystanie;*	
	IA-5(d)	**IA-5(d)[1]**	*ustanowienie i wprowadzenie w życie procedur administracyjnych dotyczących wstępnego uwierzytelnienia;*
		IA-5(d)[2]	*ustanowienie i wprowadzenie w życie procedur administracyjnych dla zagubionych/ujawnionych lub uszkodzonych elementów uwierzytelniania;*
		IA-5(d)[3]	*ustanowienie i wprowadzenie w życie procedur administracyjnych mających na celu unieważnienie metod i elementów uwierzytelniających;*
	IA-5(e)	*zmianę domyślnej zawartości metod uwierzytelnienia przed instalacją systemu informacyjnego;*	
	IA-5(f)	**IA-5(f)[1]**	*ustanowienie minimalnych ograniczeń w zakresie okresu używalności oraz warunków ponownego użycia metod uwierzytelniania;*
		IA-5(f)[2]	*ustanowienie maksymalnych ograniczeń w zakresie okresu używalności oraz warunków ponownego użycia metod uwierzytelniania;*
		IA-5(f)[3]	*ustanowienie warunków ponownego użycia metod uwierzytelniania;*
	IA-5(g)	**IA-5(g)[1]**	*określenie okresu czasu (według typu podmiotu uwierzytelniającego) na zmianę/zaktualizowanie podmiotów uwierzytelniających;*
		IA-5(g)[2]	*zmiana/odświeżenie dokumentów uwierzytelniających o określonym przez organizację okresie czasu według typu podmiotu uwierzytelniającego;*
	IA-5(h)	*ochronę treści uwierzytelniających przed nieuprawnionym:*	
		IA-5(h)[1]	*ujawnieniem;*
		IA-5(h)[2]	*modyfikacją;*

IA-5	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA**		
	IA-5(I)	**IA-5(I)[1]**	*wymaganie od osób fizycznych wdrażania i stosowania określonych metod zabezpieczeń urządzeń w celu zapewnienia uwierzytelniania;*
		IA-5(I)[2]	*posiadanie urządzeń wdrażających szczególne środki bezpieczeństwa w celu ochrony podmiotów świadczących usługi autoryzacji; oraz*
	IA-5(j)	*zmianę metod uwierzytelnienia kont grupowych / ról w przypadku zmiany członkostwa w tych kontach.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz rodzajów autoryzacji systemów informacyjnych; rejestry zabezpieczeń zmian związane z zarządzaniem uwierzytelnianiem systemów informacyjnych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wprowadzające zarządzanie metodami uwierzytelniania].		

IA-5(1)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *UWIERZYTELNIANIE OPARTE O HASŁA***		
	CEL OCENY: *Określić, czy do uwierzytelniania opartego o hasła:*		
	IA-5(1)(a)	**IA-5(1)(a)[1]**	*organizacja określa wymagania dotyczące wrażliwości;*
		IA-5(1)(a)[2]	*organizacja określa wymagania dotyczące liczby znaków;*
		IA-5(1)(a)[3]	*organizacja określa wymagania dotyczące kombinacji dużych i małych liter, cyfr i znaków specjalnych;*
		IA-5(1)(a)[4]	*organizacja określa minimalne wymagania dla każdego rodzaju znaków;*

IA-5(1)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *UWIERZYTELNIANIE OPARTE O HASŁA***		
		IA-5(1)(a)[5]	*system informacyjny wymusza minimalną złożoność haseł dla zdefiniowanych przez organizację wymagań dotyczących rozpoznawalności liter, liczby znaków, kombinacji wielkich liter, małych liter, cyfr i znaków specjalnych, w tym minimalne wymagania dla każdego typu;*
	IA-5(1)(b)	**IA-5(1)(b)[1]**	*organizacja określa minimalną liczbę zmienianych znaków, które mają być egzekwowane przy tworzeniu nowych haseł;*
		IA-5(1)(b)[2]	*system informacyjny wymusza, co najmniej, zdefiniowaną przez organizację minimalną liczbę znaków, które muszą być zmienione przy tworzeniu nowych haseł;*
	IA-5(1)(c)	*system informacyjny przechowuje i przekazuje tylko hasła chronione kryptograficznie;*	
	IA-5(1)(d)	**IA-5(1)(d)[1]**	*organizacja egzekwuje ograniczenia dotyczące minimalnego okresu ważności haseł;*
		IA-5(1)(d)[2]	*organizacja egzekwuje ograniczenia dotyczące maksymalnego okresu ważności haseł;*
		IA-5(1)(d)[3]	*system informacyjny wprowadza minimalne okresy ważności haseł, w odniesieniu do haseł zdefiniowanych przez organizację;*
		IA-5(1)(d)[4]	*system informacyjny wprowadza maksymalne okresy ważności haseł, w odniesieniu do haseł zdefiniowanych przez organizację;*
	IA-5(1)(e)	**IA-5(1)(e)[1]**	*organizacja określa liczbę wystąpień haseł, po której zabronione jest ponowne użycie hasła;*
		IA-5(1)(e)[2]	*system informacyjny zakazuje ponownego wykorzystania hasła w odniesieniu do zdefiniowanej przez organizację liczby generacji haseł; oraz*
	IA-5(1)(f)	*system informacyjny umożliwia korzystanie z tymczasowego hasła do logowania się do systemu z wymuszeniem natychmiastowej zmiany na hasło stałe.*	

IA-5(1)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *UWIERZYTELNIANIE OPARTE O HASŁA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; polityka wprowadzania haseł; procedury zarządzania metodami uwierzytelniania; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; konfiguracje haseł i związana z nimi dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie uwierzytelnianiem opartym na hasłach].

IA-5(2)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *UWIERZYTELNIANIE OPARTE O INFRASTRUKTURĘ KLUCZA PUBLICZNEGO (PKI)***		
	CEL OCENY: *ustalić, czy system informacyjny, do uwierzytelniania opartego o infrastrukturę klucza publicznego:*		
	IA-5(2)(a)	**IA-5(2)(a)[1]**	*zatwierdza certyfikaty, konstruując ścieżkę certyfikacji do zaakceptowanej kotwicy zaufania;*
		IA-5(2)(a)[2]	*poświadcza certyfikację, weryfikując ścieżkę certyfikacji do akceptowanej kotwicy ufającej;*
		IA-5(2)(a)[3]	*uwzględnia sprawdzanie informacji o statusie certyfikatu podczas konstruowania i weryfikowania ścieżki certyfikacji;*
	IA-5(2)(b)	*wymusza autoryzowany dostęp do odpowiedniego klucza prywatnego;*	
	IA-5(2)(c)	*mapuje uwierzytelnioną tożsamość do konta osoby lub grupy; oraz*	
	IA-5(2)(d)	*wdraża lokalną pamięć podręczną unieważnionych danych w celu obsługi ścieżki wykrywania i sprawdzania w przypadku braku dostępu sieciowego do tych unieważnionych danych.*	

IA-5(2)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *UWIERZYTELNIANIE OPARTE O INFRASTRUKTURĘ KLUCZA PUBLICZNEGO (PKI)***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry weryfikacji certyfikatów PKI; listy unieważniające certyfikację PKI; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie uwierzytelnianiem w oparciu o PKI; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie metodami uwierzytelniania opartymi o PKI].

IA-5(3)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *REJESTRACJA OSOBISTA LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ***		
	CEL OCENY: *Określić, czy organizacja:*		
	IA-5(3)[1]	*określa rodzaje i/lub szczególne rodzaje weryfikatorów, które mają być przyjmowane osobiście lub przez zaufaną osobę trzecią;*	
	IA-5(3)[2]	*definiuje organ rejestrujący, który nadzoruje proces rejestracji w odniesieniu do przyjmowania określonych przez organizację rodzajów i/lub specyfikacji określonych weryfikatorów;*	
	IA-5(3)[3]	*definiuje personel lub role odpowiedzialne za udzielanie zezwoleń organowi rejestracyjnemu określonemu przez organizację;*	
	IA-5(3)[4]	*określa, czy proces rejestracji ma być przeprowadzony:*	
		IA-5(3)[4][a]	*osobiście; lub*
		IA-5(3)[4][b]	*przez zaufaną trzecią stronę; oraz*
	IA-5(3)[5]	*wymaga, aby proces rejestracji w celu otrzymania określonych przez organizację rodzajów i/lub określonych autoryzacji był przeprowadzony osobiście lub przez zaufaną stronę trzecią przed organem rejestracyjnym określonym przez organizację, za zgodą i autoryzacją upoważnionego personelu lub ról określonych przez organizację.*	

IA-5(3)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *REJESTRACJA OSOBISTA LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; proces rejestracji w celu otrzymania autoryzacji systemów informacyjnych; lista autoryzacji wymagających rejestracji osobistej; lista autoryzacji wymagających rejestracji przez zaufaną osobę trzecią; dokumentacja rejestracyjna autoryzacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; organ rejestracyjny; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

IA-5(4)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *AUTOMATYCZNE WSPARCIE OKREŚLANIA SIŁY HASŁA***	
	CEL OCENY: *Określić, czy organizacja:*	
	IA-5(4)[1]	*określa wymogi, jakie muszą spełniać podmioty autoryzujące hasła; oraz*
	IA-5(4)[2]	*używa zautomatyzowanych narzędzi do określenia, czy autoryzacja haseł jest wystarczająco silna, aby spełnić wymagania określone przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zautomatyzowane narzędzia do oceny autoryzacji haseł; wyniki oceny siły hasła; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie uwierzytelnianiem opartym na hasłach; zautomatyzowane narzędzia do określania siły hasła].	

IA-5(5)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *ZMIANA METODY UWIERZYTELNIANIA PRZED DOSTAWĄ***	
	CEL OCENY: *Ustalenie, czy organizacja wymaga od deweloperów/instalatorów komponentów systemu informacyjnego:*	
	IA-5(5)[1]	*dostarczenia unikatowych uwierzytelnień przed dostawą/instalacją; lub*
	IA-5(5)[2]	*zmiany domyślnych elementów uwierzytelniających przed dostawą/instalacją.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; polityka nabywania systemów i usług; procedury zarządzania metodami uwierzytelniania; procedury dotyczące włączenia wymogów bezpieczeństwa do procesu zakupów; dokumentacja zakupów; kontrakty na zakup systemów informacyjnych lub usług; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji odpowiedzialny za bezpieczeństwo systemu informacyjnego, zakupy i zawieranie umów; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wprowadzające zarządzanie metodami uwierzytelniania].	

IA-5(6)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *OCHRONA METOD UWIERZYTELNIANIA***
	CEL OCENY: *Ustalić, czy organizacja chroni wystawców uwierzytelnień proporcjonalnie do kategorii bezpieczeństwa informacji, do których umożliwia dostęp wystawca uwierzytelnienia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; dokumentacja kategoryzacji bezpieczeństwa systemu informacyjnego; ocena bezpieczeństwa zabezpieczeń wystawców uwierzytelnień; wyniki oceny ryzyka; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji wdrażający i/lub utrzymujący zabezpieczenia wystawców uwierzytelnień; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci].

IA-5(6)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *OCHRONA METOD UWIERZYTELNIANIA***
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wprowadzające zarządzanie metodami uwierzytelniania; zautomatyzowane mechanizmy ochrony wystawców uwierzytelnień].

IA-5(7)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *BRAK WBUDOWANYCH NIEZASZYFROWANYCH STATYCZNYCH ELEMENTÓW UWIERZYTELNIANIA***	
	CEL OCENY: *Ustalić, czy organizacja zapewnia, że niezaszyfrowane statyczne urządzenia uwierzytelniające nie są:*	
	IA-5(7)[1]	*wbudowane w aplikacje;*
	IA-5(7)[2]	*wbudowane w skrypty dostępu; lub*
	IA-5(7)[3]	*zapisane na klawiszach funkcyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; skrypty dostępu logicznego; przeglądy kodów aplikacji do wykrywania nieszyfrowanych statycznych elementów uwierzytelniania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wprowadzające zarządzanie metodami uwierzytelniania; zautomatyzowane mechanizmy wdrażania uwierzytelniania w aplikacjach].	

IA-5(8)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *JEDNO KONTO W WIELU SYSTEMACH INFORMACYJNYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	IA-5(8)[1]	*określa środki bezpieczeństwa służące do zarządzania ryzykiem zagrożeń ze względu na posiadanie przez osoby kont w wielu systemach informacyjnych; oraz*
	IA-5(8)[2]	*wdraża określone przez organizację środki bezpieczeństwa w celu zarządzania ryzykiem zagrożeń bezpieczeństwa w związku z posiadaniem przez osoby kont w wielu systemach informacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; plan bezpieczeństwa; wykaz osób posiadających konta w wielu systemach informacyjnych; wykaz środków bezpieczeństwa mających na celu zarządzanie ryzykiem zagrożeń bezpieczeństwa w związku z posiadaniem przez osoby kont w wielu systemach informacyjnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zabezpieczenia w zakresie zarządzania metodami uwierzytelniania].	

IA-5(9)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *ZARZĄDZANIE DANYMI UWIERZYTELNIAJĄCYMI MIĘDZY ORGANIZACJAMI***	
	CEL OCENY: *Określić, czy organizacja:*	
	IA-5(9)[1]	*definiuje organizacje zewnętrzne, z którymi należy koordynować międzyorganizacyjne zarządzanie referencjami; oraz*
	IA-5(9)[2]	*koordynuje z określoną organizacją zewnętrzną zarządzanie poświadczeniami.*

IA-5(9)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *ZARZĄDZANIE DANYMI UWIERZYTELNIAJĄCYMI MIĘDZY ORGANIZACJAMI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; procedury dotyczące zarządzania kontami; plan bezpieczeństwa; umowy z zakresu bezpieczeństwa informacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zabezpieczenia w zakresie zarządzania metodami uwierzytelniania].

IA-5(10)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *DYNAMICZNE KOJARZENIE DANYCH UWIERZYTELNIAJĄCYCH***
	CEL OCENY: *Ustalić, czy system informacyjny dynamicznie weryfikuje tożsamość.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące zarządzania identyfikatorem; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; zautomatyzowane mechanizmy zapewniające dynamiczne powiązanie identyfikatorów i podmiotów uwierzytelniających; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie identyfikatorem; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące zarządzanie możliwościami identyfikatorów; zautomatyzowane mechanizmy realizujące dynamiczne dostarczanie identyfikatorów].

IA-5(11)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *UWIERZYTELNIANIE PRZY UŻYCIU TOKENA***	
	CEL OCENY: *Określić, czy uwierzytelnianie przy użyciu tokena:*	
	IA-5(11)[1]	*organizacja określa wymagania jakościowe, które muszą być spełnione przez tokeny; oraz*
	IA-5(11)[2]	*system informacyjny wykorzystuje mechanizmy, które spełniają zdefiniowane przez organizację wymagania jakościowe dotyczące tokenów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; zautomatyzowane mechanizmy wykorzystujące uwierzytelnianie do systemu informacyjnego przy użyciu tokena; wykaz wymagań jakościowych dla tokenów; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące sprzętowe zarządzanie metodami uwierzytelniania przy użyciu tokena].	

IA-5(12)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *UWIERZYTELNIANIE BIOMETRYCZNE***	
	CEL OCENY: *Ustalić, czy w przypadku uwierzytelniania biometrycznego:*	
	IA-5(12)[1]	*organizacja określa wymogi jakości biometrycznej, które należy spełnić; oraz*
	IA-5(12)[2]	*system informacyjny wykorzystuje mechanizmy, które spełniają określone przez organizację wymagania jakości biometrycznej.*

IA-5(12)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *UWIERZYTELNIANIE BIOMETRYCZNE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; zautomatyzowane mechanizmy wykorzystujące uwierzytelnianie oparte na danych biometrycznych; wykaz wymogów jakości biometrycznej; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie biometrycznymi metodami uwierzytelniania].

IA-5(13)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *PRZEDAWNIENIE BUFOROWANYCH ELEMENTÓW UWIERZYTELNIANIA***	
	CEL OCENY: *Określić, czy:*	
	IA-5(13)[1]	*organizacja określa okres czasu, po upływie którego system informacyjny ma zabraniać używania buforowanych elementów uwierzytelniania; oraz*
	IA-5(13)[2]	*system informacyjny uniemożliwia korzystanie z buforowanych elementów uwierzytelniania, po upływie określonego przez organizację okresu czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów].	

IA-5(13)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *PRZEDAWNIENIE BUFOROWANYCH ELEMENTÓW UWIERZYTELNIANIA***
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wprowadzające zarządzanie metodami uwierzytelniania].

IA-5(14)	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | *ZARZĄDZANIE ZAWARTOŚCIĄ ZAUFANYCH MAGAZYNÓW INFRASTRUKTURY KLUCZA PUBLICZNEGO (PKI)***	
	CEL OCENY: *określić, czy organizacja, w przypadku uwierzytelniania opartego na infrastrukturze klucza publicznego, stosuje w całej organizacji metodologię zarządzania zawartością magazynów zaufania infrastruktury klucza publicznego zainstalowanych na wszystkich platformach, w tym w:*	
	IA-5(14)[1]	sieciach;
	IA-5(14)[2]	systemach operacyjnych;
	IA-5(14)[3]	przeglądarkach; oraz
	IA-5(14)[4]	aplikacjach.
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury zarządzania metodami uwierzytelniania; plan bezpieczeństwa; metodologia organizacyjna zarządzanie zawartością zaufanych magazynów infrastruktury klucza publicznego na wszystkich zainstalowanych platformach; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja architektury bezpieczeństwa przedsiębiorstwa; dokumentacja struktury organizacyjnej; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zarządzanie metodami uwierzytelniania; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące funkcję zarządzania metodami uwierzytelniania PKI; zautomatyzowane mechanizmy wspierające i/lub implementujące funkcję magazynu zaufania PKI].	

IA-5(15)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *WYKORZYSTANIE PROFILI WYDAWANYCH PRZEZ STOSOWNE INSTYTUCJE***
	[Usunięto]

IA-6	**OCHRONA PROCESU UWIERZYTELNIANIA**
	CEL OCENY: *Ustalić, czy system informacyjny "ukrywa" informacje zwrotne dotyczące uwierzytelnienia podczas procesu uwierzytelniania w celu ochrony informacji przed ewentualnym wykorzystaniem/użyciem przez osoby nieupoważnione.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące informacji zwrotnych od podmiotów autoryzujących; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające „ukrywanie" informacji zwrotnych dotyczących uwierzytelniania podczas procesu uwierzytelniania].

IA-7	**UWIERZYTELNIANIE MODUŁU KRYPTOGRAFICZNEGO**
	CEL OCENY: *Ustalić, czy system informacyjny wdraża mechanizmy uwierzytelniania do modułu kryptograficznego, które spełniają wymagania obowiązujących przepisów, rozporządzeń, dyrektyw, polityk, regulacji, standardów i wytycznych dotyczących takiego uwierzytelniania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące uwierzytelniania modułu kryptograficznego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

IA-7	**UWIERZYTELNIANIE MODUŁU KRYPTOGRAFICZNEGO**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za uwierzytelnianie modułu kryptograficznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące uwierzytelnianie modułów kryptograficznych].

IA-8	**IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)**
	CEL OCENY: *Ustalenie, czy system informacyjny w sposób jednoznaczny identyfikuje i uwierzytelnia użytkowników spoza organizacji (lub procesy realizowane w ich imieniu).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz kont systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacji odpowiedzialny za zarządzanie kontami]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcję identyfikacji i uwierzytelniania].

IA-8(1)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *AKCEPTACJA POŚWIADCZEŃ TOŻSAMOŚCI WYDANYCH PRZEZ INNE ORGANIZACJE***	
	CEL OCENY: *Ustalić, czy system informacyjny:*	
	IA-8(1)[1]	*akceptuje poświadczenia weryfikacji tożsamości osobistej z innych organizacji; oraz*
	IA-8(1)[2]	*weryfikuje elektronicznie dane uwierzytelniające dotyczące weryfikacji tożsamości osobistej z innych agencji.*

IA-8(1)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *AKCEPTACJA POŚWIADCZEŃ TOŻSAMOŚCI WYDANYCH PRZEZ INNE ORGANIZACJE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; zapisy z weryfikacji karty dostępowej; ewidencja kart dostępowych; autoryzacje kart dostępowych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów; personel organizacji odpowiedzialny za zarządzanie kontami]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcję identyfikacji i uwierzytelniania; zautomatyzowane mechanizmy akceptujące i weryfikujące poświadczenia identyfikatorów].

IA-8(2)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *AKCEPTACJA POŚWIADCZEŃ STRON TRZECICH***
	CEL OCENY: *Ustalić, czy system informacyjny akceptuje tylko poświadczenia osób trzecich akceptowane i zatwierdzone zgodnie z procedurami przyjętymi w organizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz zatwierdzonych przez organizację produktów, komponentów lub usług uwierzytelniających strony trzecie, nabytych i wdrożonych przez organizację; zapisy z weryfikacji uwierzytelniającej strony trzeciej; poświadczenia uwierzytelniające strony trzecie akceptowane przez organizację; zezwolenia uwierzytelniające strony trzecie; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów; personel organizacji odpowiedzialny za zarządzanie kontami].

IA-8(2)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *AKCEPTACJA POŚWIADCZEŃ STRON TRZECICH***
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcję identyfikacji i uwierzytelniania; zautomatyzowane mechanizmy, dopuszczające poświadczenia zatwierdzone przez organizację].

IA-8(3)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *WYKORZYSTANIE CERTYFIKOWANYCH PRODUKTÓW***	
	CEL OCENY: *Określić, czy organizacja:*	
	IA-8(3)[1]	*definiuje systemy informacyjne, w których tylko zatwierdzone przez organizację części składowe systemu informacyjnego mogą być stosowane do przyjmowania poświadczeń stron trzecich; oraz*
	IA-8(3)[2]	*stosuje tylko zatwierdzone przez organizację komponenty systemu informacyjnego w zdefiniowanych przez organizację systemach informacyjnych, akceptujące poświadczenia stron trzecich.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; polityka nabywania systemów i usług; procedury dotyczące identyfikacji i uwierzytelniania użytkowników; procedura dotycząca włączenia wymogów bezpieczeństwa do procesów zakupu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; poświadczenia weryfikacji certyfikatów przez strony trzecie; poświadczenia autoryzacji certyfikatów przez strony trzecie; rejestry poświadczeń przez strony trzecie; wykaz zatwierdzonych przez organizację komponentów systemu informacyjnego nabytych i wdrożonych przez organizację; dokumentacja zakupów; kontrakty na zakup systemów informacyjnych lub usług; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; administratorzy systemu/sieci; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji zajmujący się bezpieczeństwem systemu informacyjnego, pozyskiwaniem i realizacją kontraktów]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcję identyfikacji i uwierzytelniania].	

IA-8(4)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *WYKORZYSTANIE PROFILI WYDAWANYCH PRZEZ STOSOWNE INSTYTUCJE***
	[Usunięto]

IA-8(5)	**IDENTYFIKACJA I UWIERZYTELNIANIE | *AKCEPTACJA POŚWIADCZEŃ OSOBISTEJ WERYFIKACJI TOŻSAMOŚCI***
	[Usunięto]

IA-9	**IDENTYFIKACJA I UWIERZYTELNIANIE USŁUGI**	
	CEL OCENY: *Określić, czy organizacja:*	
	IA-9[1]	*definiuje usługi systemu informacyjnego, które mają być identyfikowane i uwierzytelniane przy użyciu środków bezpieczeństwa;*
	IA-9[2]	*definiuje zabezpieczenia, które mają być stosowane do identyfikacji i uwierzytelniania usług systemu informacyjnego zdefiniowanych przez organizację; oraz*
	IA-9[3]	*identyfikuje i uwierzytelnia usługi systemu informacyjnego zdefiniowane przez organizację przy użyciu określonych przez organizację środków bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania usługi; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; środki bezpieczeństwa wykorzystywane do identyfikacji i uwierzytelniania usług systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów; personel organizacji odpowiedzialny za identyfikację i uwierzytelnianie]. **Test**: [*wybierz spośród:* Środki bezpieczeństwa wprowadzające identyfikację i uwierzytelnianie usług].	

IA-9(1)	**IDENTYFIKACJA I UWIERZYTELNIANIE USŁUGI | *WYMIANA INFORMACJI***	
	CEL OCENY: *Ustalić, czy organizacja zapewnia dostawcom usług:*	
	IA-9(1)[1]	*odbieranie informacji identyfikacyjnych i uwierzytelniających;*
	IA-9(1)[2]	*sprawdzanie informacji identyfikacyjnych i uwierzytelniających; oraz*
	IA-9(1)[3]	*przesyłanie informacji identyfikacyjnych i uwierzytelniających.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania usługi; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za identyfikację i uwierzytelnianie; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; dostawcy usług]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementacji identyfikacji i uwierzytelniania usług].	

IA-9(2)	**IDENTYFIKACJA I UWIERZYTELNIANIE USŁUGI | *PRZEKAZYWANIE DECYZJI O POZYTYWNEJ IDENTYFIKACJI I UWIERZYTELNIENIU***	
	CEL OCENY: *Określić, czy organizacja:*	
	IA-9(2)[1]	*definiuje usługi, dla których decyzje dotyczące identyfikacji i uwierzytelniania są przesyłane pomiędzy tymi usługami, zgodnie z zasadami ustanowionymi przez organizację; oraz*
	IA-9(2)[2]	*zapewnia, że decyzje dotyczące identyfikacji i uwierzytelniania są przekazywane pomiędzy zdefiniowanymi przez organizację usługami, zgodnie z jej polityką organizacyjną.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące identyfikacji i uwierzytelniania usługi; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; rekordy przekazu; rekordy weryfikacji przekazu; zasady	

IA-9(2)	**IDENTYFIKACJA I UWIERZYTELNIANIE USŁUGI | *PRZEKAZYWANIE DECYZJI O POZYTYWNEJ IDENTYFIKACJI I UWIERZYTELNIENIU***
	identyfikacji i uwierzytelniania decyzji o przekazie między komórkami organizacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za identyfikację i uwierzytelnianie; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementacji identyfikacji i uwierzytelniania usług].

IA-10	**IDENTYFIKACJA I UWIERZYTELNIANIE ADAPTACYJNE**	
	CEL OCENY: *Określić, czy organizacja:*	
	IA-10[1]	*określa szczególne okoliczności lub sytuacje, które wymagają od osób mających dostęp do systemu informacyjnego stosowania uzupełniających technik lub mechanizmów uwierzytelniania;*
	IA-10[2]	*definiuje techniki lub mechanizmy uwierzytelniania uzupełniającego, które mają być stosowane przy uzyskiwaniu dostępu do systemu informacyjnego w szczególnych okolicznościach lub sytuacjach określonych przez organizację; oraz*
	IA-10[3]	*wymaga, aby osoby mające dostęp do systemu informacyjnego stosowały określone przez organizację techniki lub mechanizmy dodatkowego uwierzytelniania w określonych okolicznościach lub sytuacjach określonych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące adaptacyjnych/uzupełniających technik lub mechanizmów identyfikacji i uwierzytelniania; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dodatkowe techniki lub mechanizmy identyfikacji i uwierzytelniania; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów; personel organizacji odpowiedzialny za identyfikację i uwierzytelnianie].	

IA-10	**IDENTYFIKACJA I UWIERZYTELNIANIE ADAPTACYJNE**
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcję identyfikacji i uwierzytelniania].

IA-11	**PONOWNE UWIERZYTELNIANIE**	
	CEL OCENY: *Określić, czy organizacja:*	
	IA-11[1]	*określa okoliczności lub sytuacje wymagające ponownego uwierzytelnienia;*
	IA-11[2]	*wymaga od użytkowników ponownego uwierzytelnienia, gdy okoliczności lub sytuacje określone przez organizację wymagają ponownego uwierzytelnienia; oraz*
	IA-11[3]	*wymaga ponownego uwierzytelnienia urządzeń, gdy określone okoliczności lub sytuacje organizacyjne wymagają ponownego uwierzytelnienia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka identyfikacji i uwierzytelniania; procedury dotyczące ponownego uwierzytelniania użytkowników i urządzeń; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz okoliczności lub sytuacji wymagających ponownego uwierzytelnienia; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za eksploatację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów; personel organizacji odpowiedzialny za identyfikację i uwierzytelnianie]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcję identyfikacji i uwierzytelniania].	

KATEGORIA IR - REAGOWANIE NA INCYDENTY

IR-1	**POLITYKA I PROCEDURY REAGOWANIA NA INCYDENTY**			
	CEL OCENY: *Określić, czy organizacja:*			
	IR-1(a)(1)	**IR-1(a)(1)[1]**	*opracowuje i dokumentuje politykę reagowania na incydenty, która dotyczy:*	
			IR-1(a)(1)[1][a]	*celu;*
			IR-1(a)(1)[1][b]	*zakresu stosowania;*
			IR-1(a)(1)[1][c]	*ról;*
			IR-1(a)(1)[1][d]	*odpowiedzialności;*
			IR-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			IR-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			IR-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		IR-1(a)(1)[2]	*określa personel lub role, wśród których ma być rozpowszechniana polityka reagowania na incydenty;*	
		IR-1(a)(1)[3]	*rozpowszechnia politykę reagowania na incydenty wśród personelu określonego przez organizację lub ról;*	
	IR-1(a)(2)	**IR-1(a)(2)[1]**	*opracowuje i dokumentuje procedury w celu ułatwienia wdrażania polityki reagowania na incydenty i związanych z nią zabezpieczeń reagowania na incydenty;*	
		IR-1(a)(2)[2]	*określa personel lub rolę, wśród których procedury mają być rozpowszechniane;*	
		IR-1(a)(2)[3]	*rozpowszechnia procedury wśród personelu zdefiniowanego przez organizację lub wśród ról;*	
	IR-1(b)(1)	**IR-1(b)(1)[1]**	*określa częstotliwość przeglądu i aktualizacji aktualnej polityki reagowania na incydenty;*	

IR-1	**POLITYKA I PROCEDURY REAGOWANIA NA INCYDENTY**		
		IR-1(b)(1)[2]	*opiniuje i aktualizuje bieżącą politykę reagowania na incydenty z częstotliwością określoną przez organizację;*
	IR-1(b)(2)	**IR-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji bieżących procedur reagowania na incydenty; oraz*
		IR-1(b)(2)[2]	*opiniuje i aktualizuje bieżące procedury reagowania na incydenty z określoną przez organizację częstotliwością.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury reagowania na incydenty; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za procedury reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

IR-2	**SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY**		
	CEL OCENY: *Określić, czy organizacja:*		
	IR-2(a)	**IR-2(a)[1]**	*określa okres czasu, w którym należy przeprowadzić szkolenie w zakresie reagowania na incydenty dla użytkowników systemu informacyjnego, którzy przyjmują na siebie rolę lub odpowiedzialność w zakresie reagowania na incydenty;*
		IR-2(a)[2]	*zapewnia szkolenie w zakresie reagowania na incydenty użytkownikom systemu informacyjnego zgodnie z przydzielonymi rolami i obowiązkami w ramach określonego przez organizację okresu czasu, w którym przyjmują oni rolę lub odpowiedzialność w zakresie reagowania na incydenty;*
	IR-2(b)	*prowadzi szkolenia w zakresie reagowania na incydenty wśród użytkowników systemów informacyjnych zgodnie z przypisanymi rolami i obowiązkami, gdy wymagają tego zmiany w systemie informacyjnym;*	
	IR-2(c)	**IR-2(c)[1]**	*określa częstotliwość przeprowadzania szkoleń przypominających w zakresie reagowania na incydenty wśród użytkowników systemów informacyjnych zgodnie z przypisanymi im rolami lub odpowiedzialnością; oraz*

IR-2	**SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY**		
		IR-2(c)[2]	*po szkoleniu wstępnym w zakresie reagowania na incydenty, prowadzi szkolenia aktualizujące w zakresie reagowania na incydenty skierowane do użytkowników systemów informacyjnych zgodnie z przydzielonymi rolami i obowiązkami oraz z ustaloną przez organizację częstotliwością szkoleń aktualizujących.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące szkoleń w zakresie reagowania na incydenty; program szkolenia w zakresie reagowania na incydenty; materiały szkoleniowe dotyczące reagowania na incydenty; plan bezpieczeństwa; plan reagowania na incydenty; plan bezpieczeństwa; ewidencja szkoleń w zakresie reagowania na incydenty; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji przeszkolony w zakresie reagowania na incydenty i odpowiedzialny za działania operacyjne; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

IR-2(1)	**SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | *WYDARZENIA SYMULOWANE***
	CEL OCENY: *określić, czy organizacja włącza wydarzenia symulowane do szkoleń w zakresie reagowania na incydenty w celu zapewnienia skutecznej reakcji personelu w sytuacjach kryzysowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące szkoleń w zakresie reagowania na incydenty; program szkolenia w zakresie reagowania na incydenty; materiały szkoleniowe dotyczące reagowania na incydenty; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji przeszkolony w zakresie reagowania na incydenty i odpowiedzialny za działania operacyjne; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy, wspierające lub wdrażające wydarzenia symulowane do celów szkolenia w zakresie reagowania na incydenty].

IR-2(2)	**SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | *ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE***
	CEL OCENY: *Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy, celem zapewnienia dokładniejszego i bardziej realistycznego środowisko szkolenia w zakresie reagowania na incydenty.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące szkoleń w zakresie reagowania na incydenty; program szkolenia w zakresie reagowania na incydenty; materiały szkoleniowe dotyczące reagowania na incydenty; zautomatyzowane mechanizmy wspomagające szkolenie w zakresie reagowania na incydenty; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji przeszkolony w zakresie reagowania na incydenty i odpowiedzialny za działania operacyjne; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy, zapewniające gruntowne i realistyczne szkolenie w zakresie reagowania na incydenty środowiskowe].

IR-3	**TESTOWANIE REAGOWANIA NA INCYDENTY**	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-3[1]	*określa testy reakcji na incydent w celu zbadania Zdolności systemu informacyjnego do reagowania na incydent;*
	IR-3[2]	*definiuje częstotliwość testowania Zdolności reagowania na incydenty systemów informacyjnych; oraz*
	IR-3[3]	*testuje zdolność systemu informacyjnego do reagowania na incydenty z częstotliwością określoną przez organizację, wykorzystując zdefiniowane przez organizację testy w celu określenia skuteczności reagowania na incydenty i dokumentuje ich wyniki.*

IR-3	**TESTOWANIE REAGOWANIA NA INCYDENTY**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; polityka planowania awaryjnego; procedury dotyczące testowania reagowania na incydenty; procedury dotyczące testowania planu ciągłości działania; materiały do testowania reagowania na incydenty; wyniki testu reakcji na incydent; plan testu reakcji na incydent; plan reagowania na incydenty; plan ciągłości działania; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za badanie reakcji na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

IR-3(1)	**TESTOWANIE REAGOWANIA NA INCYDENTY | *TESTOWANIE AUTOMATYCZNE***
	CEL OCENY: *Ustalenie, czy organizacja stosuje zautomatyzowane mechanizmy w celu dokładniejszego i skuteczniejszego testowania Zdolności reagowania na incydenty.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; polityka planowania awaryjnego; procedury dotyczące testowania reagowania na incydenty; procedury dotyczące testowania planu ciągłości działania; dokumentacja testowania reagowania na incydenty; wyniki testu reakcji na incydent; plan testu reakcji na incydenty; plan reagowania na incydenty; plan ciągłości działania; plan bezpieczeństwa; zautomatyzowane mechanizmy wspomagające testy reagowania na incydenty; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za badanie reakcji na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy, umożliwiające dokładniejsze i skuteczniejsze testowanie Zdolności reagowania na incydenty].

IR-3(2)	**TESTOWANIE REAGOWANIA NA INCYDENTY | *KOORDYNACJA Z POWIĄZANYMI PLANAMI***
	CEL OCENY: *Ustalić, czy organizacja koordynuje testowanie reagowania na incydenty z elementami organizacyjnymi odpowiedzialnymi za powiązane plany.*

IR-3(2)	**TESTOWANIE REAGOWANIA NA INCYDENTY | *KOORDYNACJA Z POWIĄZANYMI PLANAMI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; polityka planowania awaryjnego; procedury dotyczące testowania reagowania na incydenty; dokumentacja testowania reagowania na incydenty; plany reagowania na incydenty; plany ciągłości działania; plany awaryjne; plany odtworzenia po katastrofie; plany kontynuacji operacji; plany komunikacji kryzysowej; plany infrastruktury krytycznej; plany ewakuacji; plany bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za badanie reakcji na incydenty; personel organizacji odpowiedzialny za testowanie planów organizacyjnych związanych z testowaniem reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

IR-4	**OBSŁUGA INCYDENTÓW**			
	CEL OCENY: *Określić, czy organizacja:*			
	IR-4(a)	*implementuje możliwość obsługi incydentów bezpieczeństwa, która obejmuje*		
		IR-4(a)[1]	*przygotowanie;*	
		IR-4(a)[2]	*wykrywanie i analizę;*	
		IR-4(a)[3]	*izolację;*	
		IR-4(a)[4]	*likwidację;*	
		IR-4(a)[5]	*odzyskiwanie;*	
	IR-4(b)	*koordynuje działania związane z obsługą incydentów z działaniami w zakresie planowania awaryjnego;*		
	IR-4(c)	**IR-4(c)[1]**	*uwzględnia wnioski wyciągnięte z bieżących działań obsługi incydentów związanych z:*	
			IR-4(c)[1][a]	*procedurami reagowania na incydenty;*
			IR-4(c)[1][b]	*szkoleniem;*
			IR-4(c)[1][c]	*testowaniem/ćwiczeniami;*

<table>
<tr><td colspan="5">IR-4 OBSŁUGA INCYDENTÓW</td></tr>
<tr><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4">IR-4(c)[2]</td><td colspan="2">wprowadza w życie wynikające z tego zmiany w zakresie:</td></tr>
<tr><td>IR-4(c)[2][a]</td><td>procedur reagowania na incydenty;</td></tr>
<tr><td>IR-4(c)[2][b]</td><td>szkolenia; oraz</td></tr>
<tr><td>IR-4(c)[2][c]</td><td>testowania/ćwiczeń.</td></tr>
<tr><td></td><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka reagowania na incydenty; polityka planowania awaryjnego; procedury dotyczące obsługi incydentów; plan reagowania na incydenty; plan ciągłości działania; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za planowanie awaryjne; personel organizacji odpowiedzialny za bezpieczeństwo informacji].
Test: [wybierz spośród: Zdolność organizacji do obsługi incydentów].</td></tr>
</table>

<table>
<tr><td>IR-4(1)</td><td colspan="4">OBSŁUGA INCYDENTÓW | AUTOMATYCZNE PROCESY OBSŁUGI ZDARZEŃ</td></tr>
<tr><td></td><td colspan="4">CEL OCENY:
Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy wspomagające proces obsługi incydentów.</td></tr>
<tr><td></td><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; zautomatyzowane mechanizmy wspomagające obsługę incydentów; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji].
Test: [wybierz spośród: Zautomatyzowane mechanizmy wspierające lub wdrażające proces obsługi incydentów].</td></tr>
</table>

IR-4(2)	**OBSŁUGA INCYDENTÓW | *DYNAMICZNA REKONFIGURACJA***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-4(2)[1]	*definiuje elementy systemu informacyjnego, które mają być dynamicznie rekonfigurowane, jako elementy Zdolności do reagowania na incydenty; oraz*
	IR-4(2)[2]	*obejmuje dynamiczną rekonfigurację zdefiniowanych przez organizację komponentów systemu informacyjnego w ramach Zdolności reagowania na incydenty.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; zautomatyzowane mechanizmy wspomagające obsługę wykazu incydentów elementów systemu, które mają być dynamicznie rekonfigurowane w ramach Zdolności reagowania na incydenty; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące dynamiczną rekonfigurację komponentów w ramach reagowania na incydenty].	

IR-4(3)	**OBSŁUGA INCYDENTÓW | *CIĄGŁOŚĆ OPERACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-4(3)[1]	*definiuje klasy incydentów wymagających podjęcia określonych przez organizację działań;*
	IR-4(3)[2]	*definiuje działania, które należy podjąć w odpowiedzi na określone przez organizację klasy incydentów; oraz*
	IR-4(3)[3]	*identyfikuje zdefiniowane przez organizację klasy incydentów i zdefiniowane przez organizację działania, które należy podjąć w odpowiedzi na klasy incydentów, w celu zapewnienia kontynuacji misji organizacyjnych i funkcji biznesowych.*

IR-4(3)	**OBSŁUGA INCYDENTÓW | *CIĄGŁOŚĆ OPERACJI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; plan reagowania na incydenty; plan bezpieczeństwa; wykaz klas incydentów; wykaz podejmowanych działań w zakresie reagowania na incydenty; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy, wspierające i/lub wdrażające ciągłość operacji].

IR-4(4)	**OBSŁUGA INCYDENTÓW | *KORELACJA INFORMACJI***
	CEL OCENY: *Ustalenie, czy organizacja koreluje informacje o incydentach z indywidualnymi reakcjami na incydenty, w celu osiągnięcia ogólnoorganizacyjnej perspektywy w zakresie świadomości i reakcji na incydenty.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; plan reagowania na incydenty; plan bezpieczeństwa; zautomatyzowane mechanizmy wspomagające korelację zdarzeń i incydentów; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dzienniki korelacji zarządzania incydentami; dzienniki korelacji zarządzania zdarzeniami; dzienniki korelacji informacji dotyczących bezpieczeństwa i zarządzania zdarzeniami; sprawozdania z korelacji zarządzania incydentami; sprawozdania z korelacji zarządzania zdarzeniami; sprawozdania z korelacji informacji dotyczących bezpieczeństwa i zarządzania zdarzeniami; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji, z którym należy skorelować informacje o incydencie i indywidualne reakcje na incydent]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące korelacji informacji o incydentach z indywidualnymi reakcjami na incydenty; zautomatyzowane mechanizmy wspierające lub wdrażające korelację informacji o reakcjach na incydenty z indywidualnymi reakcjami na incydenty].

IR-4(5)	**OBSŁUGA INCYDENTÓW | *AUTOMATYCZNE WYŁĄCZENIE SYSTEMU INFORMACYJNEGO***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-4(5)[1]	*definiuje naruszenia bezpieczeństwa, które w przypadku wykrycia inicjują konfigurowalną funkcję automatycznego wyłączania systemu informacyjnego; oraz*
	IR-4(5)[2]	*wprowadza konfigurowalną zdolność do automatycznego wyłączania systemu informacyjnego w przypadku wykrycia jakiegokolwiek naruszenia bezpieczeństwa zdefiniowanego przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; zautomatyzowane mechanizmy wspomagające obsługę incydentów; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów]. **Test**: [*wybierz spośród:* Zdolność organizacji do obsługi incydentów; zautomatyzowane mechanizmy wspierające i/lub wdrażające automatyczne wyłączanie systemu informacyjnego].	

IR-4(6)	**OBSŁUGA INCYDENTÓW | *ZAGROŻENIA WEWNĘTRZNE***
	CEL OCENY: *Ustalenie, czy organizacja wdraża zdolność do obsługi incydentów w zakresie zagrożeń wewnętrznych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; zautomatyzowane mechanizmy wspomagające obsługę incydentów; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; plan reagowania na incydenty; plan bezpieczeństwa; zapisy z audytu; inne odpowiednie dokumenty lub rejestry].

IR-4(6)	**OBSŁUGA INCYDENTÓW | *ZAGROŻENIA WEWNĘTRZNE***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zdolność organizacji do obsługi incydentów].

IR-4(7)	**OBSŁUGA INCYDENTÓW | *ZAGROŻENIA WEWNĘTRZNE – KOORDYNACJA WEWNĄTRZ ORGANIZACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-4(7)[1]	*określa komponenty lub elementy organizacji, z którymi ma być skoordynowana zdolność obsługi incydentów wewnętrznych w zakresie zagrożenia; oraz*
	IR-4(7)[2]	*koordynuje zdolność obsługi incydentów dla zagrożeń wewnętrznych w obrębie zdefiniowanych komponentów lub elementów organizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel/struktury organizacyjne, z którymi należy skoordynować Zdolności obsługi incydentów]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie koordynacji obsługi incydentów].	

IR-4(8)	**OBSŁUGA INCYDENTÓW | *KOORDYNACJA Z ORGANIZACJAMI ZEWNĘTRZNYMI***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-4(8)[1]	*definiuje organizacje zewnętrzne, z którymi należy koordynować informacje o incydentach organizacyjnych;*
	IR-4(8)[2]	*definiuje informacje o incydentach, które mają być skorelowane i współdzielone z określoną organizacją zewnętrzną; oraz*

IR-4(8)	**OBSŁUGA INCYDENTÓW | *KOORDYNACJA Z ORGANIZACJAMI ZEWNĘTRZNYMI***	
	IR-4(8)[3]	*współdziała ze zdefiniowaną organizacją zewnętrzną w celu skorelowania i dzielenia się informacjami zdefiniowanymi przez organizację, aby osiągnąć międzyorganizacyjną ocenę świadomości incydentów i bardziej efektywne reagowanie na incydenty.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; wykaz organizacji zewnętrznych; dokumentacja dotycząca koordynacji obsługi incydentów z organizacjami zewnętrznymi; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji zewnętrznych, z którymi informacje o reagowaniu na incydenty mają być koordynowane/udzielane/korelowane]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie koordynacji obsługi incydentów informacyjnych z organizacjami zewnętrznymi].	

IR-4(9)	**OBSŁUGA INCYDENTÓW | *ZDOLNOŚĆ UDZIELANIA DYNAMICZNEJ ODPOWIEDZI***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-4(9)[1]	*określa możliwości dynamicznego reagowania, które należy wykorzystać do skutecznego reagowania na incydenty związane z bezpieczeństwem; oraz*
	IR-4(9)[2]	*wykorzystuje zdefiniowane przez organizację możliwości dynamicznego reagowania, aby skutecznie reagować na incydenty związane z bezpieczeństwem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; zautomatyzowane mechanizmy wspomagające dynamiczne reagowanie na incydenty; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; plan reagowania na incydenty; plan bezpieczeństwa; zapisy z audytu; inne odpowiednie dokumenty lub rejestry].	

IR-4(9)	**OBSŁUGA INCYDENTÓW | *ZDOLNOŚĆ UDZIELANIA DYNAMICZNEJ ODPOWIEDZI***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dla Zdolności udzielania dynamicznej odpowiedzi; zautomatyzowane mechanizmy wspierające i/lub wdrażające zdolność udzielania dynamicznej odpowiedzi dla organizacji].

IR-4(10)	**OBSŁUGA INCYDENTÓW | *KOORDYNACJA ŁAŃCUCHA DOSTAW***
	CEL OCENY: *Ustalić, czy organizacja koordynuje działania obsługi incydentów związanych ze zdarzeniami w łańcuchu dostaw z innymi organizacjami zaangażowanymi w łańcuch dostaw.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące koordynacji łańcucha dostaw; umowy nabycia; umowa gwarancji świadczenia usług (SLA); plan reagowania na incydenty; plan bezpieczeństwa; plan reagowania na incydenty innych organizacji zaangażowanych w działania w ramach łańcucha dostaw; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za obsługę incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za łańcuch dostaw].

IR-5	**MONITOROWANIE INCYDENTÓW**	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-5[1]	*śledzi incydenty związane z bezpieczeństwem systemu informacyjnego; oraz*
	IR-5[2]	*dokumentuje incydenty związane z bezpieczeństwem systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące monitorowanie incydentów; zapisy i dokumentacja reakcji na incydenty; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry].	

IR-5	**MONITOROWANIE INCYDENTÓW**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za monitorowanie incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* monitorowanie Zdolności organizacji do reagowania na incydenty; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie i dokumentowanie incydentów związanych z bezpieczeństwem systemu].

IR-5(1)	**MONITOROWANIE INCYDENTÓW | *AUTOMATYCZNE MONITOROWANIE / ZBIERANIE DANYCH / ANALIZA***	
	CEL OCENY: *Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy wspomagające:*	
	IR-5(1)[1]	*monitorowanie incydentów związanych z bezpieczeństwem;*
	IR-5(1)[2]	*gromadzenie informacji o zdarzeniach; oraz*
	IR-5(1)[3]	*analizę informacji o incydentach.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące monitorowanie incydentów; zautomatyzowane mechanizmy wspomagające monitorowanie incydentów; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; plan reagowania na incydenty; plan bezpieczeństwa; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za monitorowanie incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające monitorowanie incydentów związanych z bezpieczeństwem oraz zbieranie i analizę informacji o incydentach].	

IR-6	**RAPORTOWANIE INCYDENTÓW**		
	CEL OCENY: *Określić, czy organizacja:*		
	IR-6(a)	**IR-6(a)[1]**	*określa okres czasu, w którym personel zgłasza podejrzenia wystąpienia incydentów bezpieczeństwa do jednostki organizacyjnej odpowiedzialnej za reagowanie na incydenty;*
		IR-6(a)[2]	*wymaga, aby personel zgłaszał, w określonym czasie, podejrzenia wystąpienia incydentów w zakresie bezpieczeństwa do jednostki organizacyjnej odpowiedzialnej za reagowanie na incydenty;*
	IR-6(b)	**IR-6(b)[1]**	*określa podmioty, którym mają być zgłaszane informacje o incydentach w zakresie bezpieczeństwa; oraz*
		IR-6(b)[2]	*zgłasza informacje o incydentach związanych z bezpieczeństwem do organów określonych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące raportowania incydentów; zapisy i dokumentacja dotycząca zgłaszania incydentów; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji mający obowiązek zgłaszania incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel, który zgłasza/ powinien zgłaszać incydenty; personel (organy), do którego należy zgłaszać informacje o incydentach]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące raportowania incydentów; zautomatyzowane mechanizmy wspierające i/lub wdrażające raportowanie incydentów].		

IR-6(1)	**RAPORTOWANIE INCYDENTÓW | *AUTOMATYCZNE RAPORTOWANIE***
	CEL OCENY: *Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy wspomagające zgłaszanie incydentów bezpieczeństwa.*

IR-6(1)	**RAPORTOWANIE INCYDENTÓW | *AUTOMATYCZNE RAPORTOWANIE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące raportowania incydentów; zautomatyzowane mechanizmy wspomagające raportowanie incydentów; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji mający obowiązek zgłaszania incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące raportowania incydentów; zautomatyzowane mechanizmy wspierające i/lub wdrażające raportowanie incydentów bezpieczeństwa].

IR-6(2)	**RAPORTOWANIE INCYDENTÓW | *PODATNOŚĆ NA INCYDENTY***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-6(2)[1]	*określa personel lub role, którym należy zgłaszać luki w systemie informacyjnym związane ze zgłaszanymi zdarzeniami naruszającymi bezpieczeństwo; oraz*
	IR-6(2)[2]	*Zgłasza, personelowi lub rolom zdefiniowanym przez organizację, luki w systemie informacyjnym związane z zaistniałymi incydentami bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące raportowania incydentów; plan reagowania na incydenty; plan bezpieczeństwa; raporty o incydentach związanych z bezpieczeństwem i związane z nimi podatności systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji mający obowiązek zgłaszania incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel, któremu należy zgłaszać podatności personel, któremu należy zgłaszać podatności związane incydentami naruszającymi bezpieczeństwo].	

IR-6(2)	**RAPORTOWANIE INCYDENTÓW | *PODATNOŚĆ NA INCYDENTY***
	Test: [*wybierz spośród:* Procesy organizacyjne dotyczące raportowania incydentów; zautomatyzowane mechanizmy wspierające i/lub wdrażające raportowanie podatności związanych ze zdarzeniami naruszającymi bezpieczeństwo].

IR-6(3)	**RAPORTOWANIE INCYDENTÓW | *KOORDYNACJA Z ŁAŃCUCHEM DOSTAW***
	CEL OCENY: *Ustalić, czy organizacja dostarcza informacje o incydentach związanych z bezpieczeństwem innym organizacjom uczestniczącym w łańcuchu dostaw na potrzeby systemów informacyjnych lub elementów systemu informacyjnego związanych z tym incydentem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące koordynacji łańcucha dostaw; umowy nabycia; umowa gwarancji świadczenia usług (SLA); plan reagowania na incydenty; plan bezpieczeństwa; plany innych organizacji zaangażowanych w łańcuch dostaw; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji mający obowiązek zgłaszania incydentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za łańcuch dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie raportowania incydentów; zautomatyzowane mechanizmy wspierające i/lub wdrażające raportowanie informacji o incydentach związanych z łańcuchem dostaw].

IR-7	**WSPARCIE REAGOWANIA NA INCYDENTY**	
	CEL OCENY: *Ustalić, czy organizacja zapewnia personel wsparcia w zakresie reagowania na incydenty, który:*	
	IR-7[1]	*jest integralną częścią zdolności organizacji do reagowania na incydenty; oraz*
	IR-7[2]	*oferuje porady i pomoc dla użytkowników systemu informacyjnego w zakresie obsługi i zgłaszania incydentów bezpieczeństwa.*

IR-7	WSPARCIE REAGOWANIA NA INCYDENTY
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące wsparcia w zakresie reagowania na incydenty; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za wsparcie i pomoc w reagowaniu na incydenty; personel organizacji mający dostęp do wsparcia i pomocy w zakresie reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne udzielania pomocy w zakresie reagowania na incydenty; zautomatyzowane mechanizmy wspierające lub wdrażające pomoc w zakresie reagowania na incydenty].

IR-7(1)	WSPARCIE REAGOWANIA NA INCYDENTY | *AUTOMATYCZNE WSPARCIE DOSTĘPNOŚCI INFORMACJI / OBSŁUGI*
	CEL OCENY: *Ustalenie, czy organizacja stosuje zautomatyzowane mechanizmy w celu zwiększenia dostępności informacji i wsparcia związanego z reagowaniem na incydenty.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące wsparcia w zakresie reagowania na incydenty; zautomatyzowane mechanizmy wspierające wsparcie i pomoc w reagowaniu na incydenty; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za wsparcie i pomoc w reagowaniu na incydenty; personel organizacji mający dostęp do wsparcia i pomocy w zakresie reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne wsparcia w zakresie reagowania na incydenty; zautomatyzowane mechanizmy wspierające lub wprowadzające w życie zwiększenie dostępności informacji i wsparcia w zakresie reagowania na incydenty].

IR-7(2)	**WSPARCIE REAGOWANIA NA INCYDENTY | *KOORDYNACJA Z DOSTAWCAMI ZEWNĘTRZNYMI***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-7(2)(a)	*ustanawia bezpośredni, oparty na współpracy związek między własną zdolnością reagowania na incydenty, a zewnętrznymi dostawcami środków ochrony systemu informacyjnego; oraz*
	IR-7(2)(b)	*wskazuje zewnętrznym dostawcom członków zespołu reagowania na incydenty.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące wsparcia w zakresie reagowania na incydenty; plan reagowania na incydenty; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zapewniający wsparcie i pomoc w zakresie reagowania na incydenty; zewnętrzni dostawcy usług ochrony systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

IR-8	**PLAN REAGOWANIA NA INCYDENTY**			
	CEL OCENY: *Określić, czy organizacja:*			
	IR-8(a)	*opracowuje plan reagowania na incydenty, który:*		
		IR-8(a)(1)	*dostarcza organizacji strategię dotyczącą wdrażania Zdolności reagowania na incydenty;*	
		IR-8(a)(2)	*opisuje strukturę i organizację zdolności do reagowania na incydenty;*	
		IR-8(a)(3)	*zapewnia ogólne podejście do tego, jak zdolność reagowania na incydenty wpisuje się w ogólne ramy działalności organizacji;*	
		IR-8(a)(4)	*spełnia unikalne wymagania organizacji dotyczące:*	
			IR-8(a)(4)[1]	*działań biznesowych;*

IR-8	**PLAN REAGOWANIA NA INCYDENTY**			
			IR-8(a)(4)[2]	*wielkości;*
			IR-8(a)(4)[3]	*struktury;*
			IR-8(a)(4)[4]	*funkcji;*
		IR-8(a)(5)	*definiuje zdarzenia podlegające zgłoszeniu;*	
		IR-8(a)(6)	*dostarcza metryki do pomiaru zdolności reagowania na incydenty w organizacji;*	
		IR-8(a)(7)	*definiuje zasoby i wsparcie zarządzania potrzebne do skutecznego utrzymania oraz rozwijania zdolności do reagowania na incydenty;*	
		IR-8(a)(8)	**IR-8(a)(8)[1]**	*definiuje personel lub role odpowiedzialne za przegląd i zatwierdzenie planu reagowania na incydenty;*
			IR-8(a)(8)[2]	*jest weryfikowany i zatwierdzany przez personel określony przez organizację lub role;*
	IR-8(b)	**IR-8(b)[1]**	**IR-8(b)[1][a]**	*definiuje personel reagujący na incydenty (określony przez nazwisko i/lub rolę), któremu mają być przekazywane kopie planu reagowania na incydenty;*
			IR-8(b)[1][b]	*definiuje elementy organizacyjne, którym mają być przekazywane kopie planu reagowania na incydenty;*
		IR-8(b)[2]	*dystrybuuje kopie planu reagowania na incydenty do zdefiniowanego przez organizację personelu reagującego na incydenty (identyfikowanego na podstawie nazwy i/lub roli) oraz elementów organizacyjnych;*	
	IR-8(c)	**IR-8(c)[1]**	*określa częstotliwość przeglądów planu reagowania na incydenty;*	
		IR-8(c)[2]	*dokonuje przeglądu planu reagowania na incydenty z częstotliwością określoną przez organizację;*	
	IR-8(d)	*aktualizuje plan reagowania na incydenty w celu uwzględnienia zmian systemowych/organizacyjnych lub problemów napotkanych w trakcie realizacji planu, tj.:*		

IR-8	**PLAN REAGOWANIA NA INCYDENTY**			
		IR-8(d)[1]	*wdrażania;*	
		IR-8(d)[2]	*wykonywania; lub*	
		IR-8(d)[3]	*testowania;*	
	IR-8(e)	**IR-8(e)[1]**	**IR-8(e)[1][a]**	*definiuje personel reagujący na incydent (określony przez nazwisko i/lub rolę), któremu należy przekazać informacje o zmianach w planie reagowania na incydent;*
			IR-8(e)[1][b]	*definiuje elementy organizacyjne, którym należy przekazywać informacje o zmianach w planie reagowania na incydenty;*
		IR-8(e)[2]	*przekazuje informacje o zmianach w planie reagowania na incydenty do zdefiniowanego przez organizację personelu reagującego na incydenty (identyfikowanego na podstawie nazwy i/lub roli) oraz elementów organizacyjnych; oraz*	
	IR-8(f)	*zabezpiecza plan reagowania na incydenty przed nieautoryzowanym ujawnieniem i modyfikacją.*		
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące planu reagowania na incydenty; plan reagowania na incydenty; rejestry przeglądów i zatwierdzania planów reagowania na incydenty; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za plan reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Plan organizacyjny reagowania na incydenty i związane z tym procesy organizacyjne].			

IR-9	**REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI**		
	CEL OCENY: *Określić, czy organizacja:*		
	IR-9(a)	*reaguje na wycieki informacji poprzez identyfikację konkretnych informacji mających ujemny wpływ na system informacyjny;*	
	IR-9(b)	**IR-9(b)[1]**	*określa personel, który ma być powiadomiony o wycieku informacji;*
		IR-9(b)[2]	*określa metodę komunikacji niezwiązaną z ujawnieniem informacji w celu ostrzeżenia o ujawnieniu informacji zdefiniowanego przez organizację personelu;*
		IR-9(b)[3]	*reaguje na wycieki informacji, powiadamiając określony przez organizację personel o ujawnieniu informacji przy użyciu metody komunikacji niezwiązanej z ujawnieniem informacji;*
	IR-9(c)	reaguje na wycieki informacji, izolując „zakażony" system informacyjny;	
	IR-9(d)	reaguje na wycieki informacji poprzez wyeliminowanie informacji z „zakażonego" systemu informacyjnego;	
	IR-9(e)	reaguje na wycieki informacji poprzez identyfikację innych systemów informacyjnych, które mogły zostać „skażone" w późniejszym czasie;	
	IR-9(f)	**IR-9(f)[1]**	*określa inne działania, które należy podjąć w odpowiedzi na wycieki informacji; oraz*
		IR-9(f)[2]	*reaguje na wycieki informacji poprzez wykonywanie innych działań zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury reakcji na ujawnienie informacji; plan reagowania na incydenty; rejestry alarmów o wyciekach informacji/zgłoszeń, wykaz *personelu*, który powinien otrzymywać alerty o wyciekach informacji; wykaz działań, które należy podjąć w związku z wyciekiem informacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za procedury reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie reagowania na wycieki informacji; zautomatyzowane mechanizmy wspierające i/lub realizujące działania w zakresie reagowania na wycieki informacji i związanej z tym komunikacji].		

IR-9(1)	**REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | *ODPOWIEDZIALNY PERSONEL***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-9(1)[1]	*określa personel odpowiedzialny za reagowanie na wycieki informacji; oraz*
	IR-9(1)[2]	*przydziela określony przez organizację personel odpowiedzialny za reagowanie na wycieki informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury reakcji na ujawnienie informacji; plan reagowania na incydenty; wykaz *personelu* odpowiedzialnego za reagowanie na wycieki informacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za procedury reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

IR-9(2)	**REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | *SZKOLENIE***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-9(2)[1]	*określa częstotliwość szkolenia w zakresie reagowania na wycieki/ujawnienia informacji; oraz*
	IR-9(2)[2]	*zapewnia szkolenie w zakresie reagowania na wycieki/ujawnienia informacji z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź: [wybierz spośród:**: Polityka reagowania na incydenty; procedury dotyczące szkoleń w zakresie reagowania na wycieki informacji; program szkoleń w zakresie reagowania na wycieki informacji; materiały szkoleniowe w zakresie reagowania na wycieki informacji; plan reagowania na incydenty; dokumentacja szkoleniowa w zakresie reagowania na wycieki informacji; inne odpowiednie dokumenty lub rejestry].	

IR-9(2)	**REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | *SZKOLENIE***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za szkolenie w zakresie reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

IR-9(3)	**REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | *DZIAŁANIA PO UJAWNIENIU***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-9(3)[1]	*definiuje procedury, które zapewniają personelowi organizacyjnemu dotkniętemu skutkami wycieku informacji możliwość dalszego wykonywania przydzielonych zadań w czasie, gdy „skażone" systemy są poddawane działaniom naprawczym; oraz*
	IR-9(3)[2]	*wdraża określone przez organizację procedury w celu zapewnienia, że personel organizacji dotknięty skutkami wycieku informacji może nadal wykonywać przydzielone zadania, podczas gdy „skażone" systemy są poddawane działaniom naprawczym.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; procedury reakcji na ujawnienie informacji; plan reagowania na incydenty; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za procedury reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące działań podejmowanych po wycieku informacji].	

IR-9(4)	**REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | *WYSTAWIENIE NA DZIAŁANIA OSÓB NIEAUTORYZOWANYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	IR-9(4)[1]	*określa środki bezpieczeństwa, które należy stosować wobec personelu uzyskującego dostęp do informacji, które nie są objęte przyznanymi uprawnieniami dostępu; oraz*

IR-9(4)	**REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | *WYSTAWIENIE NA DZIAŁANIA OSÓB NIEAUTORYZOWANYCH***	
	IR-9(4)[2]	*stosuje określone przez organizację zabezpieczenia w stosunku personelu uzyskującego dostęp do informacji, które nie są objęte przyznanymi uprawnieniami dostępu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące obsługi incydentów; procedury reakcji na ujawnienie informacji; plan reagowania na incydenty; środki bezpieczeństwa dotyczące wycieku informacji/narażenia na kontakt z nieupoważnionym personelem; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za procedury reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące postępowania z informacjami narażonymi na kontakt z nieupoważnionym personelem; zautomatyzowane mechanizmy wspierające i/lub wdrażające zabezpieczenia dla personelu narażonego na kontakt z informacjami, które nie mieszczą się w zakresie przyznanych uprawnień dostępu].	

IR-10	**ZINTEGROWANY ZESPÓŁ REAGOWANIA NA INCYDENTY**
	CEL OCENY: *Ustalenie, czy organizacja powołuje zintegrowany zespół reagowania na incydenty zawierający twórców narzędzi i personelu operacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka reagowania na incydenty; procedury dotyczące planowania reagowania na incydenty i integracji zespołu ds. analizy bezpieczeństwa; plan reagowania na incydenty; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za reagowanie na incydenty i analizę bezpieczeństwa informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji wchodzący w skład zintegrowanych zespołów analizy bezpieczeństwa].

KATEGORIA MA - UTRZYMANIE I WSPARCIE

MA-1	**POLITYKA I PROCEDURY UTRZYMANIA SYSTEMU**			
	CEL OCENY: *Określić, czy organizacja:*			
	MA-1(a)(1)	**MA-1(a)(1)[1]**	*opracowuje i dokumentuje politykę utrzymania systemu, która dotyczy:*	
			MA-1(a)(1)[1][a]	*celu;*
			MA-1(a)(1)[1][b]	*zakresu stosowania;*
			MA-1(a)(1)[1][c]	*ról;*
			MA-1(a)(1)[1][d]	*odpowiedzialności;*
			MA-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			MA-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			MA-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		MA-1(a)(1)[2]	*określa personel lub role, wśród których ma być rozpowszechniana polityka utrzymania systemu;*	
		MA-1(a)(1)[3]	*rozpowszechnia politykę utrzymania systemu wśród personelu określonego przez organizację lub ról;*	
	MA-1(a)(2)	**MA-1(a)(2)[1]**	*opracowuje i dokumentuje procedury umożliwiające wdrożenie polityki w zakresie utrzymania i związanych z nią kontroli utrzymania systemu;*	
		MA-1(a)(2)[2]	*określa personel lub rolę, wśród których procedury mają być rozpowszechniane;*	
		MA-1(a)(2)[3]	*rozpowszechnia procedury wśród personelu lub ról zdefiniowanych przez organizację;*	
	MA-1(b)(1)	**MA-1(b)(1)[1]**	*określa częstotliwość przeglądów i aktualizacji bieżącej polityki w zakresie utrzymania systemu;*	

MA-1	**POLITYKA I PROCEDURY UTRZYMANIA SYSTEMU**		
		MA-1(b)(1)[2]	*opiniuje i aktualizuje bieżącą politykę w zakresie utrzymania systemu z częstotliwością określoną przez organizację;*
	MA-1(b)(2)	**MA-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji aktualnych procedur utrzymania systemu; oraz*
		MA-1(b)(2)[2]	*opiniuje i aktualizuje aktualne procedury utrzymania systemu z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury w zakresie utrzymania i obsługi; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za utrzymanie; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

MA-2	**NADZÓR NAD UTRZYMANIEM**			
	CEL OCENY: *Określić, czy organizacja:*			
	MA-2(a)	**MA-2(a)[1]**	*Planuje przeglądy i konserwację części składowych systemu informacyjnego zgodnie z wymogami:*	
			MA-2(a)[1][a]	*specyfikacje producenta lub sprzedawcy; i/lub*
			MA-2(a)[1][b]	*wymagania organizacyjne;*
		MA-2(a)[2]	*przeprowadza konserwację i naprawy komponentów systemu informacyjnego zgodnie z wymogami:*	
			MA-2(a)[2][a]	*specyfikacji producenta lub sprzedawcy; i/lub*
			MA-2(a)[2][b]	*wymaganiami organizacyjnymi;*
		MA-2(a)[3]	*dokumentuje konserwację i naprawy komponentów systemu informacyjnego zgodnie z wymogami:*	

MA-2	**NADZÓR NAD UTRZYMANIEM**			
			MA-2(a)[3][a]	*specyfikacji producenta lub sprzedawcy; i/lub*
			MA-2(a)[3][b]	*wymaganiami organizacyjnymi;*
		MA-2(a)[4]	*dokonuje przeglądu zapisów dotyczących konserwacji i napraw elementów systemu informacyjnego zgodnie z wymogami:*	
			MA-2(a)[4][a]	*specyfikacji producenta lub sprzedawcy; i/lub*
			MA-2(a)[4][b]	*wymaganiami organizacyjnymi;*
	MA-2(b)	**MA-2(b)[1]**	*zatwierdza wszystkie czynności związane z konserwacją, niezależnie od tego, czy są one wykonywane na miejscu, czy zdalnie oraz czy sprzęt jest serwisowany na miejscu, czy też jest przenoszony do innego miejsca;*	
		MA-2(b)[2]	*monitoruje wszystkie czynności związane z utrzymaniem, niezależnie od tego, czy są one wykonywane na miejscu, czy zdalnie, oraz czy sprzęt jest serwisowany na miejscu, czy też jest przenoszony do innego miejsca;*	
	MA-2(c)	**MA-2(c)[1]**	*określa personel lub role wymagane do jednoznacznego zatwierdzenia demontażu systemu informacyjnego lub jego komponentów z obiektów organizacyjnych w celu przeprowadzenia konserwacji lub naprawy poza miejscem instalacji;*	
		MA-2(c)[2]	*wymaga, aby określony przez organizację personel lub role jednoznacznie zatwierdzał demontaż systemu informacyjnego lub jego części składowych z obiektów należących do organizacji w celu przeprowadzenia konserwacji lub napraw poza obiektem;*	
	MA-2(d)	*sanityzuje urządzenia w celu usunięcia wszystkich informacji z powiązanych nośników przed ich demontażem z obiektów organizacyjnych w celu konserwacji lub naprawy poza siedzibą firmy;*		
	MA-2(e)	*sprawdza wszystkie zabezpieczenia, mające potencjalny wpływ na bezpieczeństwo, w celu sprawdzenia, czy zabezpieczenia te nadal zachowują właściwe działania po wykonaniu czynności konserwacyjnych lub naprawczych;*		

MA-2	**NADZÓR NAD UTRZYMANIEM**		
	MA-2(f)	**MA-2(f)[1]**	*definiuje informacje związane z konserwacją, które mają być zawarte w dokumentacji technicznej organizacji; oraz*
		MA-2(f)[2]	*zawiera informacje dotyczące obsługi technicznej zdefiniowane przez organizację w jej dokumentacji technicznej.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące kontrolowanej konserwacji systemu informacyjnego; dokumentacja konserwacyjna; specyfikacje konserwacyjne producenta/sprzedawcy; dokumentacja sanityzacji sprzętu; dokumentacja sanityzacji nośników danych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za sanityzację nośników danych; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące planowania, wykonywania, dokumentowania, przeglądania, zatwierdzania i monitorowania konserwacji i napraw systemu informacyjnego; procesy organizacyjne dotyczące sanityzacji komponentów systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające nadzór nad utrzymaniem; zautomatyzowane mechanizmy wdrażające sanityzację komponentów systemu informacyjnego].		

MA-2(1)	**NADZÓR NAD UTRZYMANIEM | *ZAWARTOŚĆ REKORDU***
[Włączone do: MA-2]	

MA-2(2)	**NADZÓR NAD UTRZYMANIEM | *AUTOMATYCZNE DZIAŁANIA KONSERWACYJNE***		
	CEL OCENY: *Określić, czy organizacja:*		
	MA-2(2)(a)	*używa automatycznych mechanizmów do:*	
		MA-2(2)(a)[1]	*planowania konserwacji i napraw;*

MA-2(2)	**NADZÓR NAD UTRZYMANIEM | *AUTOMATYCZNE DZIAŁANIA KONSERWACYJNE***		
		MA-2(2)(a)[2]	*przeprowadzania konserwacji i napraw;*
		MA-2(2)(a)[3]	*dokumentowania konserwacji i napraw;*
	MA-2(2)(b)	*sporządza aktualną, dokładną i kompletną dokumentację wszystkich czynności związanych z konserwacją i naprawą:*	
		MA-2(2)(b)[1]	*wymaganą;*
		MA-2(2)(b)[2]	*zaplanowaną;*
		MA-2(2)(b)[3]	*w trakcie realizacji; oraz*
		MA-2(2)(b)[4]	*zakończoną.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące kontrolowanej konserwacji systemu informacyjnego; zautomatyzowane mechanizmy wspomagające czynności związane z konserwacją systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry konserwacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające nadzór nad utrzymaniem; zautomatyzowane mechanizmy wspierające i/lub wdrażające tworzenie dokumentacji działań związanych z utrzymaniem i naprawą].		

MA-3	**NARZĘDZIA UTRZYMANIOWE**	
	CEL OCENY: *Określić, czy organizacja:*	
	MA-3[1]	*zatwierdza narzędzia do konserwacji systemu informacyjnego;*
	MA-3[2]	*kontroluje narzędzia konserwacji systemu informacyjnego; oraz*
	MA-3[3]	*monitoruje narzędzia do konserwacji systemu informacyjnego.*

MA-3	NARZĘDZIA UTRZYMANIOWE
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące narzędzi utrzymania systemu informacyjnego; narzędzia utrzymania systemu informacyjnego i związana z nimi dokumentacja; rejestry konserwacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące zatwierdzania, kontroli i monitorowania narzędzi utrzymaniowych; zautomatyzowane mechanizmy wspierające i/lub wdrażające zatwierdzanie, kontrolę i/lub monitorowanie narzędzi utrzymaniowych].

MA-3(1)	NARZĘDZIA UTRZYMANIOWE | *NARZĘDZIA KONTROLNE*
	CEL OCENY: *Ustalić, czy organizacja kontroluje narzędzie utrzymaniowe wniesione do obiektu przez personel obsługi technicznej pod kątem niewłaściwych lub nieautoryzowanych modyfikacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące narzędzi utrzymania systemu informacyjnego; narzędzia utrzymania systemu informacyjnego i związana z nimi dokumentacja; zapisy z kontroli narzędzi do konserwacji; rejestry konserwacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące kontroli narzędzi utrzymaniowych; zautomatyzowane mechanizmy wspomagające i/lub wdrażające kontrolę narzędzi utrzymaniowych].

MA-3(2)	**NARZĘDZIA UTRZYMANIOWE | *MEDIA KONTROLNE***
	CEL OCENY: *Ustalić, czy organizacja sprawdza nośniki zawierające programy diagnostyczne i testowe pod kątem występowania złośliwego kodu, zanim nośniki zostaną zastosowane w systemie informacyjnym.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące narzędzi utrzymania systemu informacyjnego; narzędzia utrzymania systemu informacyjnego i związana z nimi dokumentacja; rejestry konserwacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Proces organizacyjny kontroli nośników pod kątem złośliwego kodu; zautomatyzowane mechanizmy wspomagające i/lub wdrażające kontrolę nośników używanych do konserwacji].

MA-3(3)	**NARZĘDZIA UTRZYMANIOWE | *ZAPOBIEGANIE NIEAUTORYZOWANEMU USUWANIU***		
	CEL OCENY: *Ustalić, czy organizacja zapobiega nieautoryzowanemu usunięciu sprzętu konserwacyjnego zawierającego informacje organizacyjne przez:*		
	MA-3(3)(a)	*sprawdzenie, czy urządzenia nie zawierają żadnych informacji organizacyjnych;*	
	MA-3(3)(b)	*sanityzację lub zniszczenie sprzętu;*	
	MA-3(3)(c)	*przechowywanie sprzętu na terenie obiektu; lub*	
	MA-3(3)(d)	**MA-3(3)(d)[1]**	*określenie personelu lub ról, które mogą udzielić zgody na usunięcie sprzętu z obiektu; oraz*
		MA-3(3)(d)[2]	*uzyskanie zgody na usunięcie sprzętu z obiektu przez personel określony przez organizację lub role wyraźnie upoważniające do jego usunięcia.*

MA-3(3)	**NARZĘDZIA UTRZYMANIOWE | *ZAPOBIEGANIE NIEAUTORYZOWANEMU USUWANIU***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące narzędzi utrzymania systemu informacyjnego; narzędzia utrzymania systemu informacyjnego i związana z nimi dokumentacja; rejestry konserwacji; dokumentacja dotycząca sanityzacji sprzętu; dokumentacja dotycząca sanityzacji nośników; wyjątki dotyczące usuwania sprzętu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za sanityzację nośników danych]. **Test**: [*wybierz spośród:* Proces organizacyjny zapobiegający nieuprawnionemu usuwaniu informacji; zautomatyzowane mechanizmy wspomagające sanityzację lub niszczenie urządzeń; zautomatyzowane mechanizmy wspomagające weryfikację sanityzacji nośników danych].

MA-3(4)	**NARZĘDZIA UTRZYMANIOWE | *OGRANICZANIE UŻYWANIA NARZĘDZI***
	CEL OCENY: *Ustalić, czy organizacja ogranicza korzystanie z narzędzi utrzymaniowych wyłącznie przez upoważniony personel.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące narzędzi utrzymania systemu informacyjnego; narzędzia utrzymania systemu informacyjnego i związana z nimi dokumentacja; lista personelu upoważnionego do korzystania z narzędzi utrzymaniowych; ewidencja użytkowania narzędzi konserwacyjnych; rejestry konserwacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Proces organizacyjny ograniczania użycia narzędzi utrzymaniowych; zautomatyzowane mechanizmy wspierające i/lub implementujące ograniczone użycie narzędzi utrzymaniowych].

MA-4	**UTRZYMANIE ZDALNE**		
	CEL OCENY: *Określić, czy organizacja:*		
	MA-4(a)	**MA-4(a)[1]**	*zatwierdza utrzymanie zdalnych działań diagnostycznych;*
		MA-4(a)[2]	*monitoruje zdalne działania utrzymaniowe i diagnostyczne;*
	MA-4(b)	*pozwala na korzystanie tylko z narzędzi zdalnych i diagnostycznych:*	
		MA-4(b)[1]	*zgodnych z polityką organizacyjną;*
		MA-4(b)[2]	*udokumentowanych w planie bezpieczeństwa systemu informacyjnego;*
	MA-4(c)	*korzysta z silnego uwierzytelniania przy ustanawianiu zdalnych sesji do obsługi technicznej i diagnostycznej;*	
	MA-4(d)	*prowadzi ewidencję działalności związanej z działalnością zdalną i diagnostyczną;*	
	MA-4(e)	**MA-4(e)[1]**	*zamyka sesje i połączenia sieciowe po zakończeniu czynności zdalnego utrzymania; oraz*
		MA-4(e)[2]	*zamyka połączenia sieciowe po zakończeniu konserwacji zdalnej lub diagnostyki.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące zdalnej konserwacji systemów informacyjnych; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry konserwacji; zapisy diagnostyczne; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Organizacyjne procesy zarządzania utrzymaniem zdalnym; zautomatyzowane mechanizmy wdrażania, wspierania i/lub zarządzania utrzymaniem zdalnym; zautomatyzowane mechanizmy silnego uwierzytelniania zdalnych sesji diagnostycznych; zautomatyzowane mechanizmy kończenia zdalnych sesji utrzymaniowych i połączeń sieciowych].		

MA-4(1)	**UTRZYMANIE ZDALNE | *AUDYT I PRZEGLĄD***		
	CEL OCENY: *Określić, czy organizacja:*		
	MA-4(1)(a)	**MA-4(1)(a)[1]**	*definiuje zdarzenia audytowe do kontroli zdalnych sesji utrzymania i sesji diagnostycznych;*
		MA-4(1)(a)[2]	*definiuje zdarzenia audytowe dla zdalnych sesji utrzymania i diagnostyki; oraz*
	MA-4(1)(b)	*przegląda zapisy z sesji konserwacyjnych i diagnostycznych.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące zdalnej konserwacji systemów informacyjnych; lista audytowanych zdarzeń; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry konserwacji; zapisy diagnostyczne; zapisy z audytu; przeglądy zapisów z sesji konserwacyjnych i diagnostycznych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za audyt i przegląd; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z audytem i przeglądem utrzymania zdalnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające audyt i przegląd utrzymania zdalnego].		

MA-4(2)	**UTRZYMANIE ZDALNE | *DOKUMENTY ZDALNEGO UTRZYMANIA***	
	CEL OCENY: *Ustalić, czy organizacja dokumentuje w planie bezpieczeństwa systemu informacyjnego:*	
	MA-4(2)[1]	*polityki w zakresie tworzenia i wykorzystywania utrzymania połączeń zdalnych i diagnostycznych; oraz*
	MA-4(2)[2]	*procedury ustanawiania i wykorzystywania utrzymania połączeń zdalnych i diagnostycznych.*

MA-4(2)	**UTRZYMANIE ZDALNE | *DOKUMENTY ZDALNEGO UTRZYMANIA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące zdalnej konserwacji systemów informacyjnych; plan bezpieczeństwa; rejestry konserwacji; zapisy diagnostyczne; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

MA-4(3)	**UTRZYMANIE ZDALNE | *PORÓWNYWALNE POZIOMY BEZPIECZEŃSTWA / SANITYZACJA***		
	CEL OCENY: *Określić, czy organizacja:*		
	MA-4(3)(a)	*wymaga, aby utrzymanie zdalne i usługi diagnostyczne były wykonywane z systemu informacyjnego, który posiada zdolność bezpieczeństwa porównywalną do Zdolności wdrożonej w obsługiwanym systemie; lub*	
	MA-4(3)(b)	**MA-4(3)(b)[1]**	*usuwa z systemu informacyjnego element, który ma być serwisowany;*
		MA-4(3)(b)[2]	*sanityzuje komponent (w odniesieniu do informacji organizacyjnych) przed wykonaniem usług zdalnych lub diagnostycznych i/lub przed usunięciem z obiektów organizacyjnych; oraz*
		MA-4(3)(b)[3]	*sprawdza i sanityzuje komponent (w odniesieniu do potencjalnie złośliwego oprogramowania) po wykonaniu usługi serwisowej komponentu i przed ponownym podłączeniem go do systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące zdalnej konserwacji systemów informacyjnych; umowy z dostawcami usług i/lub umowy gwarancji świadczenia usług (SLA); rejestry konserwacji; protokoły z kontroli; zapisy z audytu; rejestry sanityzacji sprzętu; rejestry sanityzacji nośników danych; inne odpowiednie dokumenty lub rejestry].		

MA-4(3)	**UTRZYMANIE ZDALNE | *PORÓWNYWALNE POZIOMY BEZPIECZEŃSTWA / SANITYZACJA***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; dostawca usług konserwacji systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za sanityzację nośników danych; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne zapewniające porównywalne bezpieczeństwo i sanityzację w przypadku zdalnej konserwacji; procesy organizacyjne związane z usuwaniem, sanitycją i inspekcją komponentów obsługiwanych w ramach zdalnej konserwacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające sanitycję i inspekcję komponentów].

MA-4(4)	**UTRZYMANIE ZDALNE | *UWIERZYTELNIANIE / SEPARACJA SESJI UTRZYMANIOWYCH***		
	CEL OCENY: *Ustalić, czy organizacja chroni utrzymanie zdalnych sesji przez:*		
	MA-4(4)(a)	**MA-4(4)(a)[1]**	*określenie odpornych na odtwarzanie uwierzytelnień, które mają być stosowane w celu ochrony utrzymania zdalnych sesji;*
		MA-4(4)(a)[2]	*stosowanie definiowanych przez organizację mechanizmów uwierzytelniających, które są odporne na wielokrotne powtórzenie;*
	MA-4(4)(b)	*oddzielenie sesji konserwacyjnych od innych sesji sieciowych z systemem informacyjnym, poprzez:*	
		MA-4(4)(b)(1)	*fizycznie oddzielenie ścieżek komunikacyjnych; lub*
		MA-4(4)(b)(2)	*logicznie odseparowanie ścieżek komunikacyjnych, oparte na szyfrowaniu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące zdalnej konserwacji systemów informacyjnych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry konserwacji; zapisy z audytu; inne odpowiednie dokumenty lub rejestry].		

MA-4(4)	**UTRZYMANIE ZDALNE | *UWIERZYTELNIANIE / SEPARACJA SESJI UTRZYMANIOWYCH***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; inżynierowie sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; procesy organizacyjne związane z ochroną utrzymania sesji zdalnych; zautomatyzowane mechanizmy implementujące autoryzację odporną na powtarzanie; zautomatyzowane mechanizmy implementujące rozdzielone logicznie/szyfrowane ścieżki komunikacyjne; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne ochrony zdalnych sesji serwisowych; zautomatyzowane mechanizmy implementujące autoryzację odporną na powtórne przetwarzanie danych; zautomatyzowane mechanizmy wdrażania oddzielonych logicznie/szyfrowanych ścieżek komunikacyjnych].

MA-4(5)	**UTRZYMANIE ZDALNE | *ZGODY I POWIADOMIENIA***		
	CEL OCENY: *Określić, czy organizacja:*		
	MA-4(5)(a)	**MA-4(5)(a)[1]**	*określa personel lub role wymagane do zatwierdzenia każdej zdalnej sesji utrzymania;*
		MA-4(5)(a)[2]	*wymaga zatwierdzenia każdej zdalne sesji utrzymania przez personel lub role określone przez organizację;*
	MA-4(5)(b)	**MA-4(5)(b)[1]**	*określa personel lub role, które należy powiadomić o dacie i godzinie zaplanowanego zdalnego serwisu; oraz*
		MA-4(5)(b)[2]	*powiadamia określone role lub personel o dacie i godzinie planowanego zdalnego serwisu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące zdalnej konserwacji systemów informacyjnych; plan bezpieczeństwa; powiadomienia wspierające utrzymanie sesji zdalnych; rejestry konserwacji; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za powiadamianie; personel organizacji odpowiedzialny za zatwierdzanie; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

MA-4(5)	**UTRZYMANIE ZDALNE | *ZGODY I POWIADOMIENIA***
	Test: [*wybierz spośród:* Procesy organizacyjne zatwierdzania i powiadamiania personelu w zakresie utrzymania zdalnego; zautomatyzowane mechanizmy wspomagające powiadamianie i zatwierdzanie utrzymania zdalnego].

MA-4(6)	**UTRZYMANIE ZDALNE | *OCHRONA KRYPTOGRAFICZNA***
	CEL OCENY: *Ustalić, czy system informacyjny wdraża mechanizmy kryptograficzne w celu ochrony integralności i poufności zdalnego utrzymania i diagnostyki komunikacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące zdalnej konserwacji systemów informacyjnych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; mechanizmy kryptograficzne chroniące procesy utrzymania zdalnego; rejestry konserwacji; zapisy diagnostyczne; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; inżynierowie sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficzne chroniące komunikację utrzymania zdalnego i diagnostyki].

MA-4(7)	**UTRZYMANIE ZDALNE | *ZDALNA WERYFIKACJA ZAKOŃCZENIA SESJI***
	CEL OCENY: *Ustalić, czy system informacyjny przeprowadza zdalną weryfikację rozłączenia po zakończeniu zdalnych sesji konserwacyjnych i diagnostycznych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące zdalnej konserwacji systemów informacyjnych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; mechanizmy kryptograficzne chroniące procesy utrzymania zdalnego; rejestry konserwacji; zapisy diagnostyczne; zapisy z audytu; inne odpowiednie dokumenty lub rejestry].

MA-4(7)	**UTRZYMANIE ZDALNE | *ZDALNA WERYFIKACJA ZAKOŃCZENIA SESJI***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; inżynierowie sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące zdalną weryfikację rozłączania zakończonych zdalnych sesji konserwacyjnych i diagnostycznych].

MA-5	**PERSONEL UTRZYMANIOWY**	
	CEL OCENY: *Określić, czy organizacja:*	
MA-5(a)	**MA-5(a)[1]**	*ustanawia proces autoryzacji personelu utrzymaniowego;*
	MA-5(a)[2]	*prowadzi listę autoryzowanych podmiotów lub personelu obsługi technicznej;*
MA-5(b)	*zapewnia, że personel bez eskorty, wykonujący prace konserwacyjne w systemie informacyjnym, posiada wymagane uprawnienia dostępu; oraz*	
MA-5(c)	*wyznacza personel organizacji z wymaganymi uprawnieniami dostępu i kompetencjami technicznymi do nadzorowania czynności związanych z obsługą techniczną personelu, który nie posiada wymaganych uprawnień dostępu.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące personelu utrzymaniowego; umowy o świadczenie usług; umowa gwarancji świadczenia usług (SLA); lista upoważnionego personelu; rejestry konserwacji; rejestry kontroli dostępu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie autoryzacji i zarządzania personelem utrzymaniowym; zautomatyzowane mechanizmy wspierające i/lub wdrażające autoryzację personelu utrzymaniowego].	

MA-5(1)	**PERSONEL UTRZYMANIOWY | *OSOBY NIEPOSIADAJĄCE STOSOWNYCH PRAW DOSTĘPU***			
	CEL OCENY: *Określić, czy organizacja:*			
	MA-5(1)(a)	*wdraża procedury dotyczące korzystania z personelu obsługi technicznej, który nie posiada odpowiednich poświadczeń bezpieczeństwa lub nie jest obywatelem Polsk i określa następujące wymagania:*		
		MA-5(1)(a)(1)	*personel utrzymaniowy, który nie posiada niezbędnych uprawnień dostępu, zezwoleń lub formalnych zatwierdzeń dostępu, jest eskortowany i nadzorowany podczas wykonywania czynności konserwacyjnych i diagnostycznych w systemie informacyjnym przez uprawniony personel organizacji, który:*	
			MA-5(1)(a)(1)[1]	*posiada poświadczenia bezpieczeństwa;*
			MA-5(1)(a)(1)[2]	*ma odpowiednie uprawnienia dostępu;*
			MA-5(1)(a)(1)[3]	*posiada odpowiednie kwalifikacje techniczne;*
		MA-5(1)(a)(2)	*przed rozpoczęciem czynności konserwacyjnych lub diagnostycznych przez personel, który nie potrzebuje zezwoleń na dostęp, poświadczeń lub formalnych zatwierdzeń dostępu:*	
			MA-5(1)(a)(2)[1]	*wszystkie nietrwałe elementy przechowujące informacje w systemie informacyjnym są oczyszczane; oraz*
			MA-5(1)(a)(2)[2]	*wszystkie nietrwałe nośniki danych są usuwane; lub*
			MA-5(1)(a)(2)[3]	*wszystkie nietrwałe nośniki danych są fizycznie odłączone od systemu i zabezpieczone; oraz*

MA-5(1)	**PERSONEL UTRZYMANIOWY | *OSOBY NIEPOSIADAJĄCE STOSOWNYCH PRAW DOSTĘPU***	
	MA-5(1)(b)	*opracowuje i wdraża alternatywne środki bezpieczeństwa na wypadek, gdyby elementu systemu informacyjnego nie można było oczyścić, usunąć lub odłączyć od systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące personelu utrzymaniowego; polityka ochrony nośników danych systemu informacyjnego; polityka ochrony fizycznej i ochrony środowiska; plan bezpieczeństwa; lista personelu utrzymaniowego wymagającego eskorty/nadzoru; rejestry konserwacji; zapisy kontroli dostępu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo personelu; personel organizacji odpowiedzialny za fizyczną kontrolę dostępu; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za sanityzację nośników danych; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące zarządzania personelem utrzymaniowym nieposiadającym odpowiedniego prawa dostępu; zautomatyzowane mechanizmy wspierające i/lub wdrażające alternatywne środki bezpieczeństwa; zautomatyzowane mechanizmy wspierające i/lub wdrażające sanityzację elementów przechowywania informacji].	

MA-5(2)	**PERSONEL UTRZYMANIOWY | *POŚWIADCZENIA BEZPIECZEŃSTWA / SYSTEMY NIEJAWNE***	
	CEL OCENY: *Ustalenie, czy organizacja zapewnia, że personel wykonujący czynności konserwacyjne i diagnostyczne w systemie informacyjnym przetwarzającym, przechowującym lub przekazującym informacje niejawne posiada:*	
	MA-5(2)[1]	*poświadczenia bezpieczeństwa na poziomie co najmniej najwyższej klauzuli niejawności w systemie;*
	MA-5(2)[2]	*poświadczenia bezpieczeństwa w odniesieniu do wszystkich źródeł informacji znajdujących się w systemie;*
	MA-5(2)[3]	*formalne upoważnienia do dostępu do informacji o co najmniej najwyższym poziomie klauzuli niejawności w systemie; oraz*

MA-5(2)	**PERSONEL UTRZYMANIOWY | *POŚWIADCZENIA BEZPIECZEŃSTWA / SYSTEMY NIEJAWNE***	
	MA-5(2)[4]	*formalne zezwolenia na dostęp do wszystkich kategorii informacji w systemie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące personelu utrzymaniowego; akta osobowe; rejestry konserwacji; zapisy kontroli dostępu; dane uwierzytelniające dostęp; uprawnienia dostępu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo personelu; personel organizacji odpowiedzialny za fizyczną kontrolę dostępu; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zapisy kontroli dostępu; dane uwierzytelniające dostęp; uprawnienia dostępu; procesy organizacyjne w zakresie zarządzania poświadczeniami bezpieczeństwa personelu utrzymaniowego].	

MA-5(3)	**PERSONEL UTRZYMANIOWY | *OBYWATELSTWO / SYSTEMY NIEJAWNE***
	CEL OCENY: Ustalenie, czy zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka utrzymania systemu informacyjnego; procedury dotyczące personelu utrzymaniowego; dokumentacja dotycząca personelu; dokumentacja dotycząca utrzymania; dokumentacja dotycząca kontroli dostępu; poświadczenia dostępu; upoważnienia dostępu; inne stosowne dokumenty lub zapisy]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za utrzymanie systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

MA-5(4)	**PERSONEL UTRZYMANIOWY | *CUDZOZIEMCY***
	CEL OCENY: Ustalenie, czy zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

MA-5(4)	**PERSONEL UTRZYMANIOWY | *CUDZOZIEMCY***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka utrzymania systemu informacyjnego; procedury dotyczące personelu zajmującego się utrzymaniem; polityka ochrony nośników systemu informacyjnego; polityka i procedury kontroli dostępu; polityka i procedury ochrony fizycznej i ochrony środowiska; protokół ustaleń; dokumentacja utrzymania; dokumentacja kontroli dostępu; poświadczenia dostępu; upoważnienia dostępu; inne stosowne dokumenty lub zapisy]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za utrzymanie systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji zarządzający porozumieniami o współpracy; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące przydzielania cudzoziemców do personelu obsługi technicznej].

MA-5(5)	**PERSONEL UTRZYMANIOWY | *OBSŁUGA NIEZWIĄZANA Z UTRZYMANIEM SYSTEMU***
	CEL OCENY: *Ustalenie, czy organizacja zapewnia, że nienadzorowany personel wykonujący czynności niezwiązane bezpośrednio z systemem informacyjnym, ale w bezpośredniej odległości od systemu, będzie wymagał autoryzacji dostępu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące personelu utrzymaniowego; polityka ochrony nośników danych systemu informacyjnego; zasady i procedury kontroli dostępu; polityka i procedury ochrony fizycznej i środowiskowej; rejestry konserwacji; rejestry kontroli dostępu; upoważnienia dostępu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo personelu; personel organizacji odpowiedzialny za fizyczną kontrolę dostępu; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

MA-6	**TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI**		
	CEL OCENY: *Określić, czy organizacja:*		
	MA-6[1]	*definiuje elementy systemu informacyjnego, dla których należy uzyskać wsparcie serwisowe i/lub części zamienne;*	
	MA-6[2]	*definiuje okres czasu, w którym należy uzyskać wsparcie serwisowe i/lub części zamienne po wystąpieniu awarii;*	
	MA-6[3]	**MA-6[3][a]**	*uzyskuje wsparcie serwisowe dla zdefiniowanych przez organizację komponentów systemu informacyjnego w określonym przez nią okresie czasu trwania awarii; i/lub*
		MA-6[3][b]	*pozyskuje części zamienne do zdefiniowanych przez organizację komponentów systemu informacyjnego w określonym przez nią okresie czasu trwania awarii.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące konserwacji systemu informacyjnego; umowy o świadczenie usług; umowa gwarancji świadczenia usług (SLA); zapasy i dostępność części zamiennych; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za zakupy; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne mające na celu zapewnienie terminowej konserwacji].		

MA-6(1)	**TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI | *KONSERWACJA ZAPOBIEGAWCZA***	
	CEL OCENY: *Określić, czy organizacja:*	
	MA-6(1)[1]	*definiuje elementy systemu informacyjnego, na których ma być wykonywana konserwacja zapobiegawcza;*
	MA-6(1)[2]	*definiuje przedziały czasowe, w których ma być wykonywana konserwacja zapobiegawcza na zdefiniowanych przez organizację komponentach systemu informacyjnego; oraz*

MA-6(1)	**TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI | *KONSERWACJA ZAPOBIEGAWCZA***	
	MA-6(1)[3]	*wykonuje konserwację zapobiegawczą na zdefiniowanych organizacyjnie komponentach systemu informacyjnego w zdefiniowanych organizacyjnie odstępach czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące konserwacji systemu informacyjnego; umowy o świadczenie usług; umowa gwarancji świadczenia usług (SLA); plan bezpieczeństwa; rejestry konserwacji; lista komponentów systemu informacyjnego wymagającego konserwacji zapobiegawczej; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z konserwacją zapobiegawczą; zautomatyzowane mechanizmy wspierające i/lub wdrażające konserwację zapobiegawczą].	

MA-6(2)	**TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI | *KONSERWACJA PLANOWA***	
	CEL OCENY: *Określić, czy organizacja:*	
	MA-6(2)[1]	*definiuje elementy systemu informacyjnego, na których ma być prowadzona konserwacja planowa;*
	MA-6(2)[2]	*definiuje przedziały czasowe, w których konserwacja planowa ma być wykonywana na zdefiniowanych organizacyjnie komponentach systemu informacyjnego; oraz*
	MA-6(2)[3]	*wykonuje konserwację planową na zdefiniowanych organizacyjnie komponentach systemu informacyjnego w zdefiniowanych organizacyjnie odstępach czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące konserwacji systemu informacyjnego; umowy o świadczenie usług; umowa gwarancji świadczenia usług (SLA); plan bezpieczeństwa; rejestry konserwacji; lista elementów składowych systemu informacyjnego wymagających konserwacji planowej; inne odpowiednie dokumenty lub rejestry].	

MA-6(2)	**TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI | *KONSERWACJA PLANOWA***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z konserwacją planową; zautomatyzowane mechanizmy wspierające i/lub wdrażające konserwację planową].

MA-6(3)	**TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI | *AUTOMATYCZNE WSPARCIE W ZAKRESIE KONSERWACJI PROGNOZOWANEJ***
	CEL OCENY: *Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy transferu danych konserwacji prognozowanej do informacyjnego systemu zarządzania konserwacją.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka konserwacji systemu informacyjnego; procedury dotyczące konserwacji systemu informacyjnego; umowy o świadczenie usług; umowa gwarancji świadczenia usług (SLA); plan bezpieczeństwa; rejestry konserwacji; lista elementów składowych systemu informacyjnego wymagających konserwacji planowej; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za konserwację systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące transfer danych planowej konserwacji do informacyjnego systemu zarządzania utrzymaniem; obsługa informacyjnego systemu zarządzania utrzymaniem].

KATEGORIA MP - OCHRONA NOŚNIKÓW DANYCH

MP-1	**POLITYKA I PROCEDURY OCHRONY NOŚNIKÓW DANYCH**			
	CEL OCENY: *Określić, czy organizacja:*			
	MP-1(a)(1)	**MP-1(a)(1)[1]**	*opracowuje i dokumentuje politykę ochrony nośników danych, która dotyczy:*	
			MP-1(a)(1)[1][a]	*celu;*
			MP-1(a)(1)[1][b]	*zakresu stosowania;*
			MP-1(a)(1)[1][c]	*ról;*
			MP-1(a)(1)[1][d]	*odpowiedzialności;*
			MP-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			MP-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			MP-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		MP-1(a)(1)[2]	*określa personel lub role, wśród których powinna być rozpowszechniana polityka ochrony nośników danych;*	
		MP-1(a)(1)[3]	*rozpowszechnia politykę ochrony nośników danych wśród personelu lub ról zdefiniowanych przez organizację;*	
	MP-1(a)(2)	**MP-1(a)(2)[1]**	*opracowuje i dokumentuje procedury usprawniające wdrażanie polityki ochrony nośników danych i związane z nią mechanizmy ochrony nośników;*	
		MP-1(a)(2)[2]	*określa personel lub role, wśród których procedury mają być rozpowszechniane;*	
		MP-1(a)(2)[3]	*rozpowszechnia procedury wśród zdefiniowanego przez organizację personelu lub ról;*	
	MP-1(b)(1)	**MP-1(b)(1)[1]**	*określa częstotliwość przeglądu i aktualizacji bieżącej polityki ochrony nośników danych;*	

MP-1	**POLITYKA I PROCEDURY OCHRONY NOŚNIKÓW DANYCH**		
		MP-1(b)(1)[2]	*opiniuje i aktualizuje aktualną politykę ochrony nośników danych z określoną przez organizację częstotliwością;*
	MP-1(b)(2)	**MP-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji aktualnych procedur ochrony nośników danych; oraz*
		MP-1(b)(2)[2]	*opiniuje i aktualizuje aktualne procedury ochrony nośników danych z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury ochrony nośników danych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę nośników danych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

MP-2	**DOSTĘP DO NOŚNIKÓW**	
	CEL OCENY: *Określić, czy organizacja:*	
	MP-2[1]	*definiuje rodzaje nośników danych cyfrowych i/lub nie cyfrowych, do których dostęp jest ograniczony;*
	MP-2[2]	*definiuje personel lub role uprawnione do dostępu do zdefiniowanych przez organizację rodzajów nośników danych cyfrowych i/lub nie cyfrowych; oraz*
	MP-2[3]	*ogranicza dostęp do zdefiniowanych przez organizację rodzajów nośników danych cyfrowych i/lub nie cyfrowych do określonego personelu lub ról.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące ograniczeń dostępu do nośników danych; zasady i procedury kontroli dostępu; polityka i procedury ochrony fizycznej i środowiskowej; obiekty do przechowywania nośników danych; rejestry kontroli dostępu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę nośników danych systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci].	

MP-2	**DOSTĘP DO NOŚNIKÓW**
	Test: [*wybierz spośród:* Procesy organizacyjne ograniczające dostęp użytkowników do nośników danych; zautomatyzowane mechanizmy wspierające i/lub wdrażające ograniczenia dostępu do nośników danych.].

MP-2(1)	**DOSTĘP DO NOŚNIKÓW | *OGRANICZONY DOSTĘP AUTOMATYCZNY***
[Włączone do: MP-4(2)].	

MP-2(2)	**DOSTĘP DO NOŚNIKÓW | *OCHRONA KRYPTOGRAFICZNA***
[Włączone do: SC-28(1)].	

MP-3	**OZNAKOWANIE NOŚNIKÓW**		
	CEL OCENY: *Określić, czy organizacja:*		
	MP-3(a)	*oznacza nośniki systemu informacyjnego wskazujące:*	
		MP-3(a)[1]	*ograniczenia w rozpowszechnianiu informacji;*
		MP-3(a)[2]	*postępowanie z klauzulami informacyjnymi;*
		MP-3(a)[3]	*odpowiednie oznaczenia bezpieczeństwa (jeśli istnieją) informacji;*
	MP-3(b)	**MP-3(b)[1]**	*określa rodzaje nośników systemu informacyjnego, które mają być wyłączone z oznakowania, tak długo, jak nośniki pozostają w wyznaczonych, kontrolowanych obszarach;*
		MP-3(b)[2]	*określa kontrolowane obszary, w których powinny być przechowywane nośniki informacji o zdefiniowanych przez organizację typach, zwolnionych z obowiązku oznakowania; oraz*
		MP-3(b)[3]	*wyłącza określone przez organizację rodzaje nośników systemu informacyjnego z obowiązku znakowania tak długo, jak długo nośniki pozostają w określonych przez organizację kontrolowanych obszarach.*

MP-3	**OZNAKOWANIE NOŚNIKÓW**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące znakowania nośników; polityka i procedury ochrony fizycznej i środowiskowej; plan bezpieczeństwa; wykaz nośników systemu informacyjnego oznaczonych atrybutami bezpieczeństwa; wyznaczone obszary kontrolowane; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę i oznakowanie nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne znakowania nośników informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające znakowanie nośników informacji].

MP-4	**PRZECHOWYWANIE NOŚNIKÓW**		
	CEL OCENY: *Określić, czy organizacja:*		
	MP-4(a)	**MP-4(a)[1]**	*określa rodzaje nośników cyfrowych i/lub nie cyfrowych, które mają być fizycznie kontrolowane i bezpiecznie przechowywane w wyznaczonych strefach kontrolowanych;*
		MP-4(a)[2]	*definiuje kontrolowane obszary przeznaczone do fizycznej kontroli i bezpiecznego przechowywania zdefiniowanych przez organizację rodzajów nośników cyfrowych i/lub nie cyfrowych;*
		MP-4(a)[3]	*fizycznie kontroluje określone przez organizację rodzaje nośników cyfrowych lub nie cyfrowych w obrębie określonych przez organizację kontrolowanych obszarów;*
		MP-4(a)[4]	*bezpiecznie przechowuje zdefiniowane przez organizację rodzaje mediów cyfrowych i/lub nie cyfrowych w obrębie zdefiniowanych przez organizację obszarów kontrolowanych; oraz*
	MP-4(b)	*chroni nośniki systemu informacyjnego do momentu ich zniszczenia lub sanityzacji przy użyciu zatwierdzonego sprzętu, techniki procedur.*	

MP-4	**PRZECHOWYWANIE NOŚNIKÓW**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące przechowywania nośników danych; polityka i procedury ochrony fizycznej i środowiskowej; zasady i procedury kontroli dostępu; plan bezpieczeństwa; nośniki systemu informacyjnego; wyznaczone strefy kontrolowane; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę i przechowywanie nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące przechowywania nośników informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające bezpieczne przechowywanie/ochronę nośników informacji].

MP-4(1)	**PRZECHOWYWANIE NOŚNIKÓW | *OCHRONA KRYPTOGRAFICZNA***
[Włączone do: SC-28(1)].	

MP-4(2)	**PRZECHOWYWANIE NOŚNIKÓW | *OGRANICZONY DOSTĘP AUTOMATYCZNY***	
	CEL OCENY: *Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy do:*	
	MP-4(2)[1]	*ograniczania dostępu do miejsc przechowywania nośników;*
	MP-4(2)[2]	*audytu prób dostępu; oraz*
	MP-4(2)[3]	*audytu przyznawania dostępu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące przechowywania nośników danych; zasady i procedury kontroli dostępu; polityka i procedury ochrony fizycznej i środowiskowej; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; obiekty do przechowywania nośników danych; urządzenia kontroli dostępu; rejestry kontroli dostępu; zapisy z audytu; inne odpowiednie dokumenty lub rejestry].	

MP-4(2)	**PRZECHOWYWANIE NOŚNIKÓW | *OGRANICZONY DOSTĘP AUTOMATYCZNY***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę i przechowywanie nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy ograniczające dostęp do obszarów przechowywania nośników; zautomatyzowane mechanizmy kontrolujące próby dostępu i przyznawanie dostępu do obszarów przechowywania nośników].

MP-5	**TRANSPORT NOŚNIKÓW**		
	CEL OCENY: *Określić, czy organizacja:*		
	MP-5(a)	**MP-5(a)[1]**	*definiuje rodzaje nośników systemu informacyjnego, które mają być chronione i kontrolowane podczas transportu poza kontrolowanymi obszarami;*
		MP-5(a)[2]	*definiuje zabezpieczenia, które mają chronić i kontrolować nośniki systemów informacyjnych zdefiniowane przez organizację podczas transportu poza kontrolowanymi obszarami;*
		MP-5(a)[3]	*chroni i kontroluje zdefiniowane przez organizację nośniki systemów informacyjnych podczas transportu poza kontrolowanymi obszarami przy użyciu zdefiniowanych przez organizację środków bezpieczeństwa;*
	MP-5(b)	*zapewnia rozliczalność nośników systemu informacyjnego podczas transportu poza obszarami kontrolowanymi;*	
	MP-5(c)	*dokumentuje działania związane z transportem nośników systemów informacyjnych; oraz*	
	MP-5(d)	*zezwala na wykonywanie czynności związanych z transportem nośników systemu informacyjnego wyłącznie upoważnionemu personelowi.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące przechowywania nośników danych; polityka i procedury ochrony fizycznej i środowiskowej; zasady i procedury kontroli dostępu; plan bezpieczeństwa; nośniki systemu informacyjnego; wyznaczone strefy kontrolowane; inne odpowiednie dokumenty lub rejestry].		

MP-5	**TRANSPORT NOŚNIKÓW**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę i przechowywanie nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące przechowywania nośników informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające przechowywanie/ochronę nośników informacji].

MP-5(1)	**TRANSPORT NOŚNIKÓW | *OCHRONA POZA STREFAMI KONTROLNYMI***
[Włączone do: MP-5].	

MP-5(2)	**TRANSPORT NOŚNIKÓW | *DOKUMENTACJA DZIAŁAŃ***
[Włączone do: MP-5].	

MP-5(3)	**TRANSPORT NOŚNIKÓW | *KONWOJENCI***
	CEL OCENY: *Ustalić, czy organizacja zatrudnia konwojentów /nadzorujących transport nośników danych systemu informacyjnego poza kontrolowanymi obszarami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące transportu nośników; polityka I procedury ochrony fizycznej i środowiskowej; dokumentacja transportowa nośników danych systemu informacyjnego; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za transport nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

MP-5(4)	**TRANSPORT NOŚNIKÓW | *OCHRONA KRYPTOGRAFICZNA***
	CEL OCENY: *Ustalenie, czy organizacja stosuje mechanizmy kryptograficzne w celu ochrony poufności i integralności informacji przechowywanych na nośnikach cyfrowych podczas transportu poza kontrolowanymi strefami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące transportu nośników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja transportowa nośników danych systemu informacyjnego; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za transport nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficzne chroniące informacje na nośnikach cyfrowych podczas transportu poza kontrolowanymi strefami.].

MP-6	**SANITYZACJA NOŚNIKÓW**		
	CEL OCENY: *Określić, czy organizacja:*		
	MP-6(a)	**MP-6(a)[1]**	*definiuje nośniki systemu informacyjnego, które należy poddać sanityzacji przed:*
		MP-6(a)[1][a]	*utylizacją;*
		MP-6(a)[1][b]	*uwolnieniem spod kontroli organizacyjnej; lub*
		MP-6(a)[1][c]	*dopuszczeniem do ponownego użycia;*
		MP-6(a)[2]	*definiuje techniki lub procedury sanityzacyjne, które mają być stosowane przed sanityzacją mediów systemu informacyjnego zdefiniowanego przez organizację, przed:*
		MP-6(a)[2][a]	*utylizacją;*
		MP-6(a)[2][b]	*uwolnieniem spod kontroli organizacyjnej; lub*

MP-6	**SANITYZACJA NOŚNIKÓW**			
			MP-6(a)[2][c]	*dopuszczeniem do ponownego użycia;*
		MP-6(a)[3]	*poddaje sanityzacji nośniki systemu informacyjnego określone przez organizację przed ich usunięciem, uwolnieniem spod kontroli organizacyjnej lub udostępnieniem do ponownego wykorzystania przy użyciu określonych przez organizację technik lub procedur sanityzacyjnych, zgodnie z obowiązującymi standardami i zasadami organizacyjnymi; oraz*	
	MP-6(b)	*stosuje mechanizmy sanityzacji o sile i integralności proporcjonalnej do kategorii bezpieczeństwa lub klauzuli niejawności informacji.*		
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące sanityzacji i utylizacji nośników; obowiązujące standardy i zasady dotyczące sanityzacji nośników; rejestry sanityzacji nośników; zapisy z audytu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za sanityzację nośników informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z sanityzacją nośników; zautomatyzowane mechanizmy wspierające i/lub wdrażające sanityzację nośników].		

MP-6(1)	**SANITYZACJA NOŚNIKÓW | *PRZEGLĄD / ZATWIERDZANIE / ŚLEDZENIE / DOKUMENTOWANIE / WERYFIKACJA***	
	CEL OCENY: *Określić, czy organizacja:*	
	MP-6(1)[1]	*dokonuje przeglądu działań w zakresie sanityzacji utylizacji nośników;*
	MP-6(1)[2]	*zatwierdza działania w zakresie sanityzacji utylizacji nośników;*
	MP-6(1)[3]	*monitoruje działania w zakresie sanityzacji utylizacji nośników;*
	MP-6(1)[4]	*dokumentuje działania w zakresie sanityzacji utylizacji nośników; oraz*

MP-6(1)	**SANITYZACJA NOŚNIKÓW | *PRZEGLĄD / ZATWIERDZANIE / ŚLEDZENIE / DOKUMENTOWANIE / WERYFIKACJA***	
	MP-6(1)[5]	*weryfikuje działania w zakresie sanityzacji utylizacji nośników.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące sanityzacji utylizacji nośników; rejestry dotyczące sanityzacji usuwania nośników; rejestry przeglądowe dotyczące działań w zakresie sanityzacji usuwania nośników; zezwolenia na działania w zakresie sanityzacji usuwania nośników; rejestry dotyczące monitorowania; rejestry dotyczące; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za sanityzację i utylizację mediów w systemie informacyjnym; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z sanityzacją nośników; zautomatyzowane mechanizmy wspierające i/lub wdrażające sanityzację nośników].	

MP-6(2)	**SANITYZACJA NOŚNIKÓW | *TESTOWANIE SPRZĘTU***	
	CEL OCENY: *Określić, czy organizacja:*	
	MP-6(2)[1]	*określa częstotliwość testowania urządzeń i procedur sanityzacyjnych w celu sprawdzenia, czy osiągnięto zamierzone cele w zakresie sanityzacji; oraz*
	MP-6(2)[2]	*testuje sprzęt i procedury sanityzacyjne z częstotliwością określoną przez organizację w celu sprawdzenia, czy zamierzona sanityzacja jest osiągana.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące sanityzacji utylizacji nośników; procedury dotyczące testowania nośników poddawanych procesowi sanityzacji; wyniki testowania urządzeń i procedur służących do sanityzacji nośników; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za sanityzację nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

MP-6(2)	**SANITYZACJA NOŚNIKÓW | *TESTOWANIE SPRZĘTU***
	Test: [*wybierz spośród:* Procesy organizacyjne związane z sanityzacją nośników; zautomatyzowane mechanizmy wspierające i/lub wdrażające sanityzację nośników].

MP-6(3)	**SANITYZACJA NOŚNIKÓW | *TECHNIKI NIEDESTRUKCYJNE***	
	CEL OCENY: *Określić, czy organizacja:*	
	MP-6(3)[1]	*określa okoliczności wymagające sanityzacji przenośnych urządzeń pamięci masowej; oraz*
	MP-6(3)[2]	*stosuje niedestrukcyjne techniki sanityzacji przenośnych urządzeń pamięci masowej przed podłączeniem takich urządzeń do systemu informacyjnego, w określonych przez organizację okolicznościach wymagających sanityzacji przenośnych urządzeń pamięci masowej.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące sanityzacji utylizacji nośników; wykaz okoliczności wymagających przeprowadzenia sanityzacji przenośnych urządzeń pamięci masowej; dokumentacja dotycząca sanityzacji nośnika; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za sanityzację nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z sanityzacją nośników przenośnych urządzeń pamięci masowej; zautomatyzowane mechanizmy wspierające i/lub wdrażające sanityzację nośników].	

MP-6(4)	**SANITYZACJA NOŚNIKÓW | *KONTROLOWANE INFORMACJE JAWNE***
[Włączone do: MP-6].	

MP-6(5)	**SANITYZACJA NOŚNIKÓW | *INFORMACJE NIEJAWNE***
[Włączone do: MP-6].	

MP-6(5) SANITYZACJA NOŚNIKÓW | *INFORMACJE NIEJAWNE*
Zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

MP-6(6)SANITYZACJA NOŚNIKÓW | *NISZCZENIE NOŚNIKÓW DANYCH*
[Włączone do: MP-6].

MP-6(7) SANITYZACJA NOŚNIKÓW | *PODWÓJNA AUTORYZACJA*		
	CEL OCENY: *Określić, czy organizacja:*	
	MP-6(7)[1]	*definiuje nośniki systemu informacyjnego wymagające podwójnej autoryzacji do przeprowadzenia ich sanityzacji; oraz*
	MP-6(7)[2]	*wymusza podwójną autoryzację w celu przeprowadzenia sanityzacji nośników systemu informacyjnego zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące sanityzacji utylizacji nośników; lista nośników systemu informacyjnego wymagających podwójnej autoryzacji w celu przeprowadzenia sanityzacji; rejestry autoryzacji; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za sanityzację nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne wymagające podwójnej autoryzacji w zakresie sanityzacji nośników; zautomatyzowane mechanizmy wspierające i/lub wdrażające sanityzację nośników; zautomatyzowane mechanizmy wspierające i/lub wdrażające podwójną autoryzację].	

MP-6(8)	**SANITYZACJA NOŚNIKÓW | *ZDALNE KASOWANIE / WYMAZYWANIE INFORMACJI***		
	CEL OCENY: *Określić, czy organizacja:*		
	MP-6(8)[1]	*definiuje systemy informacyjne, komponenty systemu lub urządzenia, które mają być kasowane/wymazywane zdalnie lub w specyficznych warunkach organizacyjnych;*	
	MP-6(8)[2]	*definiuje warunki, w jakich informacje mają być kasowane/wymazywane z systemów informacyjnych, komponentów systemu lub urządzeń zdefiniowanych przez organizację; oraz*	
	MP-6(8)[3]	*zapewnia możliwość kasowania/wymazywania informacji z systemów informacyjnych, komponentów systemu lub urządzeń zdefiniowanych przez organizację:*	
		MP-6(8)[3][a]	*zdalnie; lub*
		MP-6(8)[3][b]	*w oparciu o zdefiniowane warunki organizacyjne.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące sanityzacji utylizacji nośników; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry sanityzacji nośników; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za sanityzację nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie kasowania/wymazywania nośników danych; zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcje kasowania/wymazywania nośników danych.].		

MP-7	**UŻYWANIE NOŚNIKÓW**	
	CEL OCENY: *Określić, czy organizacja:*	
	MP-7[1]	*definiuje rodzaje nośników systemu informacyjnego, które stosowanie ma być:*

MP-7	**UŻYWANIE NOŚNIKÓW**		
		MP-7[1][a]	*ograniczone do systemów informacyjnych lub części składowych systemu; lub*
		MP-7[1][b]	*zabronione w systemach informacyjnych lub komponentach systemu;*
	MP-7[2]	*definiuje systemy informacyjne lub elementy systemu, w których użycie zdefiniowanych przez organizację rodzajów nośników systemów informacyjnych ma być:*	
		MP-7[2][a]	*ograniczone; lub*
		MP-7[2][b]	*zabronione;*
	MP-7[3]	*określa środki bezpieczeństwa, które mają być stosowane w celu ograniczenia lub zakazania stosowania określonych przez organizację rodzajów nośników informacji w określonych przez organizację systemach informacyjnych lub komponentach systemu; oraz*	
	MP-7[4]	*ogranicza lub zakazuje korzystania z nośników informacji zdefiniowanych przez organizację w systemach informacyjnych lub komponentach systemu wykorzystujących zdefiniowane przez organizację zabezpieczenia bezpieczeństwa.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; polityka użytkowania systemu; procedury dotyczące ograniczeń w korzystaniu z nośników danych; plan bezpieczeństwa; zasady POSTĘPOWANIA; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za używanie nośników danych; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące używania nośników; zautomatyzowane mechanizmy ograniczające lub zakazujące używania nośników danych w systemach informacyjnych lub komponentach systemu].		

MP-7(1)	**UŻYWANIE NOŚNIKÓW | *ZABRONIONE WYKORZYSTANIE NIEZIDENTYFIKOWANEJ WŁASNOŚCI***
	CEL OCENY: *Określić, czy organizacja zakazuje stosowania przenośnych urządzeń magazynujących w systemach informacyjnych organizacji, gdy urządzenia takie nie mają możliwego do zidentyfikowania właściciela.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; polityka użytkowania systemu; procedury dotyczące ograniczeń w korzystaniu z nośników danych; plan bezpieczeństwa; zasady POSTĘPOWANIA; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za używanie nośników danych; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące wykorzystywania nośników; zautomatyzowane mechanizmy uniemożliwiające korzystanie z nośników w systemach informacyjnych lub komponentach systemu].

MP-7(2)	**UŻYWANIE NOŚNIKÓW | *ZABRONIONE WYKORZYSTANIE MEDIÓW ODPORNYCH NA SANITYZACJĘ***
	CEL OCENY: *Ustalić, czy organizacja zakazuje stosowania w systemach informacyjnych organizacji nośników odpornych na sanityzację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego, polityka użytkowania systemu; procedury dotyczące ograniczeń w korzystaniu z nośników danych; zasady postępowania; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za używanie nośników danych; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące wykorzystywania nośników; zautomatyzowane mechanizmy uniemożliwiające korzystanie z nośników w systemach informacyjnych lub komponentach systemu].

MP-8	**DEKLASYFIKACJA NOŚNIKÓW**		
	CEL OCENY: *Określić, czy organizacja:*		
	MP-8(a)	**MP-8(a)[1]**	*definiuje proces deklasyfikacji nośników w systemie informacyjnym;*
		MP-8(a)[2]	*definiuje siłę i integralność, z jaką mają być stosowane mechanizmy deklasyfikacji nośników;*
		MP-8(a)[3]	*ustanawia zdefiniowany przez organizację proces deklasyfikacji nośników systemu informacyjnego, który obejmuje stosowanie mechanizmów deklasyfikacji nośników o zdefiniowanej przez organizację sile i integralności;*
	MP-8(b)	*zapewnia, że proces deklasyfikacji nośników w systemie informacyjnym jest współmierny do procesu:*	
		MP-8(b)[1]	*kategorii bezpieczeństwa i/lub stopnia niejawności informacji, które mają zostać usunięte;*
		MP-8(b)[2]	*upoważnień dostępu posiadanych przez potencjalnych odbiorców zdeklasyfikowanych informacji;*
	MP-8(c)	*identyfikuje/definiuje nośniki systemu informacyjnego wymagające deklasyfikacji; oraz*	
	MP-8(d)	*obniża klasyfikację zidentyfikowanych nośników systemu informacyjnego za pomocą ustalonego procesu.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące obniżania kategorii nośników; dokumentacja kategoryzacji systemu; wykaz nośników wymagających obniżenia kategorii; rejestry obniżenia kategorii nośników; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za deklasyfikację nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z obniżaniem klasyfikacji nośników danych; zautomatyzowane mechanizmy wspierające i/lub wdrażające obniżanie klasyfikacji nośników danych].		

MP-8(1)	**DEKLASYFIKACJA NOŚNIKÓW | *DOKUMENTACJA PROCESU***
	CEL OCENY: *Ustalenie, czy organizacja dokumentuje działania związane z deklasyfikacją nośników systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące deklasyfikacji nośników; wykaz nośników wymagających obniżenia klasyfikacji; zapisy dotyczące obniżenia klasyfikacji nośników; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za deklasyfikację nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z obniżaniem klasyfikacji nośników danych; zautomatyzowane mechanizmy wspierające i/lub wdrażające obniżanie klasyfikacji nośników danych].

MP-8(2)	**DEKLASYFIKACJA NOŚNIKÓW | *TESTOWANIE SPRZĘTU***	
	CEL OCENY: *Określić, czy organizacja:*	
	MP-8(2)[1]	**MP-8(2)[1][a]** *definiuje testy, które mają być stosowane do obniżania klasyfikacji sprzętu;*
		MP-8(2)[1][b] *definiuje procedury weryfikacji prawidłowego wykonania deklasyfikacji;*
	MP-8(2)[2]	*określa częstotliwość przeprowadzania testów deklasyfikacji sprzętu oraz procedury weryfikacji prawidłowego wykonania deklasyfikacji; oraz*
	MP-8(2)[3]	*stosuje określone organizacyjnie testy urządzeń i procedury obniżania klasyfikacji w celu sprawdzenia poprawności działania, z częstotliwością określoną przez organizację.*

MP-8(2)	**DEKLASYFIKACJA NOŚNIKÓW | *TESTOWANIE SPRZĘTU***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; procedury dotyczące deklasyfikacji nośników; procedury dotyczące testowania urządzeń deklasyfikacji nośników; wyniki badań sprzętu i procedur obniżania klasyfikacji; zapisy z audytu: inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za deklasyfikację nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z obniżaniem klasyfikacji nośników danych; zautomatyzowane mechanizmy wspierające i/lub wdrażające obniżanie klasyfikacji nośników danych; zautomatyzowane mechanizmy wspomagające i/lub wdrażające testy urządzeń do deklasyfikacji].

MP-8(3)	**DEKLASYFIKACJA NOŚNIKÓW | *KONTROLOWANE INFORMACJE JAWNE***	
	CEL OCENY: *Określić, czy organizacja:*	
	MP-8(3)[1]	*definiuje kontrolowane informacje jawne zawarte na nośnikach systemu informacyjnego, które wymagają obniżenia klasyfikacji przed ich publicznym udostępnieniem; oraz*
	MP-8(3)[2]	*obniża klasyfikację nośników systemu informacyjnego zawierających zdefiniowane przez organizację kontrolowane informacje jawne przed ich publicznym udostępnieniem, zgodnie z obowiązującymi standardami i zasadami organizacyjnymi.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; polityka upoważnień dostępu; procedury dotyczące deklasyfikacji nośników zawierających kontrolowane informacje jawne; obowiązujące standardy i polityki organizacyjne dotyczące ochrony kontrolowanych informacji jawnych; rejestry deklasyfikacji nośników; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za deklasyfikację nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

MP-8(3)	DEKLASYFIKACJA NOŚNIKÓW | *KONTROLOWANE INFORMACJE JAWNE*
	Test: [*wybierz spośród:* Procesy organizacyjne związane z obniżaniem klasyfikacji nośników danych; zautomatyzowane mechanizmy wspierające i/lub wdrażające obniżanie klasyfikacji nośników danych].

MP-8(4)	DEKLASYFIKACJA NOŚNIKÓW | *INFORMACJE NIEJAWNE*
	CEL OCENY: *Określić, czy organizacja dokonuje deklasyfikacji (obniżenia klauzuli informacji) nośników danych zawierających informacje niejawne przed ich udostępnieniem osobom nieposiadającym stosownych poświadczeń bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony nośników danych systemu informacyjnego; polityka upoważnień dostępu; procedury dotyczące obniżania kategorii nośników zawierających informacje niejawne; procedury dotyczące postępowania z informacjami niejawnymi; przepisy, standardy i zasady dotyczące ochrony informacji niejawnych ustalone przez krajową władzę bezpieczeństwa; rejestry deklasyfikacji nośników; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za deklasyfikację nośników systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z obniżaniem klasyfikacji nośników danych; zautomatyzowane mechanizmy wspierające i/lub wdrażające obniżanie klasyfikacji nośników danych].

KATEGORIA PE - OCHRONA FIZYCZNA I ŚRODOWISKOWA

PE-1	**POLITYKA I PROCEDURY OCHRONY FIZYCZNEJ I ŚRODOWISKOWEJ**			
	CEL OCENY: *Określić, czy organizacja:*			
	PE-1(a)(1)	**PE-1(a)(1)[1]**	*opracowuje i dokumentuje politykę ochrony fizycznej i środowiskowej, która dotyczy:*	
			PE-1(a)(1)[1][a]	*celu;*
			PE-1(a)(1)[1][b]	*zakresu stosowania;*
			PE-1(a)(1)[1][c]	*ról;*
			PE-1(a)(1)[1][d]	*odpowiedzialności;*
			PE-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			PE-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			PE-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		PE-1(a)(1)[2]	*określa personel lub role, wśród których ma być rozpowszechniana polityka ochrony fizycznej i ochrony środowiskowej;*	
		PE-1(a)(1)[3]	*rozpowszechnia politykę ochrony fizycznej i ochrony środowiskowej wśród personelu lub ról zdefiniowanych przez organizację;*	
	PE-1(a)(2)	**PE-1(a)(2)[1]**	*opracowuje i dokumentuje procedury usprawniające realizację polityki ochrony fizycznej i środowiskowej oraz związane z nią zabezpieczenia w zakresie ochrony fizycznej i środowiskowej;*	
		PE-1(a)(2)[2]	*określa personel lub rolę, którym procedury mają być rozpowszechniane;*	
		PE-1(a)(2)[3]	*rozpowszechnia procedury wśród personelu i ról określonych przez organizację;*	

PE-1	**POLITYKA I PROCEDURY OCHRONY FIZYCZNEJ I ŚRODOWISKOWEJ**		
	PE-1(b)(1)	**PE-1(b)(1)[1]**	*określa częstotliwość przeglądów i aktualizacji aktualnej polityki w zakresie ochrony fizycznej i ochrony środowiskowej;*
		PE-1(b)(1)[2]	*opiniuje i aktualizuje aktualną politykę ochrony fizycznej i środowiskowej z częstotliwością określoną przez organizację;*
	PE-1(b)(2)	**PE-1(b)(2)[1]**	*określa częstotliwość przeglądów i aktualizacji obowiązujących procedur w zakresie ochrony fizycznej i ochrony środowiska; oraz*
		PE-1(b)(2)[2]	*opiniuje i aktualizuje aktualne procedury ochrony fizycznej i środowiskowej z określoną przez organizację częstotliwością.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury ochrony fizycznej i środowiskowej; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę fizyczną i ochronę środowiskową; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

PE-2	**ZEZWOLENIA NA DOSTĘP FIZYCZNY**		
	CEL OCENY: *Określić, czy organizacja:*		
	PE-2(a)	**PE-2(a)[1]**	*opracowuje listę osób mających uprawniony dostęp do obiektu, w którym znajduje się system informacyjny;*
		PE-2(a)[2]	*zatwierdza listę osób z uprawnionym dostępem do obiektu, w którym znajduje się system informacyjny;*
		PE-2(a)[3]	*prowadzi listę osób z uprawnionym dostępem do obiektu, w którym znajduje się system informacyjny;*
	PE-2(b)	*wydaje poświadczenia (przepustki) dostępu do obiektu;*	
	PE-2(c)	**PE-2(c)[1]**	*określa częstotliwość przeglądów listy dostępu wyszczególniającej autoryzowany dostęp do obiektu przez osoby;*

PE-2	**ZEZWOLENIA NA DOSTĘP FIZYCZNY**		
		PE-2(c)[2]	*dokonuje przeglądu listy dostępu zawierającej szczegółowe informacje na temat autoryzowanego dostępu do obiektów przez osoby z częstotliwością określoną przez organizację; oraz*
	PE-2(d)	*dokonuje aktualizacji listy osób posiadających dostęp do obiektu.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące zezwolenia na dostęp fizyczny; plan bezpieczeństwa; lista dostępu upoważnionego personelu; dane uwierzytelniające upoważnienia; przeglądy list dostępu fizycznego; zapisy dotyczące zakończenia dostępu fizycznego i związana z nimi dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za autoryzację dostępu fizycznego; personel organizacji posiadający fizyczny dostęp do obiektu systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące udzielania zezwoleń na dostęp fizyczny; zautomatyzowane mechanizmy wspierające i/lub wdrażające zezwolenia na dostęp fizyczny].		

PE-2(1)	**ZEZWOLENIA NA DOSTĘP FIZYCZNY | *DOSTĘP ZGODNIE Z POSIADANĄ POZYCJĄ / ROLĄ***
	CEL OCENY: *Ustalenie, czy organizacja zezwala na fizyczny dostęp do obiektu, w którym znajduje się system informacyjny, w zależności od posiadanego stanowiska lub roli.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące zezwolenia na dostęp fizyczny; dzienniki lub zapisy kontroli dostępu fizycznego; wykaz pozycji/roli i odpowiadające im zezwolenia na dostęp fizyczny; informacje dotyczące punktów wejścia i wyjścia do systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za autoryzację dostępu fizycznego; personel organizacji posiadający fizyczny dostęp do obiektu systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

PE-2(1)	**ZEZWOLENIA NA DOSTĘP FIZYCZNY | *DOSTĘP ZGODNIE Z POSIADANĄ POZYCJĄ / ROLĄ***
	Test: [*wybierz spośród:* Procesy organizacyjne dotyczące udzielania zezwoleń na dostęp fizyczny; zautomatyzowane mechanizmy wspierające i/lub wdrażające zezwolenia na dostęp fizyczny].

PE-2(2)	**ZEZWOLENIA NA DOSTĘP FIZYCZNY | *PODWÓJNA IDENTYFIKACJA***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-2(2)[1]	*określa listę dopuszczalnych form identyfikacji umożliwiających dostęp gości do obiektu, w którym znajduje się system informacyjny; oraz*
	PE-2(2)[2]	*wymaga przeprowadzenia podwójnej identyfikacji ze zdefiniowanej przez organizację listy dopuszczalnych form identyfikacji dostępu gości do obiektu, w którym znajduje się system informacyjny.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące zezwolenia na dostęp fizyczny; wykaz dopuszczalnych form identyfikacji umożliwiających dostęp gości do obiektu, w którym znajduje się system informacyjny; formularze zezwoleń na dostęp; dane uwierzytelniające dostęp; dzienniki lub rejestry kontroli dostępu fizycznego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za autoryzację dostępu fizycznego; personel organizacji posiadający fizyczny dostęp do obiektu systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące udzielania zezwoleń na dostęp fizyczny; zautomatyzowane mechanizmy wspierające i/lub wdrażające zezwolenia na dostęp fizyczny].	

<table>
<tr><th colspan="4">PE-2(3)Z ZWOLENIA NA DOSTĘP FIZYCZNY | OGRANICZANIE DOSTĘPU BEZ ASYSTY</th></tr>
<tr><td></td><td colspan="3">CEL OCENY:
Określić, czy organizacja:</td></tr>
<tr><td></td><td>PE-2(3)[1]</td><td colspan="2">określa poświadczenia dla upoważnionego personelu, które należy stosować w celu ograniczenia dostępu bez asysty do obiektu, w którym znajduje się system informacyjny;</td></tr>
<tr><td></td><td>PE-2(3)[2]</td><td colspan="2">ogranicza dostęp bez eskorty do obiektu, w którym znajduje się system informacyjny, do personelu, który posiada co najmniej jeden z poniższych elementów:</td></tr>
<tr><td></td><td></td><td>PE-2(3)[2][a]</td><td>poświadczenia bezpieczeństwa dotyczące wszystkich informacji przetwarzanych w systemie;</td></tr>
<tr><td></td><td></td><td>PE-2(3)[2][b]</td><td>formalne upoważnienia dostępu do wszystkich informacji przetwarzanych w systemie;</td></tr>
<tr><td></td><td></td><td>PE-2(3)[2][c]</td><td>konieczność uzyskania dostępu do wszystkich informacji przetwarzanych w systemie; i/lub</td></tr>
<tr><td></td><td></td><td>PE-2(3)[2][d]</td><td>poświadczenia organizacyjne.</td></tr>
<tr><td></td><td colspan="3">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące zezwolenia na dostęp fizyczny; lista dostępu upoważnionego personelu; poświadczenia bezpieczeństwa; upoważnienia dostępu; poświadczenia dostępu; dzienniki lub zapisy kontroli dostępu fizycznego; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za autoryzację dostępu fizycznego; personel organizacji posiadający fizyczny dostęp do obiektu systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji].
Test: [wybierz spośród: Procesy organizacyjne dotyczące udzielania zezwoleń na dostęp fizyczny; zautomatyzowane mechanizmy wspierające i/lub wdrażające zezwolenia na dostęp fizyczny].</td></tr>
</table>

<table>
<tr><th colspan="6">PE-3 KONTROLA DOSTĘPU FIZYCZNEGO</th></tr>
<tr><td rowspan="14"></td><td colspan="5">CEL OCENY:
Określić, czy organizacja:</td></tr>
<tr><td rowspan="13">PE-3(a)</td><td>PE-3(a)[1]</td><td colspan="3">określa punkty wejścia/wyjścia do obiektu, w którym znajduje się system informacyjny;</td></tr>
<tr><td rowspan="12">PE-3(a)[2]</td><td colspan="3">egzekwuje zezwolenie na dostęp fizyczny w zdefiniowanych przez organizację punktach wejścia/wyjścia do obiektu, w którym znajduje się system informacyjny:</td></tr>
<tr><td>PE-3(a)[2](1)</td><td colspan="2">weryfikując indywidualne upoważnienia dostępu przed udzieleniem dostępu do obiektu;</td></tr>
<tr><td rowspan="10">PE-3(a)[2](2)</td><td>PE-3(a)[2](2)[a]</td><td colspan="2">poprzez określenie systemów/urządzeń kontroli dostępu fizycznego, które mają być stosowane do kontroli wejścia / opuszczenia obiektu, w którym znajduje się system informacyjny;</td></tr>
<tr><td rowspan="9">PE-3(a)[2](2)[b]</td><td colspan="2">używając jednego lub kilku z poniższych sposobów kontroli wejścia / opuszczenia obiektu:</td></tr>
<tr><td>PE-3(a)[2](2)[b][1]</td><td>zdefiniowane organizacyjnie systemy / urządzenia kontroli dostępu fizycznego; i/lub</td></tr>
<tr><td>PE-3(a)[2](2)[b][2]</td><td>ochrona / strażnicy obiektu;</td></tr>
<tr><td rowspan="2">PE-3(b)</td><td>PE-3(b)[1]</td><td colspan="3">określa punkty wejścia/wyjścia, w których mają być prowadzone dzienniki kontroli dostępu fizycznego;</td></tr>
<tr><td>PE-3(b)[2]</td><td colspan="3">utrzymuje dzienniki kontroli dostępu fizycznego w odniesieniu do zdefiniowanych przez organizację punktów wejścia/wyjścia;</td></tr>
<tr><td>PE-3(c)</td><td>PE-3(c)[1]</td><td colspan="3">definiuje środki bezpieczeństwa, które mają być stosowane do kontroli dostępu do obszarów w obrębie obiektu oficjalnie wyznaczonych jako publicznie dostępne;</td></tr>
</table>

PE-3	**KONTROLA DOSTĘPU FIZYCZNEGO**			
		PE-3(c)[2]	*zapewnia określone przez organizację środki bezpieczeństwa, które mają być stosowane do kontroli dostępu do obszarów w obrębie obiektu, oficjalnie uznanych za publicznie dostępne;*	
	PE-3(d)	**PE-3(d)[1]**	*definiuje okoliczności podczas obecności osoby odwiedzającej, które wymagają:*	
			PE-3(d)[1][a]	*eskorty;*
			PE-3(d)[1][b]	*monitorowania;*
		PE-3(d)[2]	*zgodnie z określonymi przez organizację okolicznościami wymagającymi eskorty i monitoringu:*	
			PE-3(d)[2][a]	*eskortuje gości;*
			PE-3(d)[2][b]	*monitoruje aktywność odwiedzających;*
	PE-3(e)	**PE-3(e)[1]**	*zabezpiecza klucze;*	
		PE-3(e)[2]	*zabezpiecza kody dostępu;*	
		PE-3(e)[3]	*zabezpiecza inne fizyczne urządzenia dostępu;*	
	PE-3(f)	**PE-3(f)[1]**	*definiuje urządzenia dostępu fizycznego, które mają być ewidencjonowane;*	
		PE-3(f)[2]	*definiuje częstotliwość przeprowadzania inwentaryzacji zdefiniowanych organizacyjnie urządzeń dostępu fizycznego;*	
		PE-3(f)[3]	*przeprowadza inwentaryzację zdefiniowanych przez organizację urządzeń dostępu fizycznego z częstotliwością zdefiniowaną przez organizację;*	
	PE-3(g)	**PE-3(g)[1]**	*definiuje częstotliwość zmian kodów i kluczy; oraz*	
		PE-3(g)[2]	*zmienia kody i klucze z ustaloną przez organizację częstotliwością i/lub gdy:*	
			PE-3(g)[2][a]	*klucze zostały zgubione;*
			PE-3(g)[2][b]	*kody są naruszone;*
			PE-3(g)[2][c]	*poszczególne osoby zostaną przeniesione lub zwolnione z organizacji.*

PE-3	**KONTROLA DOSTĘPU FIZYCZNEGO**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu fizycznego; plan bezpieczeństwa; logi lub zapisy kontroli dostępu fizycznego; ewidencja urządzeń kontroli dostępu fizycznego; punkty wejścia i wyjścia do/z systemu informacyjnego; ewidencja zmian kombinacji kodów i blokad; miejsca przechowywania urządzeń kontroli dostępu fizycznego; urządzenia kontroli dostępu fizycznego; wykaz środków bezpieczeństwa kontrolujących dostęp do wyznaczonych obszarów publicznie dostępnych w obrębie obiektu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie kontroli dostępu fizycznego; zautomatyzowane mechanizmy wspierające i/lub wdrażające kontrolę dostępu fizycznego; urządzenia kontroli dostępu fizycznego].

PE-3(1)	**KONTROLA DOSTĘPU FIZYCZNEGO | *DOSTĘP DO SYSTEMU INFORMACYJNEGO***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-3(1)[1]	*definiuje przestrzenie fizyczne zawierające jeden lub więcej składników systemu informacyjnego; oraz*
	PE-3(1)[2]	*egzekwuje zezwolenia na dostęp fizyczny do systemu informacyjnego w uzupełnieniu do kontroli dostępu fizycznego do obiektu, w określonych przez organizację przestrzeniach fizycznych zawierających jeden lub więcej składników systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu fizycznego; logi lub zapisy kontroli dostępu fizycznego; urządzenia kontroli dostępu fizycznego; upoważnienia dostępu; poświadczenia dostępu; punkty wejścia i wyjścia do systemu informacyjnego; wykaz obszarów w obrębie obiektu, w których występują zagęszczenia elementów systemu informacyjnego lub elementów systemu informacyjnego wymagających dodatkowej ochrony fizycznej; inne odpowiednie dokumenty lub rejestry].	

PE-3(1)	**KONTROLA DOSTĘPU FIZYCZNEGO | *DOSTĘP DO SYSTEMU INFORMACYJNEGO***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za autoryzacją dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne kontroli dostępu fizycznego do systemu/komponentów systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające kontrolę dostępu fizycznego do obszarów obiektu zawierających komponenty systemu informacyjnego].

PE-3(2)	**KONTROLA DOSTĘPU FIZYCZNEGO | *OBIEKT / OBSZAR SYSTEMU INFORMACYJNEGO***		
	CEL OCENY: *Określić, czy organizacja:*		
	PE-3(2)[1]	*określa częstotliwość przeprowadzania kontroli bezpieczeństwa fizycznej strefy obiektu lub systemu informacyjnego przed nieautoryzowanym:*	
		PE-3(2)[1][a]	*upublicznieniem informacji; lub*
		PE-3(2)[1][b]	*usunięciem elementów systemu informacyjnego; oraz*
	PE-3(2)[2]	*przeprowadza, z częstotliwością określoną przez organizację, kontrole bezpieczeństwa fizycznej strefy obiektu lub systemu informacyjnego, przed nieautoryzowanym:*	
		PE-3(2)[2][a]	*upublicznieniem informacji; lub*
		PE-3(2)[2][b]	*usunięciem elementów systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu fizycznego; logi lub zapisy kontroli dostępu fizycznego; rejestry kontroli bezpieczeństwa; sprawozdania z audytu bezpieczeństwa; sprawozdania z inspekcji bezpieczeństwa; dokumentacja dotycząca rozmieszczenia obiektów; punkty wejścia i wyjścia z systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

PE-3(2)	**KONTROLA DOSTĘPU FIZYCZNEGO | *OBIEKT / OBSZAR SYSTEMU INFORMACYJNEGO***
	Test: [*wybierz spośród:* Procesy organizacyjne dotyczące kontroli dostępu fizycznego do obiektu i/lub systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające kontrolę dostępu fizycznego do obiektu lub systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające kontrole bezpieczeństwa w odniesieniu do nieuprawnionego dostępu do informacji].

PE-3(3)	**KONTROLA DOSTĘPU FIZYCZNEGO | *CIĄGŁOŚĆ OCHRONY / ALARMY / MONITOROWANIE***	
	CEL OCENY: *Ustalić, czy organizacja stosuje jeden lub więcej z poniższych elementów do monitorowania każdego punktu dostępu fizycznego do obiektu, w którym znajduje się system informacyjny, 24 godziny na dobę, 7 dni w tygodniu:*	
	PE-3(3)[1]	*ochrona/strażnicy; i/lub*
	PE-3(3)[2]	*system alarmowy.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu fizycznego; logi lub zapisy kontroli dostępu fizycznego; urządzenia kontroli dostępu fizycznego; zapisy nadzoru nad obiektem; dokumentacja dotycząca rozmieszczenia obiektu; punkty wejścia i wyjścia systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące kontroli dostępu fizycznego do obiektu, w którym znajduje się system informacyjny; zautomatyzowane mechanizmy wspierające lub wdrażające kontrolę dostępu fizycznego do obiektu, w którym znajduje się system informacyjny].	

PE-3(4)	**KONTROLA DOSTĘPU FIZYCZNEGO | *ZAMYKANE OBUDOWY***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-3(4)[1]	*definiuje elementy systemu informacyjnego, które mają być chronione przed nieautoryzowanym dostępem fizycznym za pomocą zamykanych na klucz fizycznych obudów; oraz*
	PE-3(4)[2]	*używa zamykanych na klucz fizycznych obudów w celu ochrony, zdefiniowanych przez organizację komponentów systemu informacyjnego, przed nieautoryzowanym fizycznym dostępem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu fizycznego; plan bezpieczeństwa; wykaz elementów systemu informacyjnego wymagających ochrony poprzez zamykane obudowy fizyczne; zamykane obudowy fizyczne; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zamykane obudowy fizyczne].	

PE-3(5)	**KONTROLA DOSTĘPU FIZYCZNEGO | *OCHRONA PRZED MANIPULACJĄ***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-3(5)[1]	*definiuje zabezpieczenia, jakie mają być stosowane w celu wykrywania i/lub zapobiegania fizycznym manipulacjom lub zmianom komponentów sprzętowych określonych przez organizację w ramach systemu informacyjnego;*
	PE-3(5)[2]	*definiuje elementy sprzętu komputerowego w ramach systemu informacyjnego, w odniesieniu do których mają być stosowane środki bezpieczeństwa w celu wykrywania lub zapobiegania fizycznym manipulacjom lub zmianom tych elementów;*
	PE-3(5)[3]	*stosuje określone przez organizację środki bezpieczeństwa w celu wykonania jednego lub więcej z poniższych działań:*

PE-3(5)	**KONTROLA DOSTĘPU FIZYCZNEGO | *OCHRONA PRZED MANIPULACJĄ***		
		PE-3(5)[3][a]	*wykrywanie fizycznej manipulacji lub zmiany w określonych przez organizację elementach sprzętowych systemu informacyjnego; i/lub*
		PE-3(5)[3][b]	*zapobieganie fizycznym manipulacjom lub zmianom w zdefiniowanych organizacyjnie komponentach sprzętowych systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu fizycznego; wykaz środków bezpieczeństwa mających na celu wykrywanie/zapobieganie fizycznym manipulacjom lub zmianom elementów sprzętowych systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne mające na celu wykrywanie / zapobieganie fizycznym manipulacjom lub zmianom elementów sprzętowych systemu informacyjnego; zautomatyzowane mechanizmy/zabezpieczenia wspierające i/lub wdrażające wykrywanie / zapobieganie fizycznym manipulacjom lub zmianom elementów sprzętowych systemu informacyjnego].		

PE-3(6)	**KONTROLA DOSTĘPU FIZYCZNEGO | *TESTY PENETRACYJNE OBIEKTU***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-3(6)[1]	*określa częstotliwość niezapowiedzianych testów penetracyjnych mających na celu ominięcie lub obejście mechanizmów bezpieczeństwa związanych z fizycznymi punktami dostępu do obiektu; oraz*
	PE-3(6)[2]	*przeprowadza testy penetracyjne z określoną przez organizację częstotliwością, które obejmują niezapowiedziane próby ominięcia lub obejścia środków bezpieczeństwa powiązanych z fizycznymi punktami dostępu do obiektu.*

PE-3(6)	**KONTROLA DOSTĘPU FIZYCZNEGO | *TESTY PENETRACYJNE OBIEKTU***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu fizycznego; procedury dotyczące przeprowadzania testów penetracyjnych; zasady zaangażowania i związana z tym dokumentacja; wyniki testów penetracyjnych; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z testami penetracyjnym i obiektu; zautomatyzowane mechanizmy wspierające i/lub wdrażające testy penetracyjne obiektu].

PE-4	**KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO**	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-4[1]	*definiuje linie dystrybucji i transmisji systemu informacyjnego wymagające fizycznej kontroli dostępu;*
	PE-4[2]	*definiuje zabezpieczenia, które mają być stosowane do kontroli fizycznego dostępu do zdefiniowanych przez organizację linii dystrybucyjnych i transmisyjnych systemu informacyjnego w obiektach organizacyjnych; oraz*
	PE-4[3]	*kontroluje fizyczny dostęp do zdefiniowanych przez organizację linii dystrybucyjnych i transmisyjnych systemu informacyjnego w obrębie obiektów organizacyjnych, przy użyciu zdefiniowanych przez organizację zabezpieczeń.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu do medium transmisyjnego; dokumentacja projektowa systemu informacyjnego; schematy łączności okablowania urządzeń; wykaz fizycznych zabezpieczeń linii dystrybucyjnych i przesyłowych systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

PE-4	**KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO**
	Test: [*wybierz spośród:* Procesy organizacyjne w zakresie kontroli dostępu do linii dystrybucyjnych i przesyłowych; zautomatyzowane mechanizmy/środki bezpieczeństwa wspierające i/lub wdrażające kontrolę dostępu do linii dystrybucyjnych i przesyłowych].

PE-5	**KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA**
	CEL OCENY: *Ustalić, czy organizacja kontroluje fizyczny dostęp do wejścia - wyjścia systemu informacyjnego, aby uniemożliwić osobom nieupoważnionym uzyskanie dostępu do wyników przetwarzania informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu do monitorów/wyświetlaczy; rozmieszczenie elementów systemu informacyjnego w obiekcie; wyświetlanie aktualnych informacji z elementów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie kontroli dostępu do urządzeń wejścia - wyjścia; zautomatyzowane mechanizmy wspierające i/lub wdrażające kontrolę dostępu do urządzeń wejścia - wyjścia].

PE-5(1)	**KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | *DOSTĘP UPOWAŻNIONYCH OSÓB DO URZĄDZEŃ***		
	CEL OCENY: *Określić, czy organizacja:*		
	PE-5(1)(a)	**PE-5(1)(a)[1]**	*definiuje urządzenia wejścia - wyjścia, wymagające fizycznego dostęp do danych wyjściowych;*
		PE-5(1)(a)[2]	*kontroluje fizyczny dostęp do danych wyjściowych z urządzeń wyjściowych zdefiniowanych przez organizację; oraz*

PE-5(1)	**KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | *DOSTĘP UPOWAŻNIONYCH OSÓB DO URZĄDZEŃ***	
	PE-5(1)(b)	*zapewnia, że tylko autoryzowane osoby mają dostęp do danych wyjściowych z urządzenia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu fizycznego; wykaz urządzeń wejścia - wyjścia i powiązanych danych wyjściowych z urządzenia wymagających fizycznej kontroli dostępu; dzienniki lub zapisy fizycznej kontroli dostępu dotyczące obszarów zawierających urządzenia wejścia - wyjścia i przetwarzane w nich dane wyjściowe; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie kontroli dostępu do urządzeń wejścia - wyjścia; zautomatyzowane mechanizmy wspierające i/lub wdrażające kontrolę dostępu do urządzeń wejścia - wyjścia].	

PE-5(2)	**KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | *DOSTĘP DO DANYCH NA PODSTAWIE INDYWIDUALNEJ TOŻSAMOŚCI***		
	CEL OCENY: *Określić, czy:*		
	PE-5(2)(a)	**PE-5(2)(a)[1]**	*organizacja określa urządzenia wejścia - wyjścia, przetwarzające dane wymagające fizycznej kontroli dostępu;*
		PE-5(2)(a)[2]	*system informacyjny kontroluje fizyczny dostęp do danych wyjściowych z urządzeń określonych przez organizację; oraz*
	PE-5(2)(b)	*system informacyjny łączy indywidualną tożsamość z udzielaniem dostępu do danych wyjściowych z urządzenia.*	

PE-5(2)	**KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | *DOSTĘP DO DANYCH NA PODSTAWIE INDYWIDUALNEJ TOŻSAMOŚCI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu fizycznego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz urządzeń wejścia - wyjścia i powiązanych danych wyjściowych z urządzenia wymagających fizycznej kontroli dostępu; dzienniki lub zapisy fizycznej kontroli dostępu dotyczące obszarów zawierających urządzenia wejścia - wyjścia i przetwarzane w nich dane wyjściowe; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie kontroli dostępu do urządzeń wejścia - wyjścia; zautomatyzowane mechanizmy wspierające i/lub wdrażające kontrolę dostępu do urządzeń wejścia - wyjścia].

PE-5(3)	**KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | *OZNACZANIE URZĄDZEŃ WEJŚCIA - WYJŚCIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-5(3)[1]	*określa urządzenia wejścia - wyjścia systemu informacyjnego, wskazuje jakie informacje mogą być wysyłane z urządzenia (klasyfikacja informacji); oraz*
	PE-5(3)[2]	*oznacza urządzenia wejścia - wyjścia systemu informacyjnego zdefiniowane przez organizację, wskazując informacje, które mogą być wysyłane z urządzenia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli dostępu fizycznego; oznaczenia bezpieczeństwa rodzajów informacji, które mogą być przesyłane z urządzeń wyjściowych systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

PE-5(3)	**KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | *OZNACZANIE URZĄDZEŃ WEJŚCIA - WYJŚCIA***
	Test: [*wybierz spośród:* Procesy organizacyjne dotyczące znakowania urządzeń wejścia - wyjścia].

PE-6	**MONITOROWANIE DOSTĘPU FIZYCZNEGO**		
	CEL OCENY: *Określić, czy organizacja:*		
	PE-6(a)	*monitoruje fizyczny dostęp do obiektu, w którym znajduje się system informacyjny, w celu wykrywania i reagowania na incydenty związane z bezpieczeństwem fizycznym;*	
	PE-6(b)	**PE-6(b)[1]**	*definiuje częstotliwość przeglądania dzienników dostępu fizycznego;*
		PE-6(b)[2]	*definiuje zdarzenia lub potencjalne wskazania zdarzeń wymagających przeglądu dzienników dostępu fizycznego;*
		PE-6(b)[3]	*dokonuje przeglądu dzienników dostępu fizycznego z określoną przez organizację częstotliwością i po wystąpieniu określonych przez organizację zdarzeń lub potencjalnych wskazań dotyczących zdarzeń; oraz*
	PE-6(c)	*koordynuje wyniki przeglądów i dochodzeń z możliwością reagowania na incydenty organizacyjne.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące monitorowania dostępu fizycznego; plan bezpieczeństwa; dzienniki lub zapisy dostępu fizycznego; zapisy dostępu fizycznego z monitoringu; przeglądy dzienników dostępu fizycznego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacji odpowiedzialny za procedury reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu dostępu fizycznego; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie dostępu fizycznego; zautomatyzowane mechanizmy wspierające i/lub wdrażające przegląd dzienników dostępu fizycznego].		

PE-6(1)	**MONITOROWANIE DOSTĘPU FIZYCZNEGO | *ALARMY WŁAMANIOWE / URZĄDZENIA NADZORUJĄCE***
	CEL OCENY: *Ustalić, czy organizacja monitoruje fizyczne alarmy włamaniowe i sprzęt nadzorujący fizyczną kontrolę dostępu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące monitorowania dostępu fizycznego; plan bezpieczeństwa; dzienniki lub zapisy dostępu fizycznego; zapisy dostępu fizycznego z monitoringu; przeglądy dzienników dostępu fizycznego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacji odpowiedzialny za procedury reagowania na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne monitorowania fizycznych alarmów o włamaniach i urządzeń nadzorujący fizyczną kontrolę dostępu; zautomatyzowane mechanizmy wspierające i/lub wdrażające fizyczne monitorowanie dostępu; zautomatyzowane mechanizmy wspierające i/lub wdrażające fizyczne alarmy o włamaniach i nadzorujące urządzenia fizycznej kontroli dostępu].

PE-6(2)	**MONITOROWANIE DOSTĘPU FIZYCZNEGO | *AUTOMATYCZNE ROZPOZNAWANIE WŁAMANIA / INFORMOWANIE***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-6(2)[1]	*definiuje klasy/typy włamań, które mają być rozpoznawane przez zautomatyzowane mechanizmy;*
	PE-6(2)[2]	*definiuje czynności zaradcze, które mają być inicjowane przez zautomatyzowane mechanizmy w przypadku rozpoznania klas/typów włamań zdefiniowanych przez organizację; oraz*
	PE-6(2)[3]	*stosuje zautomatyzowane mechanizmy rozpoznawania klas / typów włamań zdefiniowanych w organizacji oraz inicjowania zdefiniowanych w organizacji działań zaradczych.*

PE-6(2)	**MONITOROWANIE DOSTĘPU FIZYCZNEGO | *AUTOMATYCZNE ROZPOZNAWANIE WŁAMANIA / INFORMOWANIE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące monitorowania dostępu fizycznego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; lista czynności zaradczych, które należy zainicjować po rozpoznaniu określonych klas/typów włamań; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie monitorowania dostępu fizycznego; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie dostępu fizycznego; zautomatyzowane mechanizmy wspierające i/lub wdrażające rozpoznawanie klas/typów włamań i inicjowanie reakcji].

PE-6(3)	**MONITOROWANIE DOSTĘPU FIZYCZNEGO | *MONITORING WIZYJNY***		
	CEL OCENY: *Określić, czy organizacja:*		
	PE-6(3)[1]	*definiuje obszary operacyjne, w których ma być stosowany monitoring wizyjny;*	
	PE-6(3)[2]	*definiuje czas przechowywania nagrań wideo z obszarów operacyjnych zdefiniowanych przez organizację;*	
	PE-6(3)[3]	**PE-6(3)[3][a]**	*stosuje monitoring wizyjny obszarów operacyjnych zdefiniowanych organizacyjnie; oraz*
		PE-6(3)[3][b]	*zachowuje nagrania wideo przez określony przez organizację okres czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące monitorowania dostępu fizycznego; monitoring wizyjny sprzętu wykorzystywanego do nadzorowania obszarów operacyjnych; nagrywanie obrazu z obszarów operacyjnych, w których wykorzystywany jest monitoring wizyjny; monitoring wizyjny dzienników lub rejestrów sprzętu; inne odpowiednie dokumenty lub rejestry].		

PE-6(3)	**MONITOROWANIE DOSTĘPU FIZYCZNEGO | *MONITORING WIZYJNY***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne monitorowania dostępu fizycznego; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie dostępu fizycznego; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitoring wizyjny].

PE-6(4)	**MONITOROWANIE DOSTĘPU FIZYCZNEGO | *MONITOROWANIE DOSTĘPU FIZYCZNEGO DO SYSTEMÓW INFORMACYJNYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-6(4)[1]	*definiuje przestrzenie fizyczne zawierające jeden lub więcej składników systemu informacyjnego; oraz*
	PE-6(4)[2]	*monitoruje fizyczny dostęp do systemu informacyjnego, oprócz monitorowania fizycznego dostępu do obiektu, w zdefiniowanych przez organizację przestrzeniach fizycznych zawierających jeden lub więcej składników systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące monitorowania dostępu fizycznego; logi lub zapisy kontroli dostępu fizycznego; urządzenia kontroli dostępu fizycznego; upoważnienia dostępu; poświadczenia dostępu; wykaz obszarów w obrębie obiektu, na których występują koncentracje elementów systemu informacyjnego lub elementów systemu informacyjnego wymagających dodatkowego fizycznego monitorowania dostępu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za monitorowanie dostępu fizycznego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne monitorowania dostępu fizycznego do systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie dostępu fizycznego do stref obiektu zawierających komponenty systemu informacyjnego].	

PE-7	**KONTROLA GOŚCI**
[Włączone do: PE-2 i PE-3].	

PE-8	**REJESTRACJA DOSTĘPU GOŚCI**		
	CEL OCENY: *Określić, czy organizacja:*		
	PE-8(a)	**PE-8(a)[1]**	*określa okres czasu, w którym należy prowadzić ewidencję dostępu gości do obiektu, w którym znajduje się system informacyjny;*
		PE-8(a)[2]	*utrzymuje zapisy dotyczące dostępu gości do obiektu, w którym znajduje się system informacyjny, przez określony przez organizację okres czasu;*
	PE-8(b)	**PE-8(b)[1]**	*definiuje częstotliwość przeglądania zapisów dotyczących dostępu osób odwiedzających; oraz*
		PE-8(b)[2]	*przegląda zapisy dostępu odwiedzających z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące rejestracji dostępu gości; plan bezpieczeństwa; dzienniki lub rejestry kontroli dostępu osób odwiedzających; rejestr dostępu osób odwiedzających lub przeglądy dzienników dostępu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za dostęp do rejestrów gości; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z utrzymaniem i przeglądem rejestracji dostępu gości; zautomatyzowane mechanizmy wspierające i/lub wdrażające utrzymanie i przegląd rejestracji dostępu gości].		

PE-8(1)	**REJESTRACJA DOSTĘPU GOŚCI | *AUTOMATYCZNA REJESTRACJA / PRZEGLĄD***
	CEL OCENY: *Ustalić, czy organizacja stosuje zautomatyzowane mechanizmy ułatwiające utrzymanie i przegląd rejestracji dostępu gości.*

PE-8(1)	**REJESTRACJA DOSTĘPU GOŚCI | *AUTOMATYCZNA REJESTRACJA / PRZEGLĄD***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące rejestracji dostępu gości; automatyczne mechanizmy wspomagające zarządzanie rejestracją dostępu gości; dzienniki lub rejestry kontroli dostępu gości; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za dostęp do rejestrów gości; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z utrzymaniem i przeglądem rejestracji dostępu gości; zautomatyzowane mechanizmy wspierające i/lub wdrażające utrzymanie i przegląd rejestracji dostępu gości].

PE-8(2)	**REJESTRACJA DOSTĘPU GOŚCI | *EWIDENCJA DOSTĘPU FIZYCZNEGO***
[Włączone do: PE-2].	

PE-9	**WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE**
	CEL OCENY: *Ustalić, czy organizacja chroni urządzenia zasilające i okablowanie zasilające systemu informacyjnego przed uszkodzeniem i zniszczeniem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące urządzeń elektroenergetycznych / ochrony okablowania; obiekty, w których znajdują się urządzenia elektroenergetyczne / okablowanie; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę urządzeń energetycznych/ okablowania; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające ochronę urządzeń elektroenergetycznych/ okablowania].

PE-9(1)	**WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE | *REDUNDANCJA OKABLOWANIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-9(1)[1]	*określa odległość, na jaką mają być fizycznie odseparowane nadmiarowe tory okablowania zasilającego; oraz*
	PE-9(1)[2]	*korzysta z nadmiarowych torów okablowania zasilającego, które są fizycznie oddzielone przez zdefiniowaną przez organizację odległość.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące urządzeń elektroenergetycznych / ochrony okablowania; obiekty, w których znajdują się urządzenia elektroenergetyczne / okablowanie; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę urządzeń energetycznych/ okablowania; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające ochronę urządzeń elektroenergetycznych/ okablowania].	

PE-9(2)	**WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE | *AUTOMATYCZNA KONTROLA NAPIĘCIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-9(2)[1]	*definiuje krytyczne elementy systemu informacyjnego, które wymagają automatycznej kontroli napięcia; oraz*
	PE-9(2)[2]	*wykorzystuje automatyczną kontrolę napięcia w zdefiniowanych organizacyjnie krytycznych komponentach systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli napięcia; plan bezpieczeństwa; lista krytycznych elementów systemu informacyjnego wymagających automatycznej kontroli napięcia; mechanizmy automatycznej kontroli napięcia i związane z nimi konfiguracje; inne odpowiednie dokumenty lub rejestry].	

PE-9(2)	**WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE | *AUTOMATYCZNA KONTROLA NAPIĘCIA***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę środowiskową komponentów systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające automatyczną kontrolę napięcia].

PE-10	**WYŁĄCZENIE AWARYJNE**		
	CEL OCENY: *Określić, czy organizacja:*		
	PE-10(a)	*zapewnia możliwość wyłączenia zasilania systemu informacyjnego lub poszczególnych elementów systemu w sytuacjach awaryjnych;*	
	PE-10(b)	**PE-10(b)[1]**	*definiuje lokalizację wyłączników awaryjnych lub urządzeń systemu informacyjnego lub jego elementów;*
		PE-10(b)[2]	*umieszcza wyłącznik i lub urządzenia wyłączania awaryjnego w miejscu określonym przez organizację, z uwzględnieniem systemu informacyjnego lub elementu systemu, w celu ułatwienia bezpiecznego i łatwego dostępu dla personelu; oraz*
	PE-10(c)	*zabezpiecza funkcję awaryjnego wyłączania zasilania przed nieautoryzowaną aktywacją.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące wyłączania awaryjnego źródeł zasilania; plan bezpieczeństwa; sterownik i lub wyłącznik i awaryjne; miejsca, w których znajdują się wyłącznik i urządzenia do awaryjnego wyłączania; zabezpieczenia chroniące możliwość awaryjnego odcięcia zasilania przez osoby nieupoważnione; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za obsługę wyłączania zasilania awaryjnego (zarówno wdrażanie, jaki wykorzystywanie tej funkcji); personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wdrażające awaryjne wyłączanie zasilania].		

PE-10(1)	**WYŁĄCZENIE AWARYJNE | *PRZYPADKOWA / NIEAUTORYZOWANA AKTYWACJA***
[Włączone do: PE-10].	

PE-11	**ZASILANIE AWARYJNE**	
	CEL OCENY: *Ustalić, czy organizacja zapewnia krótkoterminowe, nieprzerwane zasilanie w celu wsparcia jednego lub kilku z poniższych elementów, w przypadku utraty pierwotnego źródła zasilania:*	
	PE-11[1]	*kontrolowanego zamknięcia systemu informacyjnego; i/lub*
	PE-11[2]	*przejście systemu informacyjnego na długoterminowe źródło zapasowe.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące zasilania awaryjnego; zasilacz bezprzerwowy UPS; dokumentacja dotycząca zasilacza bezprzerwowego UPS; protokoły z badań zasilacza bezprzerwowego UPS; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zasilanie awaryjne i/lub planowanie; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zasilanie bezprzerwowe; zasilanie bezprzerwowe].	

PE-11(1)	**ZASILANIE AWARYJNE | *DŁUGOTERMINOWE ALTERNATYWNE ZASILANIE - MINIMALNA ZDOLNOŚĆ OPERACYJNA***
	CEL OCENY: *Ustalić, czy organizacja zapewnia długoterminowe alternatywne źródło zasilania systemu informacyjnego, które jest zdolne do utrzymania minimalnej wymaganej Zdolności operacyjnej w przypadku przedłużonej niedostępności podstawowego źródła zasilania.*

PE-11(1)	**ZASILANIE AWARYJNE | *DŁUGOTERMINOWE ALTERNATYWNE ZASILANIE - MINIMALNA ZDOLNOŚĆ OPERACYJNA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące zasilania awaryjnego; alternatywne źródło zasilania; dokumentacja dotycząca alternatywnego źródła zasilania; zapisy z badań alternatywnego źródła zasilania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zasilanie awaryjne i/lub planowanie; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wdrażające alternatywne źródła zasilania; alternatywne źródła zasilania].

PE-11(2)	**ZASILANIE AWARYJNE | *DŁUGOTERMINOWE ALTERNATYWNE SAMOOBSŁUGOWE ŹRÓDŁO ZASILANIA***		
	CEL OCENY: *Ustalić, czy organizacja zapewnia długoterminowe zastępcze źródło zasilania dla systemu informacyjnego, które jest:*		
	PE-11(2)(a)	*samoobsługowe;*	
	PE-11(2)(b)	*niezależne od zewnętrznego źródła zasilania;*	
	PE-11(2)(c)	*zdolne do utrzymania jednej z poniższych właściwości w przypadku długotrwałej utraty pierwotnego źródła energii:*	
		PE-11(2)(c)[1]	*minimalną wymaganą zdolność operacyjną; lub*
		PE-11(2)(c)[2]	*pełną zdolność operacyjną.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące zasilania awaryjnego; alternatywne źródło zasilania; dokumentacja dotycząca alternatywnego źródła zasilania; zapisy z badań alternatywnego źródła zasilania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zasilanie awaryjne i/lub planowanie; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

PE-11(2)	**ZASILANIE AWARYJNE | *DŁUGOTERMINOWE ALTERNATYWNE SAMOOBSŁUGOWE ŹRÓDŁO ZASILANIA***
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wdrażające alternatywne źródła zasilania; alternatywne źródła zasilania].

PE-12	**OŚWIETLENIE AWARYJNE**	
	CEL OCENY: *Ustalić, czy organizacja wykorzystuje i konserwuje automatyczne oświetlenie awaryjne systemu informacyjnego, które:*	
	PE-12[1]	*aktywuje się w przypadku zaniku lub przerwy w dostawie energii elektrycznej; oraz*
	PE-12[2]	*obejmuje wyjścia awaryjne i drogi ewakuacyjne w obrębie obiektu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące oświetlenia awaryjnego; dokumentacja oświetlenia awaryjnego; zapisy testów oświetlenia awaryjnego; wyjścia awaryjne i drogi ewakuacyjne; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za oświetlenie awaryjne i/lub planowanie; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające lub wdrażające funkcje oświetlenia awaryjnego].	

PE-12(1)	**OŚWIETLENIE AWARYJNE | *ZASADNICZE DZIAŁANIA / FUNKCJE BIZNESOWE***
	CEL OCENY: *Ustalić, czy organizacja zapewnia oświetlenie awaryjne dla wszystkich obszarów w obiekcie wspomagających istotne misje i funkcje biznesowe.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące oświetlenia awaryjnego; dokumentacja oświetlenia awaryjnego; zapisy testów oświetlenia awaryjnego; wyjścia awaryjne i drogi ewakuacyjne; obszary/lokalizacje w obrębie obiektu wspierające istotne misje i funkcje biznesowe; inne odpowiednie dokumenty lub rejestry].

PE-12(1)	**OŚWIETLENIE AWARYJNE | *ZASADNICZE DZIAŁANIA / FUNKCJE BIZNESOWE***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za oświetlenie awaryjne i/lub planowanie; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające lub wdrażające funkcje oświetlenia awaryjnego].

PE-13	**OCHRONA PRZECIWPOŻAROWA**	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-13[1]	*stosuje urządzenia/systemy gaśnicze i detekcyjne na potrzeby systemu informacyjnego, które są obsługiwane przez niezależne źródło energii; oraz*
	PE-13[2]	*utrzymuje urządzenia/systemy gaśnicze i detekcji pożaru na potrzeby systemu informacyjnego, które są obsługiwane przez niezależne źródło energii.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące ochrony przeciwpożarowej; urządzenia/systemy gaśnicze i detekcyjne; dokumentacja urządzeń / systemów gaśniczych i detekcyjnych; zapisy testowe urządzeń/systemów gaśniczych i detekcyjnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za urządzenia/systemy wykrywania i gaszenia pożaru; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające urządzenia/systemy gaśnicze/wykrywające pożar].	

PE-13(1)	**OCHRONA PRZECIWPOŻAROWA | *URZĄDZENIA / SYSTEMY WYKRYWANIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-13(1)[1]	*wyznacza personel lub role, które należy powiadomić w przypadku pożaru;*

PE-13(1)	**OCHRONA PRZECIWPOŻAROWA | *URZĄDZENIA / SYSTEMY WYKRYWANIA***		
	PE-13(1)[2]	*definiuje osoby odpowiedzialne za działania ratunkowe, które należy powiadomić w przypadku pożaru;*	
	PE-13(1)[3]	*stosuje urządzenia/systemy wykrywania pożaru systemu informacyjnego, które w przypadku pożaru:*	
		PE-13(1)[3][a]	*aktywują się automatycznie;*
		PE-13(1)[3][b]	*powiadamiają personel lub role określone przez organizację; oraz*
		PE-13(1)[3][c]	*powiadamiają określone przez organizację osoby reagujące na sytuacje kryzysowe.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące ochrony przeciwpożarowej; opis obiektu, w którym znajduje się system informacyjny; umowy SAL dotyczące usług alarmowych; rejestry testów urządzeń/systemów do gaszenia i wykrywania pożaru; dokumentacja urządzeń/systemów do gaszenia i wykrywania pożaru; powiadomienia o alarmach/zdarzeniach pożarowych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za urządzenia/systemy wykrywania i gaszenia pożarów; personel organizacji odpowiedzialny za powiadamianie odpowiedniego ról i osób/służb odpowiedzialnych za reagowanie na wypadek pożaru; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające lub wdrażające urządzenia/systemy wykrywania pożaru; aktywacja urządzeń/systemów wykrywania pożaru (symulacja); zautomatyzowane powiadomienia].	

PE-13(2)	**OCHRONA PRZECIWPOŻAROWA | *URZĄDZENIA / SYSTEMY GASZENIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-13(2)[1]	*definiuje personel lub role, którym należy zapewnić automatyczne powiadamianie o wszelkich aktywacjach urządzeń/systemów przeciwpożarowych w systemie informacyjnym;*

PE-13(2)	**OCHRONA PRZECIWPOŻAROWA | *URZĄDZENIA / SYSTEMY GASZENIA***		
	PE-13(2)[2]	*definiuje osoby odpowiedzialne za reagowanie kryzysowe, które mają otrzymywać automatyczne powiadomienia o każdym uruchomieniu urządzeń/systemów gaśniczych w systemie informacyjnym;*	
	PE-13(2)[3]	*stosuje urządzenia/systemy gaśnicze w systemie informacyjnym, które zapewniają automatyczne powiadamianie o wszelkich aktywacjach urządzeń/systemów gaśniczych w systemie informacyjnym:*	
		PE-13(2)[3][a]	*personel lub role określone przez organizację; oraz*
		PE-13(2)[3][b]	*zdefiniowane organizacyjnie osoby odpowiedzialne za reagowanie w nagłych wypadkach.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące ochrony przeciwpożarowej; dokumentacja dotycząca urządzeń/systemów gaśniczych i detekcji pożaru; opis obiektu, w którym znajduje się system informacyjny; SLA usług alarmowych; dokumentacja dotycząca testów urządzeń/systemów gaśniczych i detekcji pożaru; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za urządzenia/systemy wykrywania i gaszenia pożaru; personel organizacji odpowiedzialny za automatyczne powiadamianie odpowiedniego personelu, ról i służb ratowniczych o każdym uruchomieniu urządzeń/systemów przeciwpożarowych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające lub wdrażające urządzenia/systemy gaśnicze; uruchamianie urządzeń/systemów gaśniczych (symulacja); zautomatyzowane powiadomienia].	

PE-13(3)	**OCHRONA PRZECIWPOŻAROWA | *AUTOMATYCZNE GASZENIE POŻARU***
	CEL OCENY: *Określić, czy organizacja stosuje automatyczne gaszenie pożarów w systemie informacyjnym, gdy obiekt nie jest obsługiwany w sposób ciągły.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące ochrony przeciwpożarowej; dokumentacja dotycząca urządzeń/systemów gaśniczych i detekcji pożaru; opis obiektu, w którym znajduje się system informacyjny; SLA usług alarmowych; dokumentacja

PE-13(3)	**OCHRONA PRZECIWPOŻAROWA | *AUTOMATYCZNE GASZENIE POŻARU***
	dotycząca testów urządzeń/systemów gaśniczych i detekcji pożaru; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za urządzenia/systemy wykrywania i gaszenia pożaru; personel organizacji odpowiedzialny za automatyczne powiadamianie odpowiedniego personelu, ról i służb ratowniczych o każdym uruchomieniu urządzeń/systemów przeciwpożarowych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające lub wdrażające urządzenia/systemy gaśnicze; uruchamianie urządzeń/systemów gaśniczych (symulacja)].

PE-13(4)	**OCHRONA PRZECIWPOŻAROWA | *INSPEKCJE***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-13(4)[1]	*określa częstotliwość inspekcji przeprowadzanych w obiekcie przez upoważnionych i wykwalifikowanych inspektorów;*
	PE-13(4)[2]	*zapewnia, że obiekt będzie poddawany inspekcjom przez inspektorów upoważnionych i wykwalifikowanych z częstotliwością określoną przez organizację;*
	PE-13(4)[3]	*określa okres czasu na usunięcie nieprawidłowości stwierdzonych podczas inspekcji obiektu; oraz*
	PE-13(4)[4]	*rozwiązuje stwierdzone niedociągnięcia w określonym przez organizację okresie czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące ochrony przeciwpożarowej; plan bezpieczeństwa; opis obiektu, w którym znajduje się system informacyjny; plany inspekcji; wyniki inspekcji; sprawozdania z inspekcji; protokoły z badań urządzeń/systemów wykrywania i gaszenia pożaru; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie, zatwierdzanie i przeprowadzanie inspekcji ochrony przeciwpożarowej; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

PE-14	**KONTROLA TEMPERATURY I *WILGOTNOŚCI***		
	CEL OCENY: *Określić, czy organizacja:*		
	PE-14(a)	**PE-14(a)[1]**	*określa dopuszczalne poziomy temperatury, które mają być utrzymywane w obiekcie, w którym znajduje się system informacyjny;*
		PE-14(a)[2]	*określa dopuszczalne poziomy wilgotności, które mają być utrzymywane w obiekcie, w którym znajduje się system informacyjny;*
		PE-14(a)[3]	*utrzymuje poziomy temperatury w obiekcie, w którym znajduje się system informacyjny, na określonych przez organizację poziomach;*
		PE-14(a)[4]	*utrzymuje poziomy wilgotności w obiekcie, w którym znajduje się system informacyjny, na określonych przez organizację poziomach;*
	PE-14(b)	**PE-14(b)[1]**	*określa częstotliwość monitorowania poziomów temperatury;*
		PE-14(b)[2]	*definiuje częstotliwość monitorowania poziomów wilgotności;*
		PE-14(b)[3]	*monitoruje poziomy temperatury z częstotliwością zdefiniowaną przez organizację; oraz*
		PE-14(b)[4]	*monitoruje poziom wilgotności z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli temperatury i wilgotności; plan bezpieczeństwa; kontrola temperatury i wilgotności; opis obiektu, w którym znajduje się system informacyjny; dokumentacja kontroli temperatury i wilgotności; rejestr pomiarów temperatury i wilgotności; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczenie środowiskowe systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wdrażające utrzymanie i monitorowanie poziomów temperatury i wilgotności].		

PE-14(1)	**KONTROLA TEMPERATURY I WILGOTNOŚCI | *STEROWANIE AUTOMATYCZNE***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-14(1)[1]	*stosuje automatyczną kontrolę temperatury w obiekcie, aby zapobiec potencjalnym fluktuacjom szkodliwym dla systemu informacyjnego; oraz*
	PE-14(1)[2]	*stosuje automatyczną kontrolę wilgotności w obiekcie, aby zapobiec potencjalnym fluktuacjom szkodliwym dla systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące kontroli temperatury i wilgotności; opis obiektu, w którym znajduje się system informacyjny; zautomatyzowane mechanizmy pomiaru temperatury i wilgotności; kontrola temperatury i wilgotności; dokumentacja dotycząca pomiarów temperatury i wilgotności; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczenie środowiskowe systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub zapewniające poziomy temperatury i wilgotności].	

PE-14(2)	**KONTROLA TEMPERATURY I WILGOTNOŚCI | *MONITOROWANIE, ALARMOWANIE / POWIADOMIENIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-14(2)[1]	*stosuje monitorowanie temperatury, które generuje alarm o zmianach potencjalnie szkodliwych dla personelu lub sprzętu; i/lub*
	PE-14(2)[2]	*stosuje monitorowanie temperatury, które generuje powiadomienia o zmianach potencjalnie szkodliwych dla personelu lub sprzętu;*
	PE-14(2)[3]	*stosuje monitorowanie wilgotności, które generuje alarm o zmianach potencjalnie szkodliwych dla personelu lub sprzętu; i/lub*

PE-14(2)	**KONTROLA TEMPERATURY I WILGOTNOŚCI | *MONITOROWANIE, ALARMOWANIE / POWIADOMIENIA***	
	PE-14(2)[4]	*stosuje monitoring wilgotności, który generuje powiadomienia o zmianach potencjalnie szkodliwych dla personelu lub sprzętu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące monitorowania temperatury i wilgotności; opis obiektu, w którym znajduje się system informacyjny; rejestry lub zapisy dotyczące monitorowania temperatury i wilgotności; zapisy zmian poziomu temperatury i wilgotności, które generują alarmy lub powiadomienia; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczenie środowiskowe systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wdrażające monitorowanie temperatury i wilgotności].	

PE-15	**OCHRONA PRZED ZALANIEM**	
	CEL OCENY: *Ustalić, czy organizacja chroni system informacyjny przed uszkodzeniami wynikającym i z wycieku wody, poprzez zapewnienie głównych zaworów odcinających lub izolacyjnych, które są:*	
	PE-15[1]	*dostępne;*
	PE-15[2]	*prawidłowo działają; oraz*
	PE-15[3]	*znane kluczowemu personelowi.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące ochrony przed zalaniem; opis obiektu, w którym znajduje się system informacyjny; główne zawory odcinające; lista kluczowego personelu posiadającego wiedzę na temat lokalizacji i procedur uruchamiania głównych zaworów odcinających w instalacji wodno-kanalizacyjnej; dokumentacja głównego zaworu odcinającego; inne odpowiednie dokumenty lub rejestry].	

PE-15	**OCHRONA PRZED ZALANIEM**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczenie środowiskowe systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Główne zawory odcinające; proces organizacyjny uruchamiania głównych zaworów odcinających wodę].

PE-15(1)	**OCHRONA PRZED ZALANIEM | *AUTOMATYCZNE WYKRYWANIE***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-15(1)[1]	*określa personel lub role, które mają być powiadamiane w przypadku wykrycia obecności wody w pobliżu systemu informacyjnego;*
	PE-15(1)[2]	*stosuje zautomatyzowane mechanizmy wykrywania obecności wody w pobliżu systemu informacyjnego; oraz*
	PE-15(1)[3]	*powiadamia określony przez organizację personel lub role w przypadku wykrycia obecności wody w pobliżu systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące ochrony przed zalaniem; opis obiektu, w którym znajduje się system informacyjny; zautomatyzowane mechanizmy zamykania zaworów odcinających wodę; zautomatyzowane mechanizmy wykrywające obecność wody w pobliżu systemu informacyjnego; powiadomienia/ alarmy o wykryciu wody w obiekcie systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczenie środowiskowe systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zdolność wykrywania wody i ostrzegania o zagrożeniu systemu informacyjnego.].	

PE-16	**DOSTAWA I USUWANIE**
	CEL OCENY: *Określić, czy organizacja:*

PE-16	**DOSTAWA I USUWANIE**	
	PE-16[1]	*definiuje rodzaje komponentów systemu informacyjnego, które mają być autoryzowane, monitorowane i kontrolowane, podczas dostawy i usuwania komponentów z obiektu;*
	PE-16[2]	*autoryzuje zdefiniowane przez organizację komponenty systemu informacyjnego dostarczane do obiektu;*
	PE-16[3]	*monitoruje dostarczane do obiektu, definiowane przez organizację, komponenty systemu informacyjnego;*
	PE-16[4]	*kontroluje dostarczane do obiektu, definiowane przez organizację, komponenty systemu informacyjnego;*
	PE-16[5]	*autoryzuje dostarczane do obiektu, definiowane przez organizację, komponenty systemu informacyjnego;*
	PE-16[6]	*monitoruje elementy systemu informacyjnego dostarczane do obiektu;*
	PE-16[7]	*kontroluje organizacyjnie zdefiniowane komponenty systemu informacyjnego usuwane z obiektu;*
	PE-16[8]	*prowadzi ewidencję komponentów systemu informacyjnego dostarczanych do obiektu; oraz*
	PE-16[9]	*prowadzi ewidencję elementów systemu informacyjnego usuwanych z obiektu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące dostawy i usuwania komponentów systemu informacyjnego z obiektu; plan bezpieczeństwa; opis obiektu, w którym znajduje się system informacyjny; ewidencja produktów dostarczanych i usuwanych z obiektu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kontrolę elementów systemu informacyjnego dostarczanych i usuwanych z obiektu; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie autoryzacji, monitorowania i kontroli elementów związanych z systemem informacyjnym, dostarczanych i usuwanych z obiektu; zautomatyzowane mechanizmy wspomagające i/lub wdrażające autoryzację, monitorowanie i kontrolę elementów systemu informacyjnego dostarczanych i usuwanych z obiektu].	

PE-17	**ZAPASOWE MIEJSCE PRACY**		
	CEL OCENY: *Określić, czy organizacja:*		
	PE-17(a)	**PE-17(a)[1]**	definiuje środki bezpieczeństwa, które należy stosować w zapasowych miejscach pracy;
		PE-17(a)[2]	stosuje określone organizacyjnie środki bezpieczeństwa w zapasowych miejscach pracy;
	PE-17(b)	*ocenia, w miarę możliwości, skuteczność środków bezpieczeństwa w zapasowych miejscach pracy; oraz*	
	PE-17(c)	*zapewnia personelowi możliwość komunikacji z personelem odpowiedzialnym za bezpieczeństwo informacji w przypadku zdarzeń lub problemów związanych z bezpieczeństwem.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury postępowania personelu organizacyjnego w zapasowych miejscach pracy; plan bezpieczeństwa; wykaz środków bezpieczeństwa wymaganych w zapasowych miejscach pracy; oceny środków bezpieczeństwa w z zapasowych miejscach pracy; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zatwierdzający korzystanie z zapasowych miejsc pracy; personel organizacji korzystający z zapasowych miejsc pracy; personel organizacji oceniający zabezpieczenia zapasowych miejsc pracy; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z bezpieczeństwem w zapasowym miejscu pracy; zautomatyzowane mechanizmy wspomagające pracę w zapasowym miejscu pracy; środki bezpieczeństwa w zapasowym miejscu pracy; środki komunikacji pomiędzy personelem w zapasowym miejscu pracy, a personelem ochrony].		

PE-18	**LOKALIZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO**	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-18[1]	*definiuje fizyczne zagrożenia, które mogą prowadzić do potencjalnego uszkodzenia elementów systemu informacyjnego w obiekcie;*

PE-18	**LOKALIZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO**	
	PE-18[2]	*definiuje zagrożenia środowiskowe, które mogą spowodować potencjalne szkody dla elementów systemu informacyjnego w obiekcie;*
	PE-18[3]	*pozycjonuje elementy systemów informacyjnych w obrębie obiektu w celu zminimalizowania potencjalnych szkód wynikających z zagrożeń fizycznych i środowiskowych zdefiniowanych przez organizację; oraz*
	PE-18[4]	*pozycjonuje elementy systemu informacyjnego w obiekcie, aby zminimalizować możliwość nieautoryzowanego dostępu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące rozmieszczenia elementów systemu informacyjnego; dokumentacja przedstawiająca lokalizację i rozmieszczenie elementów systemu informacyjnego na terenie obiektu; lokalizacje zawierające elementy systemu informacyjnego na terenie obiektu; wykaz zagrożeń fizycznych i środowiskowych mogących spowodować uszkodzenie elementów systemu informacyjnego na terenie obiektu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za pozycjonowanie elementów systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące rozmieszczania elementów systemu informacyjnego].	

PE-18(1)	**LOKALIZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *LOKALIZACJA OBIEKTU***	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-18(1)[1]	*planuje lokalizację lub teren obiektu, w którym znajduje się system informacyjny, w kontekście zagrożeń fizycznych;*
	PE-18(1)[2]	*planuje lokalizację lub teren obiektu, w którym znajduje się system informacyjny, w kontekście zagrożeń dla środowiska naturalnego;*
	PE-18(1)[3]	*w przypadku istniejących obiektów, uwzględnia zagrożenia fizyczne w swojej strategii ograniczania ryzyka; oraz*
	PE-18(1)[4]	*w odniesieniu do istniejących obiektów, uwzględnia zagrożenia dla środowiska naturalnego w swojej strategii ograniczania ryzyka.*

PE-18(1)	**LOKALIZACJA KOMPONENTÓW SYSTEMU INFORMACYJNEGO | *LOKALIZACJA OBIEKTU***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; dokumenty dotyczące planowania obiektu; organizacyjna szacowanie ryzyka, plan ciągłości działania; dokumentacja dotycząca strategii ograniczania ryzyka; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za wybór lokalizacji obiektu, w którym znajduje się system informacyjny; personel organizacji odpowiedzialny za ograniczanie ryzyka; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z planowaniem obiektu].

PE-19	**ULOT INFORMACJI / ELEKTROMAGNETYCZNA EMISJA UJAWNIAJĄCA**
	CEL OCENY: *Ustalić, czy organizacja chroni system informacyjny przed ulotem informacji / elektromagnetyczną emisją ujawniającą wynikającą z promieniowania elektromagnetycznego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące ulotu informacji / elektromagnetycznej emisji ujawniającej wynikającej z promieniowania elektromagnetycznego; mechanizmy zabezpieczające system informacyjny przed elektromagnetyczną emisją ujawniającą; opis obiektu, w którym znajduje się system informacyjny; zapisy z testów elektromagnetycznej emisji ujawniającej; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczenie środowiskowe systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* zautomatyzowane mechanizmy wspomagające i/lub realizujące zabezpieczenia przed ulotem informacji / elektromagnetyczną emisją ujawniającą].

PE-19(1)	**ULOT INFORMACJI / ELEKTROMAGNETYCZNA EMISJA UJAWNIAJĄCA | *POLITYKI I PROCEDURY (TEMPEST)***	
	CEL OCENY: *Określenie, czy organizacja zapewnia ochronę, zgodnie z krajowymi politykami i procedurami dotyczącymi emisji i rozwiązaniami TEMPEST, na podstawie kategorii bezpieczeństwa lub klasyfikacji informacji:*	
	PE-19(1)[1]	*komponentów systemu informacyjnego;*
	PE-19(1)[2]	*powiązanej komunikacji danych; oraz*
	PE-19(1)[3]	*sieci.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące wycieku informacji zgodne z polityką i procedurami krajowym i w zakresie emisji i rozwiązaniami TEMPEST; dokumentacja projektowa części składowych systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczenie środowiskowe systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Elementy systemu informacyjnego służące zapewnieniu zgodności z krajowymi politykami i procedurami w zakresie emisji i rozwiązaniami TEMPEST].	

PE-20	**MONITOROWANIE I ŚLEDZENIE ZASOBÓW**	
	CEL OCENY: *Określić, czy organizacja:*	
	PE-20(a)	
	PE-20(a)[1]	*określa zasoby, których lokalizacja i przemieszczanie mają być śledzone i monitorowane;*
	PE-20(a)[2]	*definiuje technologie lokalizacji zasobów, które mają być stosowane do śledzenia i monitorowania lokalizacji i przemieszczania się zasobów określonych przez organizację;*
	PE-20(a)[3]	*definiuje kontrolowane obszary, w których należy śledzić i monitorować zasoby określone przez organizację;*

PE-20	**MONITOROWANIE I ŚLEDZENIE ZASOBÓW**		
		PE-20(a)[4]	*wykorzystuje technologie lokalizacji zasobów, które mają być stosowane do śledzenia i monitorowania lokalizacji i przemieszczania zdefiniowanych przez organizację zasobów w obrębie określonych przez organizację obszarów kontrolowanych; oraz*
	PE-20(b)	*zapewnia, że technologie lokalizacji aktywów są stosowane zgodnie z obowiązującymi przepisami, rozporządzeniami wykonawczymi, dyrektywami, przepisami, zasadami, standardami i wytycznymi.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka w zakresie ochrony fizycznej i ochrony środowiskowej; procedury dotyczące monitorowania i śledzenia zasobów; technologie lokalizacji zasobów i związana z nimi dokumentacja konfiguracyjna; wykaz zasobów organizacyjnych wymagających śledzenia i monitorowania; rejestry monitorowania i śledzenia zasobów; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za monitorowanie i śledzenie zasobów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie śledzenia i monitorowania zasobów; zautomatyzowane mechanizmy wspierające i/lub wdrażające śledzenie i monitorowanie zasobów].		

KATEGORIA PL - PLANOWANIE

PL-1	**POLITYKA I PROCEDURY PLANOWANIA BEZPIECZEŃSTWA**			
	CEL OCENY: *Określić, czy organizacja:*			
	PL-1(a)(1)	**PL-1(a)(1)[1]**	*opracowuje i dokumentuje politykę planowania, która dotyczy:*	
			PL-1(a)(1)[1][a]	*celu;*
			PL-1(a)(1)[1][b]	*zakresu stosowania;*
			PL-1(a)(1)[1][c]	*ról;*
			PL-1(a)(1)[1][d]	*odpowiedzialności;*
			PL-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			PL-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			PL-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		PL-1(a)(1)[2]	*określa personel lub role, wśród których ma być rozpowszechniana polityka planowania;*	
		PL-1(a)(1)[3]	*rozpowszechnia politykę planowania wśród personelu lub ról zdefiniowanych przez organizację;*	
	PL-1(a)(2)	**PL-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrażanie polityki planowania i związanych z nią kontroli planowania;*	
		PL-1(a)(2)[2]	*określa personel lub role, wśród których procedury mają być rozpowszechniane;*	
		PL-1(a)(2)[3]	*rozpowszechnia procedury wśród personelu lub ról określonych w organizacji;*	
	PL-1(b)(1)	**PL-1(b)(1)[1]**	*definiuje częstotliwość przeglądów i aktualizacji aktualnej polityki planowania;*	
		PL-1(b)(1)[2]	*opiniuje i aktualizuje aktualne polityki planowania z częstotliwością określoną przez organizację;*	

PL-1	**POLITYKA I PROCEDURY PLANOWANIA BEZPIECZEŃSTWA**		
	PL-1(b)(2)	**PL-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji aktualnych procedur planowania; oraz*
		PL-1(b)(2)[2]	*opiniuje i aktualizuje aktualne procedury planowania z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury planowania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

PL-2	**PLAN BEZPIECZEŃSTWA SYSTEMU**		
	CEL OCENY: *Określić, czy organizacja:*		
	PL-2(a)	*opracowuje plan bezpieczeństwa systemu informacyjnego, który:*	
		PL-2(a)(1)	*jest zgodny ze strukturą organizacyjną;*
		PL-2(a)(2)	*definiuje obszary autoryzacji systemu;*
		PL-2(a)(3)	*opisuje środowisko operacyjne systemu informacyjnego w kontekście misji i procesów biznesowych;*
		PL-2(a)(4)	*zapewnia kategoryzację bezpieczeństwa systemu informacyjnego wraz z uzasadnieniem;*
		PL-2(a)(5)	*opisuje środowisko operacyjne systemu informacyjnego oraz relacje z innymi systemami informacyjnymi lub powiązania z nimi;*
		PL-2(a)(6)	*zawiera przegląd wymagań bezpieczeństwa odnoszących się do systemu;*
		PL-2(a)(7)	*identyfikuje poprawki (patche) bezpieczeństwa;*
		PL-2(a)(8)	*opisuje środki bezpieczeństwa stosowane lub planowane w celu spełnienia wymagań, w tym uzasadnienie decyzji dostosowawczych;*

PL-2	**PLAN BEZPIECZEŃSTWA SYSTEMU**		
		PL-2(a)(9)	*jest sprawdzany i zatwierdzany przed realizacją planu, przez kierownika jednostki organizacyjnej lub osobę przez niego upoważnioną;*
	PL-2(b)	**PL-2(b)[1]**	*wyznacza personel lub role, którym mają być przekazywane kopie planu bezpieczeństwa oraz kolejne zmiany w planie;*
		PL-2(b)[2]	*rozprowadza kopie planu bezpieczeństwa i informuje o kolejnych zmianach w planie personel lub role wyznaczone przez organizację;*
	PL-2(c)	**PL-2(c)[1]**	*definiuje częstotliwość przeglądów planu bezpieczeństwa systemu informacyjnego;*
		PL-2(c)[2]	*dokonuje przeglądu planu bezpieczeństwa systemu informacyjnego z częstotliwością określoną przez organizację;*
	PL-2(d)	*uaktualnia plan bezpieczeństwa na wypadek:*	
		PL-2(d)[1]	*zmiany w systemie informacyjnym/środowisku działania;*
		PL-2(d)[2]	*zidentyfikowania problemów w trakcie realizacji planu;*
		PL-2(d)[3]	*zidentyfikowania problemów w trakcie oceny środków bezpieczeństwa;*
	PL-2(e)	*chroni plan bezpieczeństwa przed nieautoryzowanym:*	
		PL-2(e)[1]	*ujawnieniem; oraz*
		PL-2(e)[2]	*modyfikacją.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania bezpieczeństwa; procedury dotyczące opracowywania i wdrażania planu bezpieczeństwa; procedury dotyczące przeglądów i aktualizacji planów bezpieczeństwa; dokumentacja struktury organizacyjnej; plan bezpieczeństwa systemu informacyjnego; rejestry przeglądów i aktualizacji planu bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie i realizację planów bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

PL-2	**PLAN BEZPIECZEŃSTWA SYSTEMU**
	Test: [*wybierz spośród:* Procesy organizacyjne związane z opracowaniem / przeglądem / aktualizacją / zatwierdzaniem planu bezpieczeństwa; zautomatyzowane mechanizmy wspierające plan bezpieczeństwa systemu informacyjnego].

PL-2(1)	**PLAN BEZPIECZEŃSTWA SYSTEMU | *KONCEPCJA DZIAŁANIA***
[Włączone do: PL-7].	

PL-2(2)	**PLAN BEZPIECZEŃSTWA SYSTEMU | *ARCHITEKTURA FUNKCJONALNA***
[Włączone do: PL-8].	

PL-2(3)	**PLAN BEZPIECZEŃSTWA SYSTEMU | *PLANOWANIE / KOORDYNACJA Z INNYMI PODMIOTAMI ORGANIZACYJNYMI***	
	CEL OCENY: *Określić, czy organizacja:*	
	PL-2(3)[1]	*definiuje osoby lub grupy, z którymi działania związane z bezpieczeństwem, wpływające na system informacyjny, mają być planowane i koordynowane przed ich wykonaniem, w celu zmniejszenia wpływu na inne jednostki organizacyjne; oraz*
	PL-2(3)[2]	*planuje i koordynuje działania związane z bezpieczeństwem, wpływające na system informacyjny, z określonymi przez organizację osobami lub grupami przed ich przeprowadzeniem, w celu zmniejszenia wpływu na inne jednostki organizacyjne.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania bezpieczeństwa; zasady kontroli dostępu; polityka planowania awaryjnego; procedury dotyczące planowania działań związanych z bezpieczeństwem systemu informacyjnego; plan bezpieczeństwa systemu informacyjnego; plan ciągłości działania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

PL-2(3)	**PLAN BEZPIECZEŃSTWA SYSTEMU | *PLANOWANIE / KOORDYNACJA Z INNYMI PODMIOTAMI ORGANIZACYJNYMI***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie i realizację planów bezpieczeństwa; osoby lub grupy organizacyjne, z którymi działania związane z bezpieczeństwem mają być planowane i koordynowane; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

PL-3	**AKTUALIZACJA PLANU BEZPIECZEŃSTWA SYSTEMU**
[Włączone do: PL-2].	

PL-4	**ZASADY POSTĘPOWANIA**		
	CEL OCENY: *Określić, czy organizacja:*		
	PL-4(a)	**PL-4(a)[1]**	*ustanawia, dla osób wymagających dostępu do systemu informacyjnego, zasady, które opisują ich obowiązki i oczekiwane zachowania w odniesieniu do informacji i korzystania z systemu informacyjnego;*
		PL-4(a)[2]	*udostępnia osobom wymagającym dostępu do systemu informacyjnego zasady opisujące ich obowiązki i oczekiwane zachowanie w odniesieniu do informacji i korzystania z systemu informacyjnego;*
	PL-4(b)	*przed udzieleniem zezwolenia na dostęp do informacji i systemu informacyjnego uzyskuje od takich osób podpisane potwierdzenia, że przeczytały, zrozumiały i zgadzają się przestrzegać zasad postępowania;*	
	PL-4(c)	**PL-4(c)[1]**	*określa częstotliwość przeglądów i aktualizacji zasad postępowania;*
		PL-4(c)[2]	*opiniuje i aktualizuje zasady postępowania z częstotliwością określoną przez organizację; oraz*
	PL-4(d)	*wymaga od osób, które podpisały poprzednią wersję zasad postepowania, przeczytania i ponownego podpisania tych reguł, w przypadku ich zmiany / zaktualizowania.*	

PL-4	**ZASADY POSTĘPOWANIA**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania bezpieczeństwa; procedury dotyczące zasad postępowania użytkowników systemu informacyjnego; zasady postępowania; podpisane oświadczenia; zapisy zasad postępowania i aktualizacja zasad postępowania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ustalanie, przegląd i aktualizację zasad zachowania; personel organizacji, który jest upoważnionym użytkownikiem systemu informacyjnego oraz podpisał i zaakceptował zasady postępowania; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące ustanawiania, przeglądu, rozpowszechniania i aktualizacji zasad postepowania; zautomatyzowane mechanizmy wspierające i/lub wdrażające ustanawianie, przegląd, rozpowszechnianie i aktualizację zasad postępowania].

PL-4(1)	**ZASADY POSTĘPOWANIA | *MEDIA SPOŁECZNE I OGRANICZENIA SIECIOWE***	
	CEL OCENY: *Ustalić, czy organizacja w regulaminie postępowania zawiera wyraźne ograniczenia w zakresie:*	
	PL-4(1)[1]	*korzystania z mediów społecznościowych / serwisów sieciowych; oraz*
	PL-4(1)[2]	*publikowania informacji organizacyjnych w publicznych stronach internetowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania bezpieczeństwa; procedury dotyczące zasad postępowania użytkowników systemu informacyjnego; zasady postępowania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ustanawianie, przeglądanie i aktualizację zasad postępowania; personel organizacji, który jest upoważnionym użytkownikiem systemu informacyjnego i podpisał zasady postępowania; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne mające na celu ustanowienie zasad postępowania; zautomatyzowane mechanizmy wspierające i/lub wdrażające ustanowienie zasad postępowania].	

PL-5	**OCENA WPŁYWU NA PRYWATNOŚĆ**
[Zgodnie z Ogólnym Rozporządzeniem o Ochronie Danych Osobowych 2016/679 (RODO)].	

PL-6	**PLANOWANIE DZIAŁALNOŚCI ZWIĄZANEJ Z BEZPIECZEŃSTWEM**
[Włączone do: PL-2].	

PL-7	**KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH**		
	CEL OCENY: *Określić, czy organizacja:*		
	PL-7(a)	*opracowuje koncepcję bezpieczeństwa działań operacyjnych (CONOPS) systemu informacyjnego zawierającą co najmniej informację, w jaki sposób organizacja zamierza obsługiwać system z punktu widzenia bezpieczeństwa informacji;*	
	PL-7(b)	**PL-7(b)[1]**	*określa częstotliwość przeglądania i aktualizowania CONOPS; oraz*
		PL-7(b)[2]	*opiniuje i aktualizuje CONOPS z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania bezpieczeństwa; procedury związane z tworzeniem CONOPS w zakresie bezpieczeństwa; procedury związane z przeglądam i aktualizacjami CONOPS w zakresie bezpieczeństwa; CONOPS w zakresie bezpieczeństwa systemu informacyjnego; plan bezpieczeństwa systemu informacyjnego; rejestry przeglądów i aktualizacji CONOPS w zakresie bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie i realizację planów bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z opracowaniem, przeglądem i aktualizacją CONOPS w zakresie bezpieczeństwa; zautomatyzowane mechanizmy wspierające i/lub wdrażające opracowanie, przegląd i aktualizację CONOPS w zakresie bezpieczeństwa].		

PL-8	**ARCHITEKTURA BEZPIECZEŃSTWA INFORMACJI**		
	CEL OCENY: *Określić, czy organizacja:*		
	PL-8(a)	*opracowuje architekturę bezpieczeństwa informacji systemu informacyjnego, która:*	
		PL-8(a)(1)	*opisuje ogólną koncepcję, wymagania i podejście, jakie należy przyjąć w odniesieniu do zachowania poufności, integralności i dostępności informacji organizacyjnych;*
		PL-8(a)(2)	*opisuje sposób, w jaki architektura bezpieczeństwa informacji jest zintegrowana ze strukturą organizacyjną i wspiera ją;*
		PL-8(a)(3)	*opisuje wszelkie założenia dotyczące bezpieczeństwa informacji oraz zależności od usług zewnętrznych;*
	PL-8(b)	**PL-8(b)[1]**	*określa częstotliwość przeglądania i aktualizacji architektury bezpieczeństwa informacji;*
		PL-8(b)[2]	*opiniuje i aktualizuje architekturę bezpieczeństwa informacji z częstotliwością określoną przez organizację, w celu odzwierciedlenia aktualności struktury organizacyjnej;*
	PL-8(c)	*zapewnia, że planowane zmiany architektury bezpieczeństwa informacji znajdują odzwierciedlenie w:*	
		PL-8(c)[1]	*planie bezpieczeństwa;*
		PL-8(c)[2]	*koncepcji bezpieczeństwa działań operacyjnych (CONOPS); oraz*
		PL-8(c)[3]	*zamówieniach/zakupach organizacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania bezpieczeństwa; procedury dotyczące rozwoju architektury bezpieczeństwa informacji; procedury dotyczące przeglądów i aktualizacji architektury bezpieczeństwa informacji; dokumentacja architektury korporacyjnej; dokumentacja architektury bezpieczeństwa informacji; plan bezpieczeństwa systemu informacyjnego; bezpieczeństwo działań operacyjnych systemu informacyjnego (CONOPS); rejestry przeglądów i aktualizacji architektury bezpieczeństwa informacji; inne odpowiednie dokumenty lub rejestry].		

PL-8	**ARCHITEKTURA BEZPIECZEŃSTWA INFORMACJI**
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie i realizację planów bezpieczeństwa; personel organizacji odpowiedzialny za rozwój architektury bezpieczeństwa informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z opracowaniem, przeglądem i aktualizacją architektury bezpieczeństwa informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające opracowanie, przegląd i aktualizację architektury bezpieczeństwa informacji].

PL-8(1)	**ARCHITEKTURA BEZPIECZEŃSTWA INFORMACJI | *ZABEZPIECZENIE WIELOSTOPNIOWE (OCHRONA WARSTWOWA)***		
	CEL OCENY: *Określić, czy organizacja:*		
	PL-8(1)(a)	**PL-8(1)(a)[1]**	*definiuje zabezpieczenia, które mają być przypisane do lokalizacji i warstw architektonicznych w ramach projektowania architektury bezpieczeństwa;*
		PL-8(1)(a)[2]	*definiuje lokalizacje i warstwy architektoniczne struktury bezpieczeństwa, w których mają być przypisane określone przez organizację środki bezpieczeństwa;*
		PL-8(1)(a)[3]	*projektuje swoją architekturę bezpieczeństwa z wykorzystaniem zabezpieczenia wielostopniowego (ochrona warstwowa), które przydziela określone przez organizację środki bezpieczeństwa do określonych lokalizacji warstw architektonicznych; oraz*
	PL-8(1)(b)	*projektuje swoją architekturę bezpieczeństwa z wykorzystaniem zabezpieczenia wielostopniowego (ochrona warstwowa), które zapewnia skoordynowane i wzajemnie wzmacniające się działanie przydzielonych zabezpieczeń zdefiniowanych przez organizację.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania bezpieczeństwa; procedury dotyczące wdrożenia architektury bezpieczeństwa informacji; dokumentacja struktury organizacyjnej; dokumentacja architektury bezpieczeństwa informacji; plan bezpieczeństwa systemu informacyjnego; koncepcja bezpieczeństwa działań operacyjnych (CONOPS); inne odpowiednie dokumenty lub rejestry].		

PL-8(1)	**ARCHITEKTURA BEZPIECZEŃSTWA INFORMACJI | *ZABEZPIECZENIE WIELOSTOPNIOWE (OCHRONA WARSTWOWA)***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie i realizację planów bezpieczeństwa; personel organizacji odpowiedzialny za rozwój architektury bezpieczeństwa informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z projektowaniem architektury bezpieczeństwa informacji; zautomatyzowane mechanizmy wspomagające i/lub implementujące projektowanie architektury bezpieczeństwa informacji].

PL-8(2)	**ARCHITEKTURA BEZPIECZEŃSTWA INFORMACJI | *DYWERSYFIKACJA DOSTAWCY***	
	CEL OCENY: *Określić, czy organizacja:*	
	PL-8(2)[1]	*definiuje zabezpieczenia, które mają być przypisane do lokalizacji i warstw architektonicznych w ramach projektowania architektury bezpieczeństwa;*
	PL-8(2)[2]	*definiuje lokalizacje i warstwy architektoniczne swojej architektury bezpieczeństwa, w których mają być przypisane określone przez organizację środki bezpieczeństwa oraz*
	PL-8(2)[3]	*wymaga uzyskania od niezależnych dostawców zdefiniowanych organizacyjnie zabezpieczeń przydzielonych do określonych lokalizacji i warstw architektonicznych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania bezpieczeństwa; procedury dotyczące wdrożenia architektury bezpieczeństwa informacji; dokumentacja struktury organizacyjnej; dokumentacja architektury bezpieczeństwa informacji; plan bezpieczeństwa systemu informacyjnego; koncepcja bezpieczeństwa działań operacyjnych (CONOPS); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie i realizację planów bezpieczeństwa; personel organizacji odpowiedzialny za rozwój architektury bezpieczeństwa informacji; personel organizacji odpowiedzialny za zakupy; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z uzyskiwaniem środków bezpieczeństwa informacji od niezależnych dostawców].	

PL-9	**ZARZĄDZANIE CENTRALNE**	
	CEL OCENY: *Określić, czy organizacja:*	
	PL-9[1]	*definiuje środki bezpieczeństwa i związane z nimi procesy, które mają być zarządzane centralnie; oraz*
	PL-9[2]	*centralnie zarządza zdefiniowanymi w organizacji środkami bezpieczeństwa i związanymi z nimi procesami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka planowania bezpieczeństwa; procedury dotyczące opracowywania i wdrażania planu bezpieczeństwa; plan bezpieczeństwa systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie i realizację planów bezpieczeństwa; personel organizacji odpowiedzialny za planowanie/wdrożenie zarządzania centralnego środków bezpieczeństwa i związanych z nim procesów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące zarządzania centralnego środkami bezpieczeństwa i powiązanym i procesami; zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie centralne środkami bezpieczeństwa i powiązanym i procesami].	

KATEGORIA PM - PROGRAMY BEZPIECZEŃSTWA INFORMACJI

PM-1	**PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI**				
	CEL OCENY: *Ustalić, czy organizacja:*				
	PM-1(a)	*opracowuje i rozpowszechnia w całej organizacji plan programu bezpieczeństwa informacji, który:*			
		PM-1(a**)(1)**	**PM-1(**a**)(1)[1]**	*zawiera przegląd wymagań dotyczących programu bezpieczeństwa;*	
			PM-1(a**)(1)[2]**	*zawiera opis:*	
				PM-1(a**)(1)[2][**a**]**	*zabezpieczeń zarządzania programem bezpieczeństwa, istniejących lub planowanych w celu spełnienia tych wymagań;*
				PM-1(a**)(1)[2][**b**]**	*zabezpieczenia wspólne, stosowane lub planowane, w celu spełnienia tych wymagań;*
		PM-1(a**)(2)**	*obejmuje identyfikację i przypisanie:*		
			PM-1(a**)(2)[1]**	ról;	
			PM-1(a**)(2)[2]**	obowiązków;	
			PM-1(a**)(2)[3]**	zobowiązania w zakresie zarządzania;	
			PM-1(a**)(2)[4]**	koordynacji pomiędzy jednostkami organizacyjnymi;	
			PM-1(a**)(2)[5]**	spójności;	

PM-1	**PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI**		
		PM-1(a)(3)	*odzwierciedla koordynację pomiędzy jednostkami organizacyjnymi odpowiedzialnymi za różne aspekty bezpieczeństwa informacji (tj. techniczne, fizyczne, kadrowe, informacyjne);*
		PM-1(a)(4)	*jest zatwierdzony przez kierownika jednostki organizacyjnej lub osobę przez niego upoważnioną, która odpowiada za ryzyko ponoszone w związku z działalnością organizacji, jej zasobami, osobami fizycznymi i innymi organizacjami;*
	PM-1(b)	**PM-1(b)[1]**	*określa częstotliwość przeglądów planu programu bezpieczeństwa systemu informacyjnego;*
		PM-1(b)[2]	*dokonuje przeglądu planu programu bezpieczeństwa informacji w całej organizacji z częstotliwością określoną przez organizację;*
	PM-1(c)	*uaktualnia plan organizacyjny, w celu uwzględnienia:*	
		PM-1(c)[1]	*zmian zidentyfikowanych podczas realizacji planu;*
		PM-1(c)[2]	*zmian zidentyfikowanych w trakcie oceny środków bezpieczeństwa;*
		PM-1(c)[3]	*problemów zidentyfikowanych w trakcie realizacji planu;*
		PM-1(c)[4]	*problemów zidentyfikowanych w trakcie oceny środków bezpieczeństwa;*
	PM-1(d)	*chroni plan bezpieczeństwa informacji przed nieautoryzowanym:*	
		PM-1(d)[1]	*ujawnieniem; oraz*
		PM-1(d)[2]	*modyfikacją.*

PM-1	**PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; procedury dotyczące opracowywania i realizacji programu planu bezpieczeństwa; procedury dotyczące uzyskiwania opinii o programie planu bezpieczeństwa i jego aktualizacji; procedury dotyczące koordynacji programu planu bezpieczeństwa z odpowiednimi podmiotami; procedury dotyczące zatwierdzania programu planu bezpieczeństwa; rejestry opiniowania programu planu bezpieczeństwa i jego aktualizacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem i realizacją programów bezpieczeństwa informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test:** [*wybierz spośród:* Procesy organizacyjne związane z opracowaniem / przeglądem / aktualizacją / zatwierdzaniem programu planu bezpieczeństwa informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające plan programu bezpieczeństwa informacji.].

PM-2	**OSOBA ODPOWIEDZIALNA ZA BEZPIECZEŃSTWO INFORMACJI (*SENIOR INFORMATION SECURITY OFFICER - SISO*)**	
	CEL OCENY: *Ustalenie, czy organizacja wyznacza osobę odpowiedzialną za bezpieczeństwo informacji (SISO) z misją i zadaniami w zakresie:*	
	PM-2[1]	*koordynowania programu bezpieczeństwa informacji w całej organizacji;*
	PM-2[2]	*opracowania programu zabezpieczeń informacji w całej organizacji;*
	PM-2[3]	*wdrożenia programu bezpieczeństwa informacji w całej organizacji; oraz*
	PM-2[4]	*utrzymywania programu bezpieczeństwa informacji w całej organizacji.*

PM-2	**OSOBA ODPOWIEDZIALNA ZA BEZPIECZEŃSTWO INFORMACJI (*SENIOR INFORMATION SECURITY OFFICER - SISO*)**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; procedury dotyczące opracowywania i realizacji planu programu bezpieczeństwa; procedury dotyczące opinii i aktualizacji planu programu bezpieczeństwa; procedury dotyczące koordynacji planu programu bezpieczeństwa z właściwym i podmiotami; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem i realizacją programów bezpieczeństwa informacji; osoba odpowiedzialna za bezpieczeństwo informacji (SISO); personel organizacji odpowiedzialny za bezpieczeństwo informacji].

PM-3	**ŚRODKI BEZPIECZEŃSTWA INFORMACJI**		
	CEL OCENY: *Ustalić, czy organizacja:*		
	PM-3(a)	**PM-3(**a**)[1]**	*zapewnia, że wszystkie środki i zasoby dotyczące planowania kapitałowego i inwestycji zawierają zasoby niezbędne do wdrożenia planu programu bezpieczeństwa informacji;*
		PM-3(a**)[2]**	*dokumentuje wszystkie wyjątki od tego wymogu;*
	PM-3(b)	*wykorzystuje uzasadnienie biznesowe w celu określenia niezbędnych zasobów;*	
	PM-3(c)	*zapewnia, że zasoby niezbędne do zapewnienia bezpieczeństwa informacji wykonują swoje zadania zgodnie z planem programu bezpieczeństwa informacji.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; uzasadnienia biznesowe dotyczące planowania finansowego i inwestycji kapitałowych; procedury dotyczące planowania finansowego i inwestycji kapitałowych; dokumentacja dotycząca wyjątków od wymogów planowania kapitałowego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie programów bezpieczeństwa informacji; personel organizacji odpowiedzialny za planowanie finansowe i inwestycyjne; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

PM-3	**ŚRODKI BEZPIECZEŃSTWA INFORMACJI**
	Test: [*wybierz spośród:* Procesy organizacyjne planowania finansowego i inwestycji; zautomatyzowane mechanizmy wspomagające planowanie finansowe i proces inwestycyjny].

PM-4	**PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ**		
	CEL OCENY: *Ustalić, czy organizacja:*		
	PM-4(a)	*wdraża proces zapewnienia, że plany działania i etapy wprowadzania (tzw. kamienie milowe) programu bezpieczeństwa i powiązanych systemów informacyjnych organizacji są:*	
		PM-4(a)(1)	**PM-4(a)(1)[1]** *opracowywane;*
			PM-4(a)(1)[2] *utrzymywane;*
		PM-4(a)(2)	*dokumentują działania zaradcze w zakresie bezpieczeństwa informacji, mające na celu odpowiednią reakcję na wystąpienie ryzyka związanego z operacjami organizacyjnymi i aktywami, osobami fizycznymi, innymi organizacjami i organami władzy państwowej;*
		PM-4(a)(3)	*są zgłaszane zgodnie z wymogami sprawozdawczości.*
	PM-4(b)	*aktualizuje plany działania i etapy wprowadzania zabezpieczeń w celu zapewnienia spójności:*	
		PM-4(b)[1]	*ze strategią zarządzania ryzykiem organizacyjnym; oraz*
		PM-4(b)[2]	*z priorytetami całej organizacji w zakresie reagowania na ryzyko.*

PM-4	**PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; plany i główne etapy działania; procedury dotyczące planów działania i głównych etapów rozwoju i utrzymania; procedury dotyczące planów działania i głównych etapów sprawozdawczości; procedury przeglądu planów działania i głównych etapów pod kątem spójności ze strategią zarządzania ryzykiem i priorytetami w zakresie reagowania na ryzyko; wyniki oceny ryzyka związane z planami i głównymi etapami działania; wymogi w zakresie sprawozdawczości; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za opracowanie, utrzymanie, przegląd i raportowanie planów i etapów działania; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test:** [*wybierz spośród:* Procesy organizacyjne związane z planami działania i etapami rozwoju, przeglądami, utrzymaniem, raportowaniem; zautomatyzowane mechanizmy wspierające plany i etapy działania].

PM-5	**INWENTARYZACJA SYSTEMU INFORMACYJNEGO**
	CEL OCENY: *Określić, czy organizacja:*
	PM-5[1] *opracowuje wykaz posiadanych systemów informacyjnych; oraz*
	PM-5[2] *prowadzi inwentaryzację posiadanych systemów informacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; inwentaryzacja systemu informacyjnego; procedury dotyczące opracowywania i utrzymywania inwentaryzacji systemów informacyjnych; wytyczne dotyczące sprawozdawczości; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem i wdrażaniem programów bezpieczeństwa informacji; personel organizacji odpowiedzialny za opracowanie i prowadzenie inwentaryzacji systemu informacyjnego; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z opracowywaniem i utrzymywaniem inwentaryzacji systemów informacyjnych; zautomatyzowane mechanizmy wspomagające inwentaryzację systemów informacyjnych].

PM-6	**SKUTECZNOŚĆ ŚRODKÓW BEZPIECZEŃSTWA INFORMACJI**	
	CEL OCENY: *Określić, czy organizacja:*	
	PM-6[1]	*wdraża skuteczne środki bezpieczeństwa informacji;*
	PM-6[2]	*monitoruje skuteczność środków bezpieczeństwa informacji; oraz*
	PM-6[3]	*raportuje wyniki skuteczności środków bezpieczeństwa informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; skuteczność środków bezpieczeństwa informacji; procedury dotyczące rozwoju, monitorowania i raportowania skuteczności środków bezpieczeństwa informacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem i wdrażaniem programów bezpieczeństwa informacji; personel organizacji odpowiedzialny za opracowywanie, monitorowanie i raportowanie skuteczności środków bezpieczeństwa informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące opracowywania, monitorowania i sprawozdawczości w zakresie skuteczności działania środków bezpieczeństwa informacji; zautomatyzowane mechanizmy wspierające opracowywanie, monitorowanie i sprawozdawczość w zakresie skuteczności działania środków bezpieczeństwa informacji].	

PM-7	**STRUKTURA ORGANIZACYJNA**	
	CEL OCENY: *Określić, czy organizacja opracowuje strukturę organizacyjną z uwzględnieniem:*	
	PM-7[1]	*bezpieczeństwo informacji; oraz*
	PM-7[2]	*ryzyka wynikającego dla działalności organizacji, majątku organizacyjnego, osób fizycznych, innych organizacji i społeczeństwa.*

PM-7	**STRUKTURA ORGANIZACYJNA**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; dokumentacja struktury organizacyjnej; dokumentacja architektury korporacyjnej; procedury dotyczące rozwoju architektury korporacyjnej; wyniki oceny ryzyka architektury korporacyjnej; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za opracowanie programu bezpieczeństwa informacji i realizację planu; personel organizacji odpowiedzialny za rozwój struktury organizacyjnej; personel organizacji odpowiedzialny za szacowanie ryzyka struktury organizacyjnej; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z rozwojem struktury organizacyjnej; zautomatyzowane mechanizmy wspierające strukturę organizacyjną i jej rozwój].

PM-8	**PLAN INFRASTRUKTURY KRYTYCZNEJ**	
	CEL OCENY: *Ustalić, czy organizacja uwzględnia kwestie bezpieczeństwa informacji w zakresie:*	
	PM-8[1]	*opracowywania planu ochrony infrastruktury krytycznej i kluczowych zasobów;*
	PM-8[2]	*opracowywania dokumentacji planu ochrony infrastruktury krytycznej i kluczowych zasobów; oraz*
	PM-8[3]	*aktualizacji planu ochrony infrastruktury krytycznej i kluczowych zasobów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; plan ochrony infrastruktury krytycznej i kluczowych zasobów; procedury dotyczące opracowywania, dokumentowania i aktualizacji planu ochrony infrastruktury krytycznej i kluczowych zasobów; Narodowy Program Ochrony Infrastruktury Krytycznej; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem i wdrażaniem programów bezpieczeństwa informacji; personel organizacji odpowiedzialny za opracowanie, udokumentowanie i aktualizację planu ochrony infrastruktury krytycznej i kluczowych zasobów; personel organizacji odpowiedzialny za bezpieczeństwo informacji].	

PM-8	**PLAN INFRASTRUKTURY KRYTYCZNEJ**
	Test: [*wybierz spośród:* Procesy organizacyjne związane z tworzeniem, dokumentowaniem i aktualizacją planu ochrony infrastruktury krytycznej i kluczowych zasobów; zautomatyzowane mechanizmy wspierające tworzenie, dokumentowanie i aktualizowanie planu ochrony infrastruktury krytycznej i kluczowych zasobów].

PM-9	**STRATEGIA ZARZĄDZANIA RYZYKIEM**		
	CEL OCENY: *Określić, czy organizacja:*		
	PM-9(a)	*opracowuje kompleksową strategię zarządzania ryzykiem operacji organizacyjnych i aktywów, personelu, innych organizacji oraz społeczeństwa, związaną z funkcjonowaniem i korzystaniem z systemów informacyjnych;*	
	PM-9(b)	*wdraża strategię zarządzania ryzykiem w sposób spójny w całej organizacji;*	
	PM-9(c)	**PM-9(c)[1]**	*definiuje częstotliwość przeglądów i aktualizacji strategii zarządzania ryzykiem;*
		PM-9(c)[2]	*dokonuje przeglądu i aktualizacji strategii zarządzania ryzykiem w celu uwzględnienia zmian organizacyjnych:*
			PM-9(c)[2][a] *z częstotliwością określoną przez organizację; lub*
			PM-9(c)[2][b] *w razie potrzeby.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; strategia zarządzania ryzykiem; procedury dotyczące opracowywania, wdrażania, przeglądu i aktualizacji strategii zarządzania ryzykiem; wyniki oceny ryzyka istotne dla strategii zarządzania ryzykiem; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem i wdrażaniem programów bezpieczeństwa informacji; personel organizacji odpowiedzialny za opracowanie, udokumentowanie i aktualizację planu ochrony infrastruktury krytycznej i kluczowych zasobów; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

PM-9	**STRATEGIA ZARZĄDZANIA RYZYKIEM**
	Test: [*wybierz spośród:* Procesy organizacyjne związane z opracowaniem, wdrożeniem, przeglądem i aktualizacją strategii zarządzania ryzykiem; zautomatyzowane mechanizmy wspierające opracowanie, wdrożenie, przegląd i aktualizację strategii zarządzania ryzykiem].

PM-10	**PROCES AUTORYZACJI ZABEZPIECZEŃ**	
	CEL OCENY: *Określić, czy organizacja:*	
	PM-10(a)	*zarządza (tj. dokumentuje, monitoruje i raportuje) stanem bezpieczeństwa systemów informacyjnych organizacji oraz środowisk, w których systemy te działają, wykorzystując proces autoryzacji zabezpieczeń;*
	PM-10(b)	*wyznacza osoby do pełnienia określonych ról i obowiązków w ramach procesu zarządzania ryzykiem organizacyjnym; oraz*
	PM-10(c)	*w sposób kompleksowy integruje proces autoryzacji zabezpieczeń z programem zarządzania ryzykiem w całej organizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; procedury dotyczące zarządzania (tj. dokumentowanie, monitorowanie i raportowanie) procesem autoryzacji bezpieczeństwa; dokumenty autoryzacji bezpieczeństwa; listy lub inna dokumentacja dotycząca ról i obowiązków w procesie autoryzacji bezpieczeństwa; wyniki oceny ryzyka istotne dla procesu autoryzacji bezpieczeństwa i programu zarządzania ryzykiem w całej organizacji; strategia zarządzania ryzykiem w organizacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem i realizacją programów bezpieczeństwa informacji; personel organizacji odpowiedzialny za zarządzanie procesem autoryzacji bezpieczeństwa; osoby autoryzujące; właściciele systemów, SISO; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne autoryzacji bezpieczeństwa; zautomatyzowane mechanizmy wspierające proces autoryzacji bezpieczeństwa].	

PM-11	**DEFINICJA MISJI / PROCESU BIZNESOWEGO**		
	CEL OCENY: *Określić, czy organizacja:*		
	PM-11(a)	*definiuje misję/procesy biznesowe z uwzględnieniem bezpieczeństwa informacji i wynikającego z tego ryzyka dla operacji organizacyjnych, majątku organizacyjnego, osób, innych organizacji i społeczeństwa;*	
	PM-11(b)	**PM-11(b)[1]**	*określa potrzeby w zakresie ochrony informacji wynikające z określonej misji/procesu biznesowego; oraz*
		PM-11(b)[2]	*weryfikuje procesy w miarę potrzeb do momentu uzyskania możliwych do osiągnięcia potrzeb w zakresie ochrony.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; strategia zarządzania ryzykiem; procedury określania potrzeb w zakresie ochrony misji/ochrony działalności gospodarczej; wyniki oceny ryzyka istotne dla określenia potrzeb w zakresie ochrony misji/ochrony działalności gospodarczej; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie i realizację programów bezpieczeństwa informacji; personel organizacji odpowiedzialny za procesy misyjne/biznesowe; personel organizacji odpowiedzialny za określanie wymagań w zakresie ochrony informacji związanych z procesami misyjnymi/biznesowymi; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące definiowaniu procesów misyjnych/biznesowych i ich potrzeb w zakresie ochrony informacji].		

PM-12	**ZAGROŻENIA WEWNĘTRZNE**
	CEL OCENY: *Ustalenie, czy organizacja wdraża program dotyczący zagrożeń wewnętrznych, który obejmuje interdyscyplinarny zespół zajmujący się incydentami związanymi z zagrożeniami wewnętrznymi.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; dokumentacja programu przeciwdziałania zagrożeniom wewnętrznym; procedury dotyczące programu przeciwdziałania zagrożeniom wewnętrznym; wyniki oceny ryzyka związane z zagrożeniami wewnętrznymi; lista lub inna dokumentacja

PM-12	ZAGROŻENIA WEWNĘTRZNE
	dotycząca interdyscyplinarnego zespołu zajmującego się zagrożeniami wewnętrznymi; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem i realizacją programów bezpieczeństwa informacji; personel organizacji odpowiedzialny za program przeciwdziałania zagrożeniom wewnętrznym; członkowie interdyscyplinarnego zespołu ds. przeciwdziałania zagrożeniom wewnętrznym; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z wdrażaniem programu przeciwdziałania zagrożeniom wewnętrznym oraz interdyscyplinarnego zespołu ds. przeciwdziałania zagrożeniom wewnętrznym; zautomatyzowane mechanizmy wspierające i/lub wdrażające program przeciwdziałania zagrożeniom wewnętrznym oraz interdyscyplinarny zespół ds. obsługi incydentów wewnętrznych].

PM-13	PERSONEL BEZPIECZEŃSTWA INFORMACJI
	CEL OCENY: *Ustalenie, czy organizacja ustanawia program rozwoju i doskonalenia personelu bezpieczeństwa informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; dokumentacja programu rozwoju i doskonalenia personelu bezpieczeństwa informacji; procedury dotyczące programu rozwoju i doskonalenia personelu bezpieczeństwa informacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem i wdrażaniem programów bezpieczeństwa informacji; personel organizacji odpowiedzialny za program rozwoju i doskonalenia personelu bezpieczeństwa informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące wdrażania programu rozwoju i doskonalenia personelu bezpieczeństwa informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające program rozwoju i doskonalenia personelu bezpieczeństwa informacji].

<table>
<tr><th colspan="5">PM-14 TESTOWANIE, SZKOLENIA I MONITOROWANIE</th></tr>
<tr><td></td><td colspan="4">CEL OCENY:
Określić, czy organizacja:</td></tr>
<tr><td></td><td>PM-14(a)</td><td colspan="3">wdraża proces zapewniający, że plany organizacyjne dotyczące przeprowadzania testów bezpieczeństwa, szkoleń i monitorowania działań związanych z systemami informacyjnymi organizacji:</td></tr>
<tr><td></td><td></td><td>PM-14(a)(1)</td><td>PM-14(a)(1)[1]</td><td>są opracowywane;</td></tr>
<tr><td></td><td></td><td></td><td>PM-14(a)(1)[2]</td><td>są utrzymywane;</td></tr>
<tr><td></td><td></td><td>PM-14(a)(2)</td><td colspan="2">wykonywane w odpowiednim czasie;</td></tr>
<tr><td></td><td>PM-14(b)</td><td colspan="3">przegląda plany testowania, szkolenia i monitorowania pod kątem zgodności:</td></tr>
<tr><td></td><td></td><td>PM-14(b)[1]</td><td colspan="2">ze strategią zarządzania ryzykiem organizacji; oraz</td></tr>
<tr><td></td><td></td><td>PM-14(b)[2]</td><td colspan="2">z ogólnym i priorytetami organizacji w zakresie działań związanych z reagowaniem na ryzyko.</td></tr>
<tr><td></td><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Plan programu bezpieczeństwa informacji; plany przeprowadzania testów bezpieczeństwa, szkoleń i działań monitorujących; procedury organizacyjne związane z opracowaniem i utrzymaniem planów przeprowadzania testów bezpieczeństwa, szkoleń i działań monitorujących; strategia zarządzania ryzykiem; procedury przeglądu planów przeprowadzania testów bezpieczeństwa, szkoleń i działań monitorujących pod kątem zgodności ze strategią zarządzania ryzykiem i priorytetami reakcji na ryzyko; wyniki oceny ryzyka związanego z przeprowadzaniem testów bezpieczeństwa, szkoleń i działań monitorujących; ewidencja terminowości realizacji planów przeprowadzania testów bezpieczeństwa, szkoleń i działań monitorujących; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za opracowanie i utrzymanie planów przeprowadzania testów bezpieczeństwa, szkoleń i działań monitorujących; personel organizacji odpowiedzialny za bezpieczeństwo informacji].
Test: [wybierz spośród: Procesy organizacyjne tworzenia i utrzymywania planów przeprowadzania testów bezpieczeństwa, szkoleń i działań monitorujących; zautomatyzowane mechanizmy wspomagające tworzenie i utrzymywanie planów przeprowadzania testów bezpieczeństwa, szkoleń i działań monitorujących].</td></tr>
</table>

PM-15	**KONTAKTY Z GRUPAMI I STOWARZYSZENIAMI ZAJMUJĄCYMI SIĘ BEZPIECZEŃSTWEM INFORMACJI**	
	CEL OCENY: *Ustalić, czy organizacja nawiązuje i ustanawia kontakty z wybranymi grupami i stowarzyszeniami ze środowiska bezpieczeństwa, w celu:*	
	PM-15(a)	*umożliwienie stałej edukacji szkoleń z zakresu bezpieczeństwa personelu organizacyjnego;*
	PM-15(b)	*utrzymywania bieżącej pomocy w zakresie zalecanych praktyk, techniki technologii bezpieczeństwa; oraz*
	PM-15(c)	*udostępniania bieżących informacji związanych z bezpieczeństwem, w tym informacji o zagrożeniach, podatnościach i incydentach.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; strategia zarządzania ryzykiem; procedury dotyczące kontaktów z grupami stowarzyszeniami bezpieczeństwa; potwierdzenia ustalonych i sformalizowanych kontaktów z grupami stowarzyszeniami bezpieczeństwa; wykazy lub inna dokumentacja dotycząca kontaktów z grupami i stowarzyszeniami bezpieczeństwa i/lub członkostwa w nich; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie i wdrażanie programów bezpieczeństwa informacji; personel organizacji odpowiedzialny za nawiązywanie i ustanawianie kontaktów z grupami i stowarzyszeniami bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel z wybranych grup i stowarzyszeń, z którymi organizacja nawiązała i ustanowiła kontakt]. **Test**: [*wybierz spośród:* Procesy organizacyjne nawiązywania i ustanawiania kontaktów z grupami stowarzyszeniami bezpieczeństwa; zautomatyzowane mechanizmy wspierające kontakty z grupami stowarzyszeniami bezpieczeństwa].	

PM-16	**OSTRZEGANIE O ZAGROŻENIACH**
	CEL OCENY: *Określić, czy organizacja wdraża ostrzeganie o zagrożeniach, które obejmuje możliwość wymiany informacji pomiędzy różnymi organizacjami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Plan programu bezpieczeństwa informacji; dokumentacja ostrzegania o zagrożeniach; procedury ostrzegania o zagrożeniach; wyniki oceny ryzyka istotne z punktu widzenia świadomości zagrożeń; wykaz lub

PM-16	**OSTRZEGANIE O ZAGROŻENIACH**
	inna dokumentacja dotycząca możliwości wymiany informacji w ramach różnych organizacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za planowanie i realizację programu bezpieczeństwa informacji; personel organizacji odpowiedzialny za program świadomości zagrożeń; personel organizacji odpowiedzialny za współdzielenie informacji między organizacjami; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel, z którym organizacja wymienia informacje o zagrożeniach]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące wdrożeniu programu zwiększania świadomości zagrożeń; procesy organizacyjne służące wdrożeniu Zdolności w zakresie wymiany informacji pomiędzy poszczególnym i organizacjami; zautomatyzowane mechanizmy wspierające i/lub wdrażające program zwiększania świadomości zagrożeń; zautomatyzowane mechanizmy wspierające i/lub wdrażające zdolność w zakresie wymiany informacji pomiędzy poszczególnym i organizacjami.].

KATEGORIA PS - BEZPIECZEŃSTWO OSOBOWE

PS-1	**BEZPIECZEŃSTWO OSOBOWE – POLITYKA I PROCEDURY**			
	CEL OCENY: *Określić, czy organizacja:*			
	PS-1(a)(1)	**PS-1(a)(1)[1]**	*opracowuje i dokumentuje politykę bezpieczeństwa personelu, która dotyczy:*	
			PS-1(a)(1)[1][a]	*celu;*
			PS-1(a)(1)[1][b]	*zakresu stosowania;*
			PS-1(a)(1)[1][c]	*ról;*
			PS-1(a)(1)[1][d]	*odpowiedzialności;*
			PS-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			PS-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			PS-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		PS-1(a)(1)[2]	*określa personel lub role, wśród których ma być rozpowszechniana polityka bezpieczeństwa personelu;*	
		PS-1(a)(1)[3]	*rozpowszechnia politykę bezpieczeństwa personelu wśród personelu lub ról określonych przez organizację;*	
	PS-1(a)(2)	**PS-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrażanie polityki bezpieczeństwa personelu i powiązanych środków bezpieczeństwa;*	
		PS-1(a)(2)[2]	*określa personel lub role, wśród których procedury mają być rozpowszechniane;*	
		PS-1(a)(2)[3]	*rozpowszechnia procedury wśród personelu lub ról określonych przez organizację;*	
	PS-1(b)(1)	**PS-1(b)(1)[1]**	*określa częstotliwość przeglądów i aktualizacji aktualnej polityki bezpieczeństwa personelu;*	
		PS-1(b)(1)[2]	*opiniuje i aktualizuje aktualną politykę bezpieczeństwa personelu z częstotliwością określoną przez organizację;*	

PS-1	**BEZPIECZEŃSTWO OSOBOWE – POLITYKA I PROCEDURY**		
	PS-1(b)(2)	**PS-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji aktualnej polityki bezpieczeństwa personelu; oraz*
		PS-1(b)(2)[2]	*opiniuje i aktualizuje aktualne procedury bezpieczeństwa personelu z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury w zakresie bezpieczeństwa osobowego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji z obowiązkami w zakresie kontroli dostępu; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

PS-2	**OKREŚLANIE RYZYKA DLA STANOWISKA PRACY**		
	CEL OCENY: *Określić, czy organizacja:*		
	PS-2(a)	*szacuje ryzyko utraty bezpieczeństwa informacji w odniesieniu do wszystkich stanowisk do w organizacji;*	
	PS-2(b)	*ustanawia kryteria selekcji osób zajmujących te stanowiska;*	
	PS-2(c)	**PS-2(c)[1]**	*określa częstotliwość przeglądów i aktualizacji oznaczeń ryzyka pozycji; oraz*
		PS-2(c)[2]	*przegląda i aktualizuje oszacowane ryzyko danego stanowiska z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury dotyczące kategoryzacji stanowisk; odpowiednie przepisy; lista klasyfikacji ryzyka dla stanowisk organizacyjnych; plan bezpieczeństwa; zapisy przeglądów i aktualizacji klasyfikacji ryzyka dla stanowisk; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

PS-2	**OKREŚLANIE RYZYKA DLA STANOWISKA PRACY**
	Test: [*wybierz spośród:* Procesy organizacyjne związane z przypisywaniem, przeglądem i aktualizacją oznaczeń ryzyka stanowiska; procesy organizacyjne związane z ustalaniem kryteriów oceny].

PS-3	**DOBÓR PERSONELU**		
	CEL OCENY: *Określić, czy organizacja:*		
	PS-3(a)	*sprawdza osoby przed autoryzowaniem dostępu do systemu informacyjnego;*	
	PS-3(b)	**PS-3(b)[1]**	*definiuje warunki wymagające ponownego przeprowadzenia przeglądu;*
		PS-3(b)[2]	*definiuje częstotliwość powtórnego przeglądu, jeśli jest on wskazany; oraz*
		PS-3(b)[3]	*dokonuje ponownego przeglądu osób zgodnie z warunkami zdefiniowanymi przez organizację, które wymagają ponownego przeglądu, oraz, jeżeli taki przegląd jest wskazany, z określoną przez organizację częstotliwością dokonywania ponownego przeglądu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury dotyczące doboru personelu; rejestry personelu poddanego procedurze bezpieczeństwa osobowego; plan bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne doboru personelu].		

PS-3(1)	**DOBÓR PERSONELU | *INFORMACJE NIEJAWNE***	
	CEL OCENY: *Określić, czy organizacja:*	
	PS-3(1)[1]	*zapewnia, że osoby mające dostęp do systemu informacyjnego przetwarzające, przechowujące lub przekazujące informacje niejawne są sprawdzone do najwyższej klauzuli informacji, do których mają dostęp w systemie; oraz*
	PS-3(1)[2]	*zapewnia, żeby osoby uzyskujące dostęp do systemu informacyjnego przetwarzającego, przechowującego lub przesyłającego informacje niejawne posiadały poświadczenia bezpieczeństwa do najwyższego poziomu klasyfikacji informacji, do których mają dostęp w systemie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury dotyczące doboru personelu; rejestry personelu poddanego procedurze bezpieczeństwa osobowego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne sprawdzeń osobowych i uzyskiwania poświadczeń bezpieczeństwa w zakresie dostępu do informacji niejawnych].	

PS-3(2)	**DOBÓR PERSONELU | *POSTĘPOWANIA SPRAWDZAJĄCE***
	CEL OCENY: *Ustalenie, czy organizacja zapewnia, że osoby uzyskujące dostęp do systemu informacyjnego przetwarzającego, przechowującego lub przekazującego informacje niejawne, podlegały, zgodnie z ustawą o ochronie informacji niejawnych, stosownemu postępowaniu sprawdzającemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury dotyczące doboru personelu; rejestry personelu poddanego procedurze bezpieczeństwa osobowego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne postępowania sprawdzającego dla wszystkich rodzajów informacji, do których personel ma dostęp].

PS-3(3)	**DOBÓR PERSONELU | *INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY***		
	CEL OCENY: *Określić, czy organizacja:*		
	PS-3(3)(a)	*zapewnia, aby osoby mające dostęp do systemu informacyjnego przetwarzającego, przechowującego lub przekazującego informacje wymagające szczególnej ochrony posiadały ważne upoważnienie do dostępu, czego potwierdzeniem są przydzielone im obowiązki służbowe;*	
	PS-3(3)(b)	**PS-3(3)(b)[1]**	*określa dodatkowe kryteria doboru personelu, które muszą być spełnione przez osoby mające dostęp do systemu informacyjnego przetwarzającego, przechowującego lub przekazującego informacje wymagające szczególnej ochrony; oraz*
		PS-3(3)(b)[2]	*zapewnia, że osoby mające dostęp do systemu informacyjnego przetwarzającego, przechowującego lub przekazującego informacje wymagające specjalnej ochrony spełniają określone przez organizację dodatkowe kryteria doboru personelu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; zasady kontroli dostępu, procedury dotyczące doboru personelu; zapisy dotyczące personelu poddanego procedurze sprawdzenia bezpieczeństwa osobowego; kryteria sprawdzania; zapisy dotyczące upoważnienia do dostępu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne zapewniające aktualne upoważnienia dostępu do informacji wymagających szczególnej ochrony; proces organizacyjny dodatkowego doboru personelu do udzielenia dostępu do informacji wymagających szczególnej ochrony].		

PS-4	**ZAKOŃCZENIE ZATRUDNIENIA**		
	CEL OCENY: *Ustalić, czy organizacja, po zakończeniu indywidualnego zatrudnienia:*		
	PS-4(a)	**PS-4(a)[1]**	*określa okres czasu, w którym można wyłączyć dostęp do systemu informacyjnego;*

PS-4	**ZAKOŃCZENIE ZATRUDNIENIA**		
		PS-4(a)[2]	*wyłącza dostęp do systemu informacyjnego w określonym przez organizację okresie czasu;*
	PS-4(b)	*kończy / odwołuje wszelkie dokumenty uwierzytelniające / pełnomocnictwa związane z daną osobą;*	
	PS-4(c)	**PS-4(c)[1]**	*określa tematy związane z bezpieczeństwem informacji, które należy omówić podczas przeprowadzania wywiadów końcowych;*
		PS-4(c)[2]	*przeprowadza rozmowy końcowe, które obejmują dyskusję na tematy związane z bezpieczeństwem informacji określone przez organizację;*
	PS-4(d)	*odbiera wszystkie związane z bezpieczeństwem aktywa/pasywa systemu informacyjnego organizacji;*	
	PS-4(e)	*zachowuje dostęp do informacji organizacyjnych i systemów informacyjnych kontrolowanych wcześniej przez osobę zlikwidowaną;*	
	PS-4(f)	**PS-4(f)[1]**	*określa personel lub role, które należy powiadomić o rozwiązaniu umowy ze zwalnianą osobą;*
		PS-4(f)[2]	*określa okres czasu, w którym należy powiadomić personel lub role określone przez organizację; oraz*
		PS-4(f)[3]	*powiadamia określony przez organizację personel lub role w określonym przez nią okresie czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury dotyczące zakończenia zatrudnienia; rejestry działań związanych z zakończeniem zatrudnienia; wykaz kont systemu informacyjnego; rejestry zakończonych lub unieważnionych autoryzacji/dokumentów uwierzytelniających; rejestry przeprowadzonych rozmów końcowych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* procesy organizacyjne związane z rozwiązywaniem umów o pracę/współpracę; zautomatyzowane mechanizmy obsługi i/lub wdrażania powiadomień o rozwiązaniu umowy o pracę/współpracę; zautomatyzowane mechanizmy wyłączania dostępu do systemu informacyjnego/cofania autoryzacji].		

PS-4(1)	**ZAKOŃCZENIE ZATRUDNIENIA | *ZOBOWIĄZANIA PO ZAKOŃCZENIU ZATRUDNIENIU***	
	CEL OCENY: *Określić, czy organizacja:*	
	PS-4(1)(a)	*powiadamia zwalniane osoby o obowiązujących w zakresie ochrony informacji organizacyjnych prawnie wiążących wymaganiach po okresie zatrudnienia; oraz*
	PS-4(1)(b)	*wymaga podpisania przez zwalniane osoby oświadczenie w zakresie zachowania tajemnicy organizacji po okresie zatrudnienia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury kadrowe dotyczące zwalniania osób; podpisane przez pracownika formularze potwierdzenia odbioru dokumentów po okresie zatrudnienia; wykaz obowiązujących, prawnie wiążących wymogów po okresie zatrudnienia; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące obowiązków osób po okresie zatrudnienia].	

PS-4(2)	**ZAKOŃCZENIE ZATRUDNIENIA | *AUTOMATYCZNE POWIADAMIANIE***	
	CEL OCENY: *Określić, czy organizacja:*	
	PS-4(2)[1]	*określa personel lub role, które należy powiadomić po zakończeniu zatrudnienia danej osoby; oraz*
	PS-4(2)[2]	*stosuje zautomatyzowane mechanizmy powiadamiania zdefiniowanego przez organizację personelu lub ról po zakończeniu zatrudnienia danej osoby.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury kadrowe dotyczące zwalniania osób; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry czynności związanych z zakończeniem stosunku pracy	

PS-4(2)	**ZAKOŃCZENIE ZATRUDNIENIA | *AUTOMATYCZNE POWIADAMIANIE***
	z pracownikami; automatyczne powiadomienia o rozwiązaniu stosunku pracy z pracownikami; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z rozwiązaniem stosunku pracy; zautomatyzowane mechanizmy wspierające i/lub wdrażające powiadomienia o rozwiązaniu stosunku pracy z personelem].

PS-5	**OBSADZENIE LUB PRZENIESIENIE STANOWISKA**		
	CEL OCENY: *Określić, czy organizacja:*		
	PS-5(a)	*w przypadku zmiany przydziału lub przeniesienia osób na inne stanowiska w organizacji, sprawdza i potwierdza aktualne potrzeby operacyjne:*	
		PS-5(a)[1]	*logiczne upoważnienia dostępu do systemów informacyjnych;*
		PS-5(a)[2]	*zezwolenie na dostęp fizyczny do systemów i urządzeń informacyjnych;*
	PS-5(b)	**PS-5(b)[1]**	*definiuje działania związane z przeniesieniem lub zmianą stanowiska, które mają być zainicjowane po przeniesieniu lub zmianie miejsca przydziału;*
		PS-5(b)[2]	*definiuje okres czasu, w którym po przeniesieniu lub zmianie stanowiska powinny nastąpić działania związane z przeniesieniem lub zmianą stanowiska;*
		PS-5(b)[3]	*inicjuje zdefiniowane przez organizację działania przeniesienia lub zmiany stanowiska w określonym przez organizację okresie czasu następującym po przeniesieniu lub zmianie przydziału;*
	PS-5(c)	*modyfikuje uprawnienia dostępu w zależności od potrzeb, tak, aby odpowiadały one wszelkim zmianom w zakresie potrzeb operacyjnych wynikających ze zmiany stanowiska lub przeniesienia;*	
	PS-5(d)	**PS-5(d)[1]**	*określa personel lub role, które należy powiadomić w przypadku zmiany przydziału lub przeniesienia osób na inne stanowiska w organizacji;*

PS-5	**OBSADZENIE LUB PRZENIESIENIE STANOWISKA**		
		PS-5(d)[2]	*definiuje okres czasu, w którym należy powiadomić o zmianie przydziału lub przeniesieniu osób na inne stanowiska w organizacji; oraz*
		PS-5(d)[3]	*powiadamia określony przez organizację personel lub role w ramach określonego przez organizację okresie czasu o zmianie przydziału lub przeniesieniu osób na inne stanowiska w organizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury kadrowe dotyczące obsadzenia lub zmiany stanowiska; plan bezpieczeństwa; rejestry działań związanych z przeniesieniem personelu; wykaz upoważnień dostępu do systemu informacyjnego i obiektu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji odpowiedzialny za zarządzanie kontami; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z przeniesieniem personelu; zautomatyzowane mechanizmy wspierające i/lub wdrażające powiadomienia o przeniesieniu personelu; zautomatyzowane mechanizmy wyłączania dostępu do systemu informacyjnego/cofnięcia autoryzacji].		

PS-6	**UMOWY DOSTĘPU / WSPÓŁPRACY**		
	CEL OCENY: *Określić, czy organizacja:*		
	PS-6(a)	*opracowuje i dokumentuje umowy o dostępie do organizacyjnych systemów informacyjnych;*	
	PS-6(b)	**PS-6(b)[1]**	*określa częstotliwość przeglądów i aktualizacji umów o dostępie;*
		PS-6(b)[2]	*opiniuje i aktualizuje umowy o dostępie z częstotliwością określoną przez organizację;*
	PS-6(c)	**PS-6(c)(1)**	*zapewnia, że osoby wymagające dostępu do informacji organizacyjnych i systemów informacyjnych podpisują odpowiednie umowy o dostępie przed uzyskaniem dostępu;*

PS-6	**UMOWY DOSTĘPU / WSPÓŁPRACY**			
		PS-6(c)(2)	**PS-6(c)(2)[1]**	*określa częstotliwość ponownego podpisywania umów o dostępie w celu zachowania dostępu do systemów informacyjnych organizacji po aktualizacji umów o dostępie;*
			PS-6(c)(2)[2]	*zapewnia, że osoby wymagające dostępu do informacji organizacyjnych i systemów informacyjnych ponownie podpisują umowy o dostępie w celu zachowania dostępu do systemów informacyjnych organizacji, po aktualizacji umów o dostępie lub z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury dotyczące umów o dostępie do informacji organizacyjnych i systemów informacyjnych; plan bezpieczeństwa; umowy o dostępie; rejestry przeglądów i aktualizacji umów o dostępie; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; wykaz personelu organizacyjnego, który podpisał/odwołał umowy o dostępie; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące umów o dostępie; zautomatyzowane mechanizmy wspierające umowy o dostępie].			

PS-6(1)	**UMOWY DOSTĘPU / WSPÓŁPRACY | *INFORMACJE WYMAGAJĄCE SPECJALNEJ OCHRONY***
[Włączone do: PS-3].	

PS-6(2)	**UMOWY DOSTĘPU / WSPÓŁPRACY | *INFORMACJE NIEJAWNE WYMAGAJĄCE OCHRONY SPECJALNEJ***
	CEL OCENY: *Ustalić, czy organizacja zapewnia dostęp do informacji niejawnych wymagających ochrony specjalnej tylko osobom, które:*

PS-6(2)	**UMOWY DOSTĘPU / WSPÓŁPRACY | *INFORMACJE NIEJAWNE WYMAGAJĄCE OCHRONY SPECJALNEJ***	
	PS-6(2)(a)	*posiadają aktualne poświadczenia bezpieczeństwa, wydane przez krajową władzę bezpieczeństwa, czego dowodami są przydzielone im oficjalne obowiązki służbowe;*
	PS-6(2)(b)	*spełniają kryteria bezpieczeństwa osobowego; oraz*
	PS-6(2)(c)	*przeczytali, zrozumieli i podpisali umowę o zachowaniu poufności.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury dotyczące umów o dostępie do informacji organizacyjnych i systemów informacyjnych; umowy/porozumienia o dostępie; upoważnienia dostępu; kryteria bezpieczeństwa osobowego; podpisane umowy/porozumienia o poufności; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji, który podpisał umowy/porozumienia o poufności; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące dostępu do informacji niejawnych wymagających ochrony specjalnej].	

PS-6(3)	**UMOWY DOSTĘPU / WSPÓŁPRACY | *WYMOGI PO ZAKOŃCZENIU ZATRUDNIENIU***	
	CEL OCENY: *Określić, czy organizacja:*	
	PS-6(3)(a)	*powiadamia osoby o obowiązujących po okresie zatrudnienia, prawnie wiążących wymaganiach zachowania tajemnicy informacji organizacyjnych; oraz*
	PS-6(3)(b)	*wymaga od osób podpisania oświadczeniu o zachowaniu tajemnicy informacji organizacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury dotyczące umów o dostępie do informacji organizacyjnych i systemów informacyjnych; podpisane formularze potwierdzenia zakończenia zatrudnienia; umowy/porozumienia o dostępie; wykaz mających zastosowanie, prawnie wiążących wymogów po zakończeniu zatrudnienia; inne odpowiednie dokumenty lub rejestry].	

PS-6(3)	**UMOWY DOSTĘPU / WSPÓŁPRACY | *WYMOGI PO ZAKOŃCZENIU ZATRUDNIENIU***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji, który podpisał umowy o dostępie określające zobowiązania po zakończeniu zatrudnienia; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące spełniania wymogów po zakończeniu zatrudnienia; zautomatyzowane mechanizmy wspierające powiadamianie I indywidualne potwierdzanie spełniania zobowiązań po zakończeniu zatrudnienia].

PS-7	**BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH**		
	CEL OCENY: *Określić, czy organizacja:*		
	PS-7(a)	*ustanawia wymagania dotyczące bezpieczeństwa osobowego, w tym ról i obowiązków w zakresie bezpieczeństwa, dotyczące dostawców zewnętrznych;*	
	PS-7(b)	*wymaga, aby dostawcy zewnętrzni przestrzegali zasad i procedur bezpieczeństwa osobowego ustanowionych przez organizację;*	
	PS-7(c)	*dokumentuje wymagania w zakresie bezpieczeństwa osobowego;*	
	PS-7(d)	**PS-7(d)[1]**	*definiuje personel lub role, które powinny być powiadamiane o wszelkich przeniesieniach lub zakończeniu pracy personelu zewnętrznego, który posiada poświadczenia i/lub identyfikatory organizacyjne, lub który posiada uprawnienia do korzystania z systemu informacyjnego;*
		PS-7(d)[2]	*definiuje okres czasu, w którym zewnętrzni dostawcy usług są zobowiązani do powiadamiania o wszelkich przeniesieniach lub zwolnieniach personelu lub ról zdefiniowanych przez organizację, którzy posiadają poświadczenia i/lub identyfikatory organizacyjne, lub którzy mają uprawnienia do korzystania z systemu informacyjnego;*

PS-7	**BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH**		
		PS-7(d)[3]	*wymaga od zewnętrznych dostawców usług, informowania określonego przez organizację personelu lub ról w ramach określonego przez organizację okresu czasu, o wszelkich przeniesieniach lub zwolnieniach personelu zewnętrznego posiadającego poświadczenia i/lub identyfikatory organizacyjne lub posiadającego uprawnienia do korzystania z systemu informacyjnego; oraz*
	PS-7(e)	*monitoruje stosowanie przez dostawcę zasad i procedur bezpieczeństwa.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury dotyczące bezpieczeństwa osobowego stron trzecich; wykaz obowiązków w zakresie bezpieczeństwa osobowego; dokumenty zakupów; umowa gwarancji świadczenia usług (SLA); proces stosowanie przez dostawcę zasad i procedur bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; zewnętrzni dostawcy; administratorzy systemu/sieci; personel organizacji odpowiedzialny za zarządzanie kontami; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie zarządzania i monitorowania bezpieczeństwa osobowego stron trzecich; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie zgodności z przepisami przez usługodawcę].		

PS-8	**SANKCJE PERSONALNE**		
	CEL OCENY: *Określić, czy organizacja:*		
	PS-8(a)	*stosuje formalny proces sankcji wobec osób, które nie przestrzegają ustalonych zasad i procedur bezpieczeństwa informacji;*	
	PS-8(b)	**PS-8(b)[1]**	*definiuje personel lub role, które należy powiadomić w przypadku wszczęcia formalnego procesu sankcji pracowniczych;*
		PS-8(b)[2]	*definiuje okres czasu, w którym należy powiadomić określony przez organizację personel lub role, o rozpoczęciu formalnego procesu nakładania sankcji na pracownika; oraz*

PS-8	**SANKCJE PERSONALNE**		
		PS-8(b)[3]	*powiadamia określony przez organizację personel lub role w określonym przez nią okresie czasu, o rozpoczęciu formalnego procesu nakładania sankcji na pracownika, wskazując osobę, na którą nałożono sankcje, oraz powód nałożenia sankcji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka bezpieczeństwa osobowego; procedury dotyczące nakładania sankcji na personel; zasady postępowania; rejestry zastosowanych sankcji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo osobowe; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie zarządzania sankcjami personalnymi; zautomatyzowane mechanizmy wspierające i/lub wdrażające powiadomienia].		

KATEGORIA RA - SZACOWANIE RYZYKA

RA-1	**POLITYKA I PROCEDURY SZACOWANIA RYZYKA**			
	CEL OCENY: *Określić, czy organizacja:*			
	RA-1(a)(1)	**RA-1(a)(1)[1]**	*opracowuje i dokumentuje politykę oceny ryzyka, która dotyczy:*	
			RA-1(a)(1)[1][a]	*celu;*
			RA-1(a)(1)[1][b]	*zakresu stosowania;*
			RA-1(a)(1)[1][c]	*ról;*
			RA-1(a)(1)[1][d]	*odpowiedzialności;*
			RA-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			RA-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			RA-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		RA-1(a)(1)[2]	*określa personel lub role, wśród których ma być rozpowszechniana polityka oceny ryzyka;*	
		RA-1(a)(1)[3]	*rozpowszechnia politykę oceny ryzyka wśród personelu lub ról zdefiniowanych przez organizację;*	
	RA-1(a)(2)	**RA-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrożenie polityki oceny ryzyka i związanych z nią mechanizmów oceny ryzyka;*	
		RA-1(a)(2)[2]	*określa personel lub rolę, wśród których procedury mają być rozpowszechniane;*	
		RA-1(a)(2)[3]	*rozpowszechnia procedury wśród personelu lub ról określonych w organizacji;*	
	RA-1(b)(1)	**RA-1(b)(1)[1]**	*definiuje częstotliwość przeglądów i aktualizacji aktualnej polityki oceny ryzyka;*	
		RA-1(b)(1)[2]	*opiniuje i aktualizuje aktualną politykę oceny ryzyka z częstotliwością określoną przez organizację;*	

RA-1	**POLITYKA I PROCEDURY SZACOWANIA RYZYKA**		
	RA-1(b)(2)	**RA-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji bieżących procedur oceny ryzyka; oraz*
		RA-1(b)(2)[2]	*opiniuje i aktualizuje aktualne procedury oceny ryzyka z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury szacowania ryzyka; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za szacowanie ryzyka; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

RA-2	**KATEGORYZACJA BEZPIECZEŃSTWA**	
	CEL OCENY: *Określić, czy organizacja:*	
	RA-2(a)	*kategoryzuje informacje i system informacyjny zgodnie z obowiązującym prawem, rozporządzeniami wykonawczymi, dyrektywami, politykami, przepisami, normami, standardami i wytycznymi;*
	RA-2(b)	*dokumentuje wyniki kategoryzacji bezpieczeństwa (w tym uzasadnienie) w planie bezpieczeństwa systemu informacyjnego; oraz*
	RA-2(c)	*zapewnienia, że osoba autoryzująca lub wyznaczony przez niego przedstawiciel dokonuje przeglądu i zatwierdza decyzję w sprawie kategoryzacji bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny ryzyka; polityka i procedury planowania bezpieczeństwa; procedury organizacyjne dotyczące kategoryzacji bezpieczeństwa informacji i systemów informacyjnych; plan bezpieczeństwa; dokumentacja kategoryzacji bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za kategoryzację bezpieczeństwa i szacowanie ryzyka; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne kategoryzacji bezpieczeństwa].	

RA-3	**SZACOWANIE RYZYKA**			
	CEL OCENY: *Określić, czy organizacja:*			
	RA-3(a)	*przeprowadza szacowanie ryzyka, w tym prawdopodobieństwa i skali szkód, wynikających z nieuprawnionego dostępu, użytkowania, ujawniania, zakłócania, modyfikacji lub zniszczenia:*		
		RA-3(a)[1]	*systemu informacyjnego;*	
		RA-3(a)[2]	*informacji, które system przetwarza, przechowuje lub przekazuje;*	
	RA-3(b)	**RA-3(b)[1]**	*określa dokument, w którym należy udokumentować wyniki szacowania ryzyka (jeśli nie są one udokumentowane w planie bezpieczeństwa lub raporcie szacowania ryzyka);*	
		RA-3(b)[2]	*dokumentuje wyniki szacowania ryzyka w jednym z poniższych:*	
			RA-3(b)[2][a]	*planie bezpieczeństwa;*
			RA-3(b)[2][b]	*sprawozdaniu z szacowania ryzyka; lub*
			RA-3(b)[2][c]	*dokumencie zdefiniowany przez organizację;*
	RA-3(c)	**RA-3(c)[1]**	*określa częstotliwość weryfikacji wyników szacowania ryzyka;*	
		RA-3(c)[2]	*dokonuje przeglądu wyników szacowania ryzyka z częstotliwością określoną przez organizację;*	
	RA-3(d)	**RA-3(d)[1]**	*definiuje personel lub role, wśród których powinny być rozpowszechniane wyniki szacowania ryzyka;*	
		RA-3(d)[2]	*rozpowszechnia wyniki szacowania ryzyka wśród określonego przez organizację personelu lub ról;*	
	RA-3(e)	**RA-3(e)[1]**	*definiuje częstotliwość aktualizacji wyników szacowania ryzyka;*	
		RA-3(e)[2]	*aktualizuje wyniki szacowania ryzyka:*	
			RA-3(e)[2][a]	*z częstotliwością określoną przez organizację;*

RA-3	**SZACOWANIE RYZYKA**			
			RA-3(e)[2][b]	*w każdym przypadku wystąpienia istotnych zmian w systemie informacyjnym lub środowisku działania (w tym identyfikacji nowych zagrożeń i słabych punktów); oraz*
			RA-3(e)[2][c]	*gdy tylko zaistnieją inne warunki, które mogą mieć wpływ na stan bezpieczeństwa systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny ryzyka; polityka i procedury planowania bezpieczeństwa; procedury organizacyjne dotyczące szacowania ryzyka; plan bezpieczeństwa; szacowanie ryzyka; wyniki szacowania ryzyka; przeglądy szacowania ryzyka; aktualizacje szacowania ryzyka; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za szacowanie ryzyka; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące do szacowania ryzyka; zautomatyzowane mechanizmy wspierające i/lub służące do prowadzenia, dokumentowania, przeglądu, rozpowszechniania i aktualizacji szacowania ryzyka].			

RA-4	**AKTUALIZACJA SZACOWANIA RYZYKA**
[Włączone do: RA-3].	

RA-5	**SKANOWANIE PODATNOŚCI**			
	CEL OCENY: *Określić, czy organizacja:*			
	RA-5(a)	**RA-5(a)[1]**	**RA-5(a)[1][a]**	*określa częstotliwość przeprowadzania skanowania podatności na zagrożenia w systemie informacyjnymi hostowanych aplikacjach; i/lub*
			RA-5(a)[1][b]	*definiuje proces przeprowadzania losowych skanowań luk w systemie informacyjnymi hostowanych aplikacjach;*

RA-5	**SKANOWANIE PODATNOŚCI**			
		RA-5(a)[2]	*zgodnie ze zdefiniowaną przez organizację częstotliwością i/lub zdefiniowanym przez organizację procesem przeprowadzania skanowań losowych, skanuje pod kątem podatności na luki:*	
			RA-5(a)[2][a]	*system informacyjny;*
			RA-5(a)[2][b]	*hostowane aplikacje;*
		RA-5(a)[3]	*po zidentyfikowaniu i zgłoszeniu nowych podatności, które mogą mieć wpływ na system/aplikacje, przeprowadza skanowanie w poszukiwaniu podatności:*	
			RA-5(a)[3][a]	*systemu informacyjnego;*
			RA-5(a)[3][b]	*hostowanych aplikacji;*
	RA-5(b)	*stosuje narzędzia i techniki skanowania podatności, które ułatwiają współdziałanie narzędzi i automatyzują części procesu zarządzania podatnościami, wykorzystując do tego celu standardy:*		
		RA-5(b)(1)	**RA-5(b)(1)[1]**	*wyliczania platform;*
			RA-5(b)(1)[2]	*wykazania błędów w oprogramowaniu;*
			RA-5(b)(1)[3]	*Wyliczania niewłaściwych konfiguracji;*
		RA-5(b)(2)	**RA-5(b)(2)[1]**	*formatowania list kontrolnych;*
			RA-5(b)(2)[2]	*procedur testowania formatowania;*
		RA-5(b)(3)	*pomiaru wpływu podatności;*	
	RA-5(c)	**RA-5(c)[1]**	*analizy raportów ze skanowania podatności;*	
		RA-5(c)[2]	*analizy wyników oceny środków bezpieczeństwa;*	
	RA-5(d)	**RA-5(d)[1]**	*definicji czasu reakcji na usunięcie uzasadnionych podatności zgodnie z organizacyjnym oszacowaniem ryzyka;*	
		RA-5(d)[2]	*usunięcia uzasadnionych podatności w ramach zdefiniowanych przez organizację czasów reakcji zgodnie z organizacyjną oceną ryzyka;*	

RA-5	**SKANOWANIE PODATNOŚCI**		
	RA-5(e)	**RA-5(e)[1]**	*określenia personelu lub ról, którym mają być udostępniane informacje uzyskane w procesie skanowania podatności i oceny środków bezpieczeństwa;*
		RA-5(e)[2]	*dzielenia się informacjami uzyskanymi w ramach procesu skanowania podatności z personelem lub rolami zdefiniowanymi przez organizację w celu wyeliminowania analogicznych podatności w innych systemach informacyjnych (tj. słabości lub braków systemowych); oraz*
		RA-5(e)[3]	*dzielenia się informacjami uzyskanymi z ocen środków bezpieczeństwa, z osobami lub rolami wyznaczonym i przez organizację, w celu wyeliminowania analogicznych słabych punktów w innych systemach informacyjnych (tj. słabych punktów lub braków systemowych).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny ryzyka; procedury dotyczące skanowania podatności; szacowanie ryzyka; plan bezpieczeństwa; raport z oceny bezpieczeństwa; narzędzia do skanowania podatności i związana z nimi dokumentacja konfiguracyjna; wyniki skanowania podatności; rejestry zarządzania łatam i podatnościami; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się oceną ryzyka, oceną środków bezpieczeństwa i skanowaniem podatności; personel organizacji zajmujący się analizą podatności; personel organizacji zajmujący się eliminowaniem podatności; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane ze skanowaniem, analizą, usuwaniem i wymianą informacji o lukach; zautomatyzowane mechanizmy wspierające i/lub wdrażające skanowanie, analizę, usuwanie i wymianę informacji o lukach].		

RA-5(1)	**SKANOWANIE PODATNOŚCI | *AKTUALIZACJA NARZĘDZI***
	CEL OCENY: *Ustalenie, czy organizacja stosuje narzędzia do skanowania podatności, umożliwiające natychmiastową aktualizację luk w systemie informacyjnym, które mają być skanowane.*

RA-5(1)	**SKANOWANIE PODATNOŚCI | *AKTUALIZACJA NARZĘDZI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Procedury dotyczące skanowania podatności; plan bezpieczeństwa; raport z oceny bezpieczeństwa; narzędzia do skanowania podatności i związana z nimi dokumentacja konfiguracyjna; wyniki skanowania podatności; rejestry zarządzania łatam i podatnościami; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za skanowanie podatności na zagrożenia; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane ze skanowaniem podatności; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające skanowanie podatności].

RA-5(2)	**SKANOWANIE PODATNOŚCI | *AKTUALIZACJA CZĘSTOTLIWOŚCI PRZEPROWADZANIA / AKTUALIZACJA PRZED NOWYM SKANOWANIEM / AKTUALIZACJA PO ZIDENTYFIKOWANIU ZAGROŻENIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	RA-5(2)[1]	*definiuje częstotliwość aktualizacji wykrytych podatności systemu informacyjnego;*
	RA-5(2)[2]	*aktualizuje zeskanowane podatności systemu informacyjnego:*
		RA-5(2)[2][a] *z częstotliwością określoną przez organizację; i/lub*
		RA-5(2)[2][b] *przed nowym skanowaniem; i/lub*
		RA-5(2)[2][c] *gdy zostaną zidentyfikowane i zgłoszone nowe podatności.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Procedury dotyczące skanowania podatności; plan bezpieczeństwa; raport z oceny bezpieczeństwa; narzędzia do skanowania podatności i związana z nimi dokumentacja konfiguracyjna; wyniki skanowania podatności; rejestry zarządzania łatam i podatnościami; inne odpowiednie dokumenty lub rejestry].	

RA-5(2)	**SKANOWANIE PODATNOŚCI | *AKTUALIZACJA CZĘSTOTLIWOŚCI PRZEPROWADZANIA / AKTUALIZACJA PRZED NOWYM SKANOWANIEM / AKTUALIZACJA PO ZIDENTYFIKOWANIU ZAGROŻENIA***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za skanowanie podatności na zagrożenia; personel organizacji odpowiedzialny za analizę podatności na zagrożenia; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane ze skanowaniem podatności; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające skanowanie podatności].

RA-5(3)	**SKANOWANIE PODATNOŚCI | *ZAKRES PODATNOŚCI***	
	CEL OCENY: *Ustalić, czy organizacja stosuje procedury skanowania podatności, które mogą zidentyfikować:*	
	RA-5(3)[1]	*zakres podatności (tj. zeskanowane elementy systemu informacyjnego); oraz*
	RA-5(3)[2]	*głębokość podatności (tzn. zweryfikowane podatności).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Procedury dotyczące skanowania podatności; plan bezpieczeństwa; raport z oceny bezpieczeństwa; narzędzia do skanowania podatności i związana z nimi dokumentacja konfiguracyjna; wyniki skanowania podatności; rejestry zarządzania łatam i podatnościami; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za skanowanie podatności na zagrożenia; personel organizacji odpowiedzialny za analizę podatności na zagrożenia; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane ze skanowaniem podatności; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające skanowanie podatności].	

RA-5(4)	**SKANOWANIE PODATNOŚCI | *WYKRYWANIE SKANOWANIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	RA-5(4)[1]	*definiuje działania naprawcze, które należy podjąć, jeżeli informacje o systemie informacyjnym są możliwe do wykrycia przez przeciwników;*
	RA-5(4)[2]	*określa, jakie informacje o systemie informacyjnym mogą zostać wykryte przez przeciwników; oraz*
	RA-5(4)[3]	*następnie podejmuje określone organizacyjnie działania naprawcze.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Procedury dotyczące skanowania podatności; raport z oceny bezpieczeństwa; wyniki testów penetracyjnych; wyniki skanowania podatności; sprawozdanie z szacowania ryzyka; zapisy podjętych działań naprawczych; zapisy dotyczące reagowania na incydenty; zapisy z audytu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się skanowaniem podatności i/lub badaniami penetracyjnymi; personel organizacji odpowiedzialny za analizę podatności na zagrożenia; personel organizacji odpowiedzialny za reagowanie na ryzyko; personel organizacji odpowiedzialny za zarządzanie i reagowanie na incydenty; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące do skanowania podatności; procesy organizacyjne służące do reagowania na ryzyko; procesy organizacyjne służące do zarządzania i reagowania na incydenty; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające skanowanie podatności; zautomatyzowane mechanizmy wspierające i/lub wdrażające reagowanie na ryzyko; zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie incydentami reagowanie na nie].	

RA-5(5)	**SKANOWANIE PODATNOŚCI | *DOSTĘP UPRZYWILEJOWANY***	
	CEL OCENY: *Określić, czy:*	
	RA-5(5)[1]	*organizacja wprowadza autoryzację dostępu uprzywilejowanego do komponentów systemu informacyjnego przeznaczonych do przeprowadzania wybranych działań związanych ze skanowaniem podatności na zagrożenia;*

RA-5(5)	**SKANOWANIE PODATNOŚCI | *DOSTĘP UPRZYWILEJOWANY***	
	RA-5(5)[2]	*organizacja definiuje działania w zakresie skanowania podatności na zagrożenia wybrane do autoryzacji uprzywilejowanego dostępu do zdefiniowanych przez organizację komponentów systemu informacyjnego; oraz*
	RA-5(5)[3]	*system informacyjny wdraża uprawnienia uprzywilejowanego dostępu do zdefiniowanych przez organizację komponentów systemu informacyjnego do przeprowadzania zdefiniowanych przez organizację działań w zakresie skanowania podatności na zagrożenia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny ryzyka; procedury dotyczące skanowania podatności; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista komponentów systemu informacyjnego do skanowania podatności; lista uprawnień dostępu personelu; dane uwierzytelniające; rejestry uprawnień dostępu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za skanowanie podatności na zagrożenia; administratorzy systemu/sieci; personel organizacji odpowiedzialny za kontrolę dostępu do systemu informacyjnego; personel organizacji odpowiedzialny za zarządzanie konfiguracją systemu informacyjnego; deweloperzy systemów; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie skanowania podatności; procesy organizacyjne do kontroli dostępu; zautomatyzowane mechanizmy wspierające i/lub wdrażające kontrolę dostępu; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające skanowanie podatności].	

RA-5(6)	**SKANOWANIE PODATNOŚCI | *AUTOMATYCZNE ANALIZY TRENDÓW***
	CEL OCENY: *Ustalenie, czy organizacja stosuje zautomatyzowane mechanizmy do porównywania wyników skanowania podatności w czasie, w celu określenia trendów w podatnościach systemów informacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny ryzyka; procedury dotyczące skanowania podatności; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik skanowania podatności; wyniki skanowania podatności; inne odpowiednie dokumenty lub rejestry].

RA-5(6)	**SKANOWANIE PODATNOŚCI | *AUTOMATYCZNE ANALIZY TRENDÓW***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za skanowanie podatności na zagrożenia; personel organizacji odpowiedzialny za analizę podatności na zagrożenia; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane ze skanowaniem podatności; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające skanowanie podatności; zautomatyzowane mechanizmy wspierające i/lub wdrażające analizę trendów wyników skanowania podatności na zagrożenia].

RA-5(7)	**SKANOWANIE PODATNOŚCI | *AUTOMATYCZNE WYKRYWANIE I POWIADAMIANIE O NIEAUTORYZOWANYCH KOMPONENTACH***
[Włączone do: CM-8].	

RA-5(8)	**SKANOWANIE PODATNOŚCI | *PRZEGLĄD HISTORYCZNYCH LOGÓW AUDYTU***
	CEL OCENY: *Ustalenie, czy organizacja dokonuje przeglądu historycznych dzienników audytów w celu ustalenia, czy podatność zidentyfikowana w systemie informacyjnym nie została wcześniej wykorzystana.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny ryzyka; procedury dotyczące skanowania podatności; dzienniki audytów; rejestry przeglądów dzienników audytów; wyniki skanowania podatności; rejestry zarządzania łatam i podatnościami; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za skanowanie podatności na zagrożenia; personel organizacji odpowiedzialny za analizę podatności na zagrożenia; personel organizacji odpowiedzialny za przegląd dokumentacji audytowej; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane ze skanowaniem podatności; proces organizacyjny związany z przeglądem dokumentacji audytowej i działaniami zaradczymi; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające skanowanie podatności; zautomatyzowane mechanizmy wspierające i/lub wdrażające przegląd dokumentacji audytowej].

RA-5(9)	**SKANOWANIE PODATNOŚCI | *TESTY PENETRACYJNE I ANALIZY***
[Włączone do: CA-8].	

RA-5(10)	**SKANOWANIE PODATNOŚCI | *KORELACJA SKANOWANYCH DANYCH***
	CEL OCENY: *Ustalenie, czy organizacja koreluje dane wyjściowe z narzędzi do skanowania w poszukiwaniu luk w celu ustalenia obecności wektorów ataku z wieloma podatnościami / wektorami ataku.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka oceny ryzyka; procedury dotyczące skanowania podatności; szacowanie ryzyka; plan bezpieczeństwa; dokumentacja narzędzi i technik skanowania podatności; wyniki skanowania podatności; rejestry zarządzania podatnościami; zapisy z audytu; dzienniki korelacji zdarzenia z podatnością; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za skanowanie podatności na zagrożenia; personel organizacji odpowiedzialny za analizę podatności na zagrożenia; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane ze skanowaniem podatności; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające skanowanie podatności; zautomatyzowane mechanizmy wprowadzające korelację wyników skanowania podatności].

RA-6	**TECHNICZNE ZABEZPIECZENIE PRZED PODGLĄDEM I PODSŁUCHEM**	
	CEL OCENY: *Określić, czy organizacja:*	
	RA-6[1]	*określa lokalizacje, w których należy stosować techniczne zabezpieczenia przed podglądem i podsłuchem;*
	RA-6[2]	*definiuje częstotliwość przeprowadzania badań technicznego zabezpieczenia przed podglądem i podsłuchem;*
	RA-6[3]	*definiuje zdarzenia lub wskaźniki, które w przypadku ich wystąpienia uruchamiają techniczne zabezpieczenie przed podglądem i podsłuchem;*

<table>
<tr><th colspan="2">RA-6</th><th colspan="2">TECHNICZNE ZABEZPIECZENIE PRZED PODGLĄDEM I PODSŁUCHEM</th></tr>
<tr><td></td><td>RA-6[4]</td><td colspan="2">stosuje techniczne zabezpieczenie przed podglądem i podsłuchem w określonych organizacyjnie lokalizacjach:</td></tr>
<tr><td></td><td></td><td>RA-6[4][a]</td><td>z częstotliwością określoną przez organizację; i/lub</td></tr>
<tr><td></td><td></td><td>RA-6[4][b]</td><td>w przypadku wystąpienia zdefiniowanych przez organizację zdarzeń lub czynników.</td></tr>
<tr><td></td><td colspan="3">POTENCJALNE METODY I OBIEKTY OCENY:

Sprawdź: [wybierz spośród: Polityka oceny ryzyka; procedury dotyczące technicznego zabezpieczenia przed podglądem i podsłuchem; plan bezpieczeństwa; zapisy z audytu/zdarzenia; inne odpowiednie dokumenty lub rejestry].

Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za techniczne zabezpieczenia przed podglądem i podsłuchem; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

Test: [wybierz spośród: Procesy organizacyjne dotyczące badań w zakresie technicznego zabezpieczenia przed podglądem i podsłuchem; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające techniczne zabezpieczenia przed podglądem i podsłuchem].</td></tr>
</table>

KATEGORIA SA - NABYWANIE SYSTEMU I USŁUG

SA-1	**POLITYKA I PROCEDURY NABYWANIA SYSTEMU I USŁUG**			
	CEL OCENY: *Określić, czy organizacja:*			
	SA-1(a)(1)	**SA-1(a)(1)[1]**	*opracowuje i dokumentuje politykę i procedury nabywania usług, która dotyczy:*	
			SA-1(a)(1)[1][a]	*celu;*
			SA-1(a)(1)[1][b]	*zakresu stosowania;*
			SA-1(a)(1)[1][c]	*ról;*
			SA-1(a)(1)[1][d]	*odpowiedzialności;*
			SA-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			SA-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			SA-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		SA-1(a)(1)[2]	*określa personel lub role, wśród których polityka nabywania systemów i usług ma być rozpowszechniana;*	
		SA-1(a)(1)[3]	*rozpowszechnia politykę nabywania systemów i usług wśród personelu lub ról zdefiniowanych w organizacji;*	
	SA-1(a)(2)	**SA-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrażanie polityki nabywania systemów i usług oraz związanych z nimi kontroli nabywania systemów i usług;*	
		SA-1(a)(2)[2]	*określa personel lub rolę, wśród których procedury mają być rozpowszechniane;*	
		SA-1(a)(2)[3]	*rozpowszechnia procedury wśród personelu lub ról zdefiniowanych w organizacji;*	
	SA-1(b)(1)	**SA-1(b)(1)[1]**	*definiuje częstotliwość przeglądów i aktualizacji bieżącej polityki nabywania systemów i usług;*	

SA-1	**POLITYKA I PROCEDURY NABYWANIA SYSTEMU I USŁUG**		
		SA-1(b)(1)[2]	*opiniuje i aktualizuje obowiązującą politykę zakupu systemów i usług z częstotliwością określoną przez organizację;*
	SA-1(b)(2)	**SA-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji obowiązującej polityki nabywania systemów i usług; określa częstotliwość przeglądów i aktualizacji obowiązującej polityki nabywania systemów i usług z określoną przez organizację częstotliwością; oraz*
		SA-1(b)(2)[2]	*opiniuje i aktualizuje istniejące systemy i procedury pozyskiwania usług z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury nabywania systemu i usług; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

SA-2	**PRZYDZIAŁ ZASOBÓW**		
	CEL OCENY: *Określić, czy organizacja:*		
	SA-2(a)	*określa wymagania bezpieczeństwa informacji w systemie informacyjnym lub usług systemu informacyjnego w planowaniu misji / procesów biznesowych;*	
	SA-2(b)	*określa, dokumentuje i przydziela zasoby wymagane do ochrony systemu informacyjnego lub usług systemu informacyjnego w ramach procesu planowania i kontroli inwestycji:*	
		SA-2(b)[1]	*określa wymagane zasoby;*
		SA-2(b)[2]	*dokumentuje wymagane zasoby;*
		SA-2(b)[3]	*przydziela wymagane zasoby; oraz*
	SA-2(c)	*ustanawia oddzielne pozycje zamówień dotyczące bezpieczeństwa informacji w dokumentacji programowej i budżetowej organizacji.*	

SA-2	**PRZYDZIAŁ ZASOBÓW**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące przydziału środków na potrzeby bezpieczeństwa informacji; procedury dotyczące planowania finansowego i kontroli inwestycji; dokumentacja organizacyjna dotycząca projektowania i budżetowania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji zajmujący się planowaniem finansowym, kontrolą inwestycji, projektowaniem i budżetowaniem; personel organizacji odpowiedzialny za określenie wymagań bezpieczeństwa informacji w systemach/usługach informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne określające wymogi bezpieczeństwa informacji; procesy organizacyjne planowania inwestycyjnego, projektowe i budżetowania; zautomatyzowane mechanizmy wspierające i/lub wdrażające organizacyjne planowanie inwestycyjne, projektowanie i budżetowanie].

SA-3	**CYKL ŻYCIA SYSTEMU**	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-3(a)	**SA-3(a)[1]** *definiuje cykl życia systemu, uwzględniający kwestie bezpieczeństwa informacji, który ma być wykorzystywany do zarządzania systemem informacyjnym;*
		SA-3(a)[2] *zarządza systemem informacyjnym przy użyciu zdefiniowanego przez organizację cyklu rozwoju systemu;*
	SA-3(b)	*definiuje i dokumentuje role i obowiązki w zakresie bezpieczeństwa informacji w całym cyklu życia systemu;*
	SA-3(c)	*określa osoby pełniące role i obowiązki w zakresie bezpieczeństwa informacji; oraz*
	SA-3(d)	*integruje proces zarządzania ryzykiem w zakresie bezpieczeństwa informacji organizacyjnych z cyklem życia systemu.*

SA-3	**CYKL ŻYCIA SYSTEMU**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące integracji bezpieczeństwa informacji z procesem cyklu życia systemu; dokumentacja cyklu życia systemu informacyjnego; strategia zarządzania ryzykiem związanym z bezpieczeństwem informacji/ dokumentacja programowa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczeństwo informacji i rozwój cyklu życia systemu; personel organizacji odpowiedzialny za zarządzanie ryzykiem związanym z bezpieczeństwem informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące definiowania i dokumentowania SDLC[5]; procesy organizacyjne dotyczące identyfikacji ról i odpowiedzialności SDLC; proces organizacyjny dotyczący włączenia zarządzania ryzykiem związanym z bezpieczeństwem informacji do SDLC; zautomatyzowane mechanizmy wspierające i/lub wdrażające SDLC].

SA-4	**PROCES NABYCIA**	
	CEL OCENY: *Ustalić, czy organizacja zawiera następujące wymagania, opisy i kryteria, wprost lub przez odniesienie, w umowie nabycia systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego, zgodnie z obowiązującymi przepisami prawnymi, zarządzeniami wykonawczymi, dyrektywami, politykami, przepisami, standardami, oraz wytycznymi:*	
	SA-4(a)	*wymagania funkcjonalne w zakresie bezpieczeństwa;*
	SA-4(b)	*wymagania dotyczące poziomów bezpieczeństwa;*
	SA-4(c)	*wymogi zapewnienia bezpieczeństwa;*
	SA-4(d)	*wymagania dotyczące dokumentacji związanej z bezpieczeństwem;*
	SA-4(e)	*wymagania dotyczące ochrony dokumentacji związanej z bezpieczeństwem;*
	SA-4(f)	*opis:*

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

SA-4	**PROCES NABYCIA**		
		SA-4(f)[1]	*środowiska rozwoju systemu informacyjnego;*
		SA-4(f)[2]	*środowiska, w którym system ma funkcjonować; oraz*
	SA-4(g)	*kryteria komisyjnego odbioru.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące włączania wymogów bezpieczeństwa informacji, opisów i kryteriów do procesu nabywania; umowy nabycia dotyczące systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za realizację umowy kupna/sprzedaży; personel organizacji odpowiedzialny za określenie wymagań funkcjonalnych, eksploatacyjnych i bezpieczeństwa systemu informacyjnego; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne określające wymagania funkcjonalne, jakościowe i bezpieczeństwa systemu informacyjnego; procesy organizacyjne związane z opracowywaniem umów kupna-sprzedaży; zautomatyzowane mechanizmy wspierające i/lub realizujące zakupy oraz uwzględnianie wymagań bezpieczeństwa w umowach].		

SA-4(1)	**PROCES NABYCIA | *WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ***
	CEL OCENY: *Ustalić, czy organizacja wymaga od wykonawcy systemu informacyjnego, komponentu systemu lub serwisu systemu informacyjnego, przedstawienia opisu funkcjonalnych właściwości stosowanych środków bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące włączania wymogów, opisów i kryteriów bezpieczeństwa informacji do procesu nabycia; dokumentacja przetargowa; dokumentacja zakupowa; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

SA-4(1)	**PROCES NABYCIA | *WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za zakupy/umowy; personel organizacji odpowiedzialny za określenie wymagań funkcjonalnych w zakresie bezpieczeństwa systemu informacyjnego; deweloper systemu informacyjnego lub dostawca usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne określające wymagania funkcjonalne bezpieczeństwa systemu informacyjnego; procesy organizacyjne związane z opracowywaniem umów kupna-sprzedaży; zautomatyzowane mechanizmy wspierające i/lub realizujące przejęcia i umieszczanie wymagań bezpieczeństwa w umowach].

SA-4(2)	**PROCES NABYCIA | *PROJEKTOWANIE / IMPLEMENTACJA ZABEZPIECZEŃ***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-4(2)[1]	*określa poziom szczegółowości informacji, jaki deweloper ma obowiązek przedstawić w projekcie i implementacji elementów zabezpieczeń, które mają być zastosowane w systemie informacyjnym, komponencie systemu lub usłudze systemu informacyjnego;*
	SA-4(2)[2]	*definiuje informacje dotyczące projektu/wdrożenia, które deweloper ma obowiązek dostarczyć w celu zastosowania środków bezpieczeństwa;*
	SA-4(2)[3]	*wymaga, aby wykonawca systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego dostarczył stosowne dane dotyczące projektu i wdrożenia środków bezpieczeństwa, które obejmują, na określonym przez organizację poziomie szczegółowości, jedną lub więcej z poniższych informacji:*
		SA-4(2)[3][a] *zewnętrzne interfejsy systemowe związane z bezpieczeństwem;*
		SA-4(2)[3][b] *projekt wysokopoziomowy;*
		SA-4(2)[3][c] *projekt niskopoziomowy;*
		SA-4(2)[3][d] *kod źródłowy;*
		SA-4(2)[3][e] *schematy sprzętowe; i/lub*
		SA-4(2)[3][f] *wymagania projektowe/wdrożeniowe zdefiniowane przez organizację.*

SA-4(2)	**PROCES NABYCIA | *PROJEKTOWANIE / IMPLEMENTACJA ZABEZPIECZEŃ***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące integracji wymogów, opisów i kryteriów bezpieczeństwa informacji z procesem nabycia; dokumentacja przetargowa; dokumentacja zakupu; umowy nabycia systemu, komponentów systemu lub usług systemu informacyjnego; informacje dotyczące projektowania i wdrażania środków bezpieczeństwa stosowanych w systemie informacyjnym, komponencie systemu lub usłudze systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zakupy/umowy; personel organizacji odpowiedzialny za określanie wymogów bezpieczeństwa systemów informacyjnych; deweloperzy systemów informacyjnych lub dostawcy usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne określające poziom szczegółowości projektu systemu i środków bezpieczeństwa; procesy organizacyjne związane z opracowaniem umowy nabycia; zautomatyzowane mechanizmy wspierające i/lub wdrażające opracowanie szczegółów projektu systemu].

SA-4(3)	**PROCES NABYCIA | *METODY ROZWOJU / TECHNIKI / PRAKTYKI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-4(3)[1]	*określa aktualny stan techniczny systemu/ metod inżynierii bezpieczeństwa, które mają być włączone do cyklu życia systemu wdrożonego przez dewelopera systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego;*
	SA-4(3)[2]	*definiuje metody tworzenia oprogramowania, które mają zostać włączone do cyklu życia systemu, stosowane przez dewelopera systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego;*
	SA-4(3)[3]	*definiuje techniki testowania/oceny/zatwierdzania, które mają być włączone do cyklu życia systemu stosowanego przez dewelopera systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego;*
	SA-4(3)[4]	*definiuje procesy kontroli jakości, które mają zostać włączone do cyklu życia systemu stosowanego przez dewelopera systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego;*

SA-4(3)	**PROCES NABYCIA |** ***METODY ROZWOJU / TECHNIKI / PRAKTYKI***		
	SA-4(3)[5]	*wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego, przedstawienia opisu wykorzystania cyklu życia systemu, który obejmuje:*	
		SA-4(3)[5][a]	*zdefiniowany organizacyjnie stan systemu/ metod inżynierii bezpieczeństwa;*
		SA-4(3)[5][b]	*zdefiniowane organizacyjnie metody tworzenia oprogramowania;*
		SA-4(3)[5][c]	*zdefiniowane organizacyjnie techniki testowania / oceny / zatwierdzania; oraz*
		SA-4(3)[5][d]	*zdefiniowane organizacyjnie procesy kontroli jakości.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące integracji wymogów, opisów i kryteriów bezpieczeństwa informacji z procesem nabycia; dokumentacja przetargowa; dokumentacja zakupu; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; zestawienie metod inżynierii systemów/techniki bezpieczeństwa, które mają być włączone do procesu rozwoju cyklu życia systemu; zestawienie metod opracowywania oprogramowania, które mają być włączone do procesu rozwoju cyklu życia systemu; zestawienie technik testowania / oceny / zatwierdzania, które mają być włączone do procesu rozwoju cyklu życia systemu; zestawienie procesów kontroli jakości, które mają być włączone do procesu rozwoju cyklu życia systemu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zakupy/umowy; personel organizacji odpowiedzialny za określanie wymogów bezpieczeństwa systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji i cykl życia systemu; deweloperzy systemów informacyjnych lub dostawcy usług]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące metod, techniki procesów rozwoju].		

SA-4(4)	**PROCES NABYCIA |** ***PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW***
[Włączone do: CM-8(9)].	

<table>
<tr><th colspan="2">SA-4(5)</th><th colspan="3">PROCES NABYCIA | KONFIGURACJA SYSTEMU / KOMPONENTÓW / USŁUG</th></tr>
<tr><td></td><td colspan="4">CEL OCENY:
Określić, czy organizacja:</td></tr>
<tr><td></td><td>SA-4(5)(a)</td><td>SA-4(5)(a)[1]</td><td colspan="2">definiuje konfiguracje bezpieczeństwa, które mają być wdrożone przez dewelopera systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego;</td></tr>
<tr><td></td><td></td><td>SA-4(5)(a)[2]</td><td colspan="2">wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego dostarczył system, komponent lub usługi z wdrożonymi konfiguracjami bezpieczeństwa zdefiniowanymi przez organizację; oraz</td></tr>
<tr><td></td><td>SA-4(5)(b)</td><td colspan="3">nakłada na dewelopera systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego obowiązek stosowania domyślnej konfiguracji w przypadku każdej kolejnej ponownej instalacji lub aktualizacji systemu, komponentu lub usługi.</td></tr>
<tr><td></td><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka nabywania systemów i usług; procedury dotyczące integracji wymogów, opisów i kryteriów bezpieczeństwa informacji z procesem nabycia; dokumentacja przetargowa; dokumentacja zakupu; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; konfiguracje bezpieczeństwa, które mają być wdrożone przez dewelopera systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; umowa gwarancji świadczenia usług (SLA); inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za zakupy/umowy; personel organizacji odpowiedzialny za określanie wymogów bezpieczeństwa systemów informacyjnych; deweloperzy systemów informacyjnych lub dostawcy usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji].
Test: [wybierz spośród: Zautomatyzowane mechanizmy służące do sprawdzania, czy konfiguracja dostarczonego systemu informacyjnego, komponentu lub usług jest taka, jak przedstawiono w specyfikacji.].</td></tr>
</table>

SA-4(6)	**PROCES NABYCIA | *UŻYWANIE PRODUKTÓW ZAPEWNIAJĄCYCH BEZPIECZEŃSTWO INFORMACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-4(6)(a)	*korzysta wyłącznie z gotowych rozwiązań rządowych (GOTS) lub dostępnych gotowych rozwiązań komercyjnych (COTS) gwarantujących zaufanie do informacji (IA) oraz produktów informacyjnych z obsługą IA, zawierających zatwierdzone przez krajową władzę bezpieczeństwa rozwiązania służące do ochrony informacji niejawnych, gdy sieci wykorzystywane do przesyłania informacji są na niższym poziomie klauzuli niejawności niż informacje przesyłane; oraz*
	SA-4(6)(b)	*zapewnia, że produkty bezpieczeństwa informacji zostały ocenione i / lub zatwierdzone przez krajową władzę bezpieczeństwa zgodnie z obowiązującymi przepisami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące integracji wymogów, opisów i kryteriów bezpieczeństwa informacji z procesem nabycia; dokumentacja przetargowa; dokumentacja zakupu; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; konfiguracje bezpieczeństwa, które mają być wdrożone przez dewelopera systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; umowa gwarancji świadczenia usług (SLA); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zakupy/umowy; personel organizacji odpowiedzialny za określanie wymagań w zakresie bezpieczeństwa systemów informacyjnych; personel organizacji odpowiedzialny za zapewnienie, że produkty zapewniające bezpieczeństwo informacji są zatwierdzone przez krajową władzę bezpieczeństwa i są oceniane i/lub zatwierdzane zgodnie z procedurami zatwierdzonymi przez krajową władzę bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące wyboru i stosowania ocenionych i/lub zatwierdzonych produktów i usług w zakresie bezpieczeństwa informacji, składających się z zatwierdzonych przez krajową władzę bezpieczeństwa rozwiązań w zakresie ochrony informacji niejawnych.].	

SA-4(7)	**PROCES NABYCIA | *ZATWIERDZONE PROFILE OCHRONY***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-4(7)(a)	*korzysta z komercyjnych produktów technologii informacyjnych, które zostały pomyślnie ocenione przez krajową władzę bezpieczeństwa zgodnie z obowiązującymi przepisami; oraz*
	SA-4(7)(b)	*wymaga, aby moduł kryptograficzny stosowany w systemie informacyjnym został zatwierdzony przez krajową władzę bezpieczeństwa zgodnie z obowiązującymi przepisami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące integracji wymogów, opisów i kryteriów bezpieczeństwa informacji z procesem nabycia; dokumentacja przetargowa; dokumentacja zakupu; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; profile ochrony zatwierdzone przez krajową władzę bezpieczeństwa; informacje na temat certyfikacji funkcji kryptograficznych przez krajową władzę bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zakupy/umowy; personel organizacji odpowiedzialny za określanie wymagań w zakresie bezpieczeństwa systemu informacyjnego; personel organizacji odpowiedzialny za zapewnienie, że produkty zapewniające bezpieczeństwo informacji zostały ocenione pod kątem profilu ochrony zatwierdzonego przez krajową władzę bezpieczeństwa lub za zapewnienie, że produkty wykorzystujące funkcje kryptograficzne są zgodne z wymaganiami krajowej władzy bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z wyborem i wykorzystaniem wyrobów/usług ocenianych i zatwierdzanych przez krajową władzę bezpieczeństwa].	

SA-4(8)	**PROCES NABYCIA | *PLAN CIĄGŁOŚCI MONITOROWANIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-4(8)[1]	*określa poziom szczegółowości, jaki deweloper systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego jest zobowiązany zapewnić przy tworzeniu planu ciągłości monitorowania skuteczności stosowanych zabezpieczeń; oraz*

SA-4(8)	**PROCES NABYCIA | *PLAN CIĄGŁOŚCI MONITOROWANIA***	
	SA-4(8)[2]	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego opracował plan ciągłości monitorowania skuteczności kontroli bezpieczeństwa stosowanych zabezpieczeń, zawierający określony przez organizację poziom szczegółowości.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące wdrażania planu ciągłości monitorowania; procedury dotyczące włączania wymogów bezpieczeństwa informacji, opisów i kryteriów do procesu zakupów; wdrożony plan ciągłości monitorowania; plan oceny bezpieczeństwa; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja zakupowa; dokumentacja przetargowa, umowa gwarancji świadczenia usług (SLA); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zakupy/umowy; personel organizacji odpowiedzialny za określanie wymagań w zakresie bezpieczeństwa systemu informacyjnego; deweloperzy systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy dostawcy zapewniające ciągłość monitorowania; zautomatyzowane mechanizmy wspierające i/lub wdrażające ciągłość monitorowania].	

SA-4(9)	**PROCES NABYCIA | *FUNKCJE / PORTY / PROTOKOŁY / USŁUGI***	
	CEL OCENY: *Ustalić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego w początkowym cyklu życia system, identyfikacji:*	
	SA-4(9)[1]	*funkcji przeznaczonych do użytku organizacyjnego;*
	SA-4(9)[2]	*portów przeznaczonych do użytku organizacyjnego;*
	SA-4(9)[3]	*protokołów przeznaczonych do użytku organizacyjnego; oraz*
	SA-4(9)[4]	*usług przeznaczonych do użytku organizacyjnego.*

SA-4(9)	**PROCES NABYCIA | *FUNKCJE / PORTY / PROTOKOŁY / USŁUGI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące integracji wymagań, opisów i kryteriów bezpieczeństwa informacji z procesem zakupu; dokumentacja projektowa systemu informacyjnego; dokumentacja systemu informacyjnego uwzględniająca funkcje, porty, protokoły i usługi przeznaczone do użytku organizacyjnego; umowy nabycia systemów lub usług informacyjnych; dokumentacja zakupowa; dokumentacja przetargowa, umowa gwarancji świadczenia usług (SLA); wymagania, opisy i kryteria bezpieczeństwa organizacyjnego dla deweloperów systemów informacyjnych, komponentów systemów i usług systemów informacyjnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zakupy/umowy; personel organizacji odpowiedzialny za określanie wymagań w zakresie bezpieczeństwa systemu informacyjnego; administratorzy systemu/sieci; personel organizacji obsługujący, korzystający i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

SA-4(10)	**PROCES NABYCIA | *WYKORZYSTANIE ZATWIERDZONYCH PRODUKTÓW***
	CEL OCENY: *Ustalenie, czy organizacja stosuje wyłącznie technologie informacyjne, znajdujące się na liście produktów zatwierdzonych zgodnie z wewnętrznymi regulacjami organizacji lub wymaganiami ustalonymi przepisami prawa, do celów weryfikacji tożsamości osobistej zaimplementowanych w organizacyjnych systemach informacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące włączania wymogów bezpieczeństwa informacji, opisów i kryteriów do procesów nabycia; dokumentacja przetargowa; dokumentacja nabycia; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; umowa gwarancji świadczenia usług (SLA); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zakupy/umowy; personel organizacji odpowiedzialny za określanie wymagań w zakresie bezpieczeństwa systemu informacyjnego; personel organizacji odpowiedzialny za zapewnienie wdrożenia wyłącznie produktów certyfikowanych przez stosowne organy; personel organizacji odpowiedzialny za bezpieczeństwo informacji].

SA-4(10)	**PROCES NABYCIA | *WYKORZYSTANIE ZATWIERDZONYCH PRODUKTÓW***
	Test: [*wybierz spośród:* Procesy organizacyjne dotyczące wyboru i stosowania certyfikowanych produktów].

SA-5	**DOKUMENTACJA SYSTEMU INFORMACYJNEGO**			
	CEL OCENY: *Określić, czy organizacja:*			
	SA-5(a)	*tworzy dokumentację administratora systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego, która opisuje:*		
		SA-5(a)(1)	**SA-5(a)(1)[1]**	*bezpieczną konfigurację systemu, komponentu systemu lub usług;*
			SA-5(a)(1)[2]	*bezpieczną instalację systemu, komponentu systemu lub usług;*
			SA-5(a)(1)[3]	*bezpieczną eksploatację systemu, komponentu systemu lub usług;*
		SA-5(a)(2)	**SA-5(a)(2)[1]**	*efektywne wykorzystanie funkcji/mechanizmów bezpieczeństwa;*
			SA-5(a)(2)[2]	*skuteczną obsługę funkcji/mechanizmów bezpieczeństwa;*
		SA-5(a)(3)	*znane luki dotyczące konfiguracji i korzystania z funkcji administracyjnych (tj. uprzywilejowanych);*	
	SA-5(b)	*uzyskuje/tworzy dokumentację użytkownika dotyczącą systemu informacyjnego, komponentu systemu lub serwisu systemu informacyjnego, która opisuje:*		
		SA-5(b)(1)	**SA-5(b)(1)[1]**	*dostępne dla użytkownika funkcje/mechanizmy bezpieczeństwa;*
			SA-5(b)(1)[2]	*jak efektywnie wykorzystywać te funkcje/mechanizmy;*
		SA-5(b)(2)	*metody interakcji z użytkownikiem, które pozwalają na bezpieczniejsze korzystanie z systemu, komponentu lub usługi;*	

SA-5	**DOKUMENTACJA SYSTEMU INFORMACYJNEGO**		
		SA-5(b)(3)	*obowiązki użytkownika w zakresie zachowania bezpieczeństwa systemu, komponentu lub usługi;*
	SA-5(c)	**SA-5(c)[1]**	*określa działania, które należy wykonać po udokumentowanych próbach uzyskania informacji o systemie, komponencie systemu lub dokumentacji serwisowej systemu informacyjnego, gdy taka dokumentacja jest niedostępna lub nie istnieje;*
		SA-5(c)[2]	*dokumentuje próby pozyskania dokumentacji systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego, gdy taka dokumentacja jest niedostępna lub nie istnieje;*
		SA-5(c)[3]	*w odpowiedzi podejmuje działania określone przez organizację;*
	SA-5(d)	*chroni dokumentację stosownie do potrzeb, zgodnie ze strategią zarządzania ryzykiem;*	
	SA-5(e)	**SA-5(e)[1]**	*określa personel lub role, którym ma być przekazywana dokumentacja; oraz*
		SA-5(e)[2]	*dystrybuuje dokumentację do personelu lub ról zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące dokumentacji systemu informacyjnego; dokumentacja systemu informacyjnego, w tym instrukcje administratora i użytkownika; rejestry dokumentujące próby uzyskania niedostępnej lub nieistniejącej dokumentacji systemu informacyjnego; lista działań, jakie należy podjąć w odpowiedzi na udokumentowane próby uzyskania dokumentacji systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego; dokumentacja strategii zarządzania ryzykiem; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zakupy/umowy; personel organizacji odpowiedzialny za określanie wymagań w zakresie bezpieczeństwa systemu informacyjnego; administratorzy systemu; personel organizacji obsługujący, korzystający i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z pozyskiwaniem, ochroną i dystrybucją dokumentacji administratora systemu informacyjnego i użytkownika].		

SA-5(1)	**DOKUMENTACJA SYSTEMU INFORMACYJNEGO | *FUNKCJONALNE WŁAŚCIWOŚCI ŚRODKÓW BEZPIECZEŃSTWA***
[Włączone do: SA-4(1)].	

SA-5(2)	**DOKUMENTACJA SYSTEMU INFORMACYJNEGO | *BEZPIECZEŃSTWO INTERFEJSÓW SYSTEMU ZEWNĘTRZNEGO***
[Włączone do: SA-4(2)].	

SA-5(3)	**DOKUMENTACJA SYSTEMU INFORMACYJNEGO | *PROJEKTOWANIE WYSOKOPOZIOMOWE***
[Włączone do: SA-4(2)].	

SA-5(4)	**DOKUMENTACJA SYSTEMU INFORMACYJNEGO | *PROJEKTOWANIE NISKOPOZIOMOWE***
[Włączone do: SA-4(2)].	

SA-5(5)	**DOKUMENTACJA SYSTEMU INFORMACYJNEGO | *KOD ŹRÓDŁOWY***
[Włączone do: SA-4(2)].	

SA-6	**OGRANICZENIA W UŻYCIU OPROGRAMOWANIA**
[Włączone do: CM-10 oraz SI-7].	

SA-7	**OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA**
[Włączone do: CM-11 oraz SI-7].	

SA-8	**ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI**	
	CEL OCENY: *Ustalić, czy organizacja określa zasady inżynierii bezpieczeństwa systemu informacyjnego, podczas:*	
	SA-8[1]	*tworzenia specyfikacji systemu informacyjnego;*
	SA-8[2]	*projektowania systemu informacyjnego;*
	SA-8[3]	*opracowywania systemu informacyjnego;*
	SA-8[4]	*wdrażania systemu informacyjnego; oraz*
	SA-8[5]	*modyfikacji systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące zasad inżynierii bezpieczeństwa stosowanych w specyfikacji, projektowaniu, opracowywaniu, wdrażaniu i modyfikacji systemu informacyjnego; wymagania dotyczące bezpieczeństwa informacji oraz specyfikacje systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zakupy/umowy; personel organizacji odpowiedzialny za określanie wymagań w zakresie bezpieczeństwa systemu informacyjnego; personel organizacji odpowiedzialny za specyfikację, projektowanie, rozwój, wdrażanie i modyfikację systemu informacyjnego; deweloperzy systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie stosowania zasad inżynierii bezpieczeństwa w specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu informacyjnego; zautomatyzowane mechanizmy wspierające stosowanie zasad inżynierii bezpieczeństwa w specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu informacyjnego].	

SA-9	**USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMACYJNEGO**		
	CEL OCENY: *Określić, czy organizacja:*		
	SA-9(a)	**SA-9(a)[1]**	*definiuje środki bezpieczeństwa, które mają być stosowane przez dostawców usług zewnętrznego systemu informacyjnego;*

SA-9	**USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMACYJNEGO**		
		SA-9(a)[2]	*wymaga, aby dostawcy usług zewnętrznego systemu informacyjnego stosowali się do organizacyjnych wymogów bezpieczeństwa informacji;*
		SA-9(a)[3]	*wymaga, aby dostawcy usług zewnętrznego systemu informacyjnego stosowali określone przez organizację środki bezpieczeństwa zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, normami, standardami i wytycznymi;*
	SA-9(b)	**SA-9(b)[1]**	*definiuje oraz dokumentuje nadzór w odniesieniu do usług zewnętrznego systemu informacyjnego;*
		SA-9(b)[2]	*definiuje oraz dokumentuje role i obowiązki użytkowników w odniesieniu do usług zewnętrznego systemu informacyjnego;*
	SA-9(c)	**SA-9(c)[1]**	*definiuje procesy, metody oraz techniki, które mają być stosowane do monitorowania zgodności środków bezpieczeństwa przez usługodawcę zewnętrznego; oraz*
		SA-9(c)[2]	*wykorzystuje zdefiniowane organizacyjnie procesy, metody i techniki do bieżącego monitorowania zgodności środków bezpieczeństwa przez usługodawcę zewnętrznego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące usług zewnętrznego systemu informacyjnego; procedury dotyczące metod i technik monitorowania przestrzegania kontroli bezpieczeństwa przez zewnętrznych dostawców usług systemu informacyjnego; umowy nabycia; umowa gwarancji świadczenia usług (SLA); wymagania organizacyjne dotyczące bezpieczeństwa oraz specyfikacje bezpieczeństwa dla usług świadczonych przez dostawców zewnętrznych; ewidencja wyników kontroli bezpieczeństwa uzyskana od zewnętrznych dostawców usług systemów informacyjnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; zewnętrzni dostawcy usług systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące bieżącemu monitorowaniu zgodności środków bezpieczeństwa przez zewnętrznych dostawców usług; zautomatyzowane mechanizmy stałego monitorowania zgodności środków bezpieczeństwa przez zewnętrznych dostawców usług].		

<table>
<tr><th colspan="4">SA-9(1) USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMACYJNEGO | OCENA RYZYKA / ZATWIERDZENIA ORGANIZACYJNE</th></tr>
<tr><td></td><td colspan="3">CEL OCENY:
Określić, czy organizacja:</td></tr>
<tr><td></td><td>SA-9(1)(a)</td><td colspan="2">przeprowadza ocenę organizacyjną ryzyka przed nabyciem lub zleceniem na zewnątrz dedykowanych usług bezpieczeństwa informacji;</td></tr>
<tr><td></td><td rowspan="2">SA-9(1)(b)</td><td>SA-9(1)(b)[1]</td><td>określa personel lub role wyznaczone do zatwierdzania nabywania lub zlecania na zewnątrz dedykowanych usług w zakresie bezpieczeństwa informacji; oraz</td></tr>
<tr><td></td><td>SA-9(1)(b)[2]</td><td>zapewnia, że nabycie lub powierzenie na zewnątrz dedykowanych usług bezpieczeństwa informacji jest zatwierdzone przez personel lub role określone przez organizację.</td></tr>
<tr><td></td><td colspan="3">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka nabywania systemów i usług; procedury dotyczące usług zewnętrznego systemu informacyjnego; dokumentacja nabycia; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; raporty z szacowania ryzyka; dokumentacja zatwierdzająca nabycie lub powierzenie na zewnątrz dedykowanych usług bezpieczeństwa informacji; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo systemu informacyjnego; zewnętrzni dostawcy usług systemów informacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].
Test: [wybierz spośród: Procesy organizacyjne przeprowadzenia szacowania ryzyka przed nabyciem lub powierzeniem dedykowanych usług bezpieczeństwa informacji; procesy organizacyjne zatwierdzania powierzenia dedykowanych usług bezpieczeństwa informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające szacowanie ryzyka; zautomatyzowane mechanizmy wspierające i/lub wdrażające procesy zatwierdzania].</td></tr>
</table>

<table>
<tr><th colspan="4">SA-9(2) USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMACYJNEGO | IDENTYFIKACJA FUNKCJI / PORTÓW / PROTOKOŁÓW / USŁUG</th></tr>
<tr><td></td><td colspan="3">CEL OCENY:
Określić, czy organizacja:</td></tr>
<tr><td></td><td>SA-9(2)[1]</td><td colspan="2">definiuje usługi zewnętrznego systemu informacyjnego, w przypadku których dostawcy usług mają określić funkcje, porty, protokoły oraz inne usługi wymagane do korzystania z takich usług;</td></tr>
<tr><td></td><td rowspan="5">SA-9(2)[2]</td><td colspan="2">wymaga od dostawców zdefiniowanych organizacyjnie usług zewnętrznego systemu informacyjnego zidentyfikowania:</td></tr>
<tr><td>SA-9(2)[2][a]</td><td>funkcji wymaganych do korzystania z takich usług;</td></tr>
<tr><td>SA-9(2)[2][b]</td><td>portów wymagane do korzystania z takich usług;</td></tr>
<tr><td>SA-9(2)[2][c]</td><td>protokołów wymaganych do korzystania z takich usług; oraz</td></tr>
<tr><td>SA-9(2)[2][d]</td><td>inne usługi wymagane do korzystania z takich usług.</td></tr>
<tr><td></td><td colspan="3">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka nabywania systemów i usług; procedury dotyczące usług zewnętrznego systemu informacyjnego; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja zakupowa; dokumentacja przetargowa, umowa gwarancji świadczenia usług (SLA); wymagania organizacyjne dotyczące bezpieczeństwa oraz specyfikacje bezpieczeństwa dotyczące usługodawcy zewnętrznego; wykaz wymaganych funkcji, portów, protokołów i innych usług; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; zewnętrzni dostawcy usług systemów informacyjnych].</td></tr>
</table>

SA-9(3)	**USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMACYJNEGO | *TWORZENIE / UTRZYMANIE RELACJI ZAUFANIA Z DOSTAWCAMI***		
	CEL OCENY: *Określić, czy organizacja:*		
	SA-9(3)[1]	*definiuje wymagania, właściwości, czynniki lub warunki określające akceptowalne relacje zaufania;*	
	SA-9(3)[2]	*w oparciu o zdefiniowane przez organizację wymagania, właściwości, czynniki lub warunki definiujące akceptowalne relacje oparte na zaufaniu:*	
		SA-9(3)[2][a]	*ustanawia relacje zaufania z zewnętrznymi dostawcami usług;*
		SA-9(3)[2][b]	*dokumentuje relacje oparte na zaufaniu z zewnętrznymi dostawcami usług; oraz*
		SA-9(3)[2][c]	*utrzymuje relacje zaufania z zewnętrznymi dostawcami usług.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące usług zewnętrznego systemu informacyjnego; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja zakupowa; dokumentacja przetargowa, umowa gwarancji świadczenia usług (SLA); wymogi bezpieczeństwa organizacyjnego, właściwości, czynniki lub warunki określające dopuszczalne relacje zaufania; dokumentacja relacji zaufania z usługodawcą zewnętrznym; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; zewnętrzni dostawcy usług systemów informacyjnych].		

SA-9(4)	**USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMACYJNEGO | *ZGODNOŚĆ INTERESÓW KONSUMENTÓW I DOSTAWCÓW***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-9(4)[1]	*definiuje usługodawcę zewnętrznego, którego interesy są zgodne i odzwierciedlają interesy organizacyjne;*

SA-9(4)	**USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMACYJNEGO | *ZGODNOŚĆ INTERESÓW KONSUMENTÓW I DOSTAWCÓW***	
	SA-9(4)[2]	*definiuje zabezpieczenia, które należy stosować w celu zapewnienia, że interesy zdefiniowane przez usługodawcę zewnętrznego są spójne z interesami organizacyjnymi i odzwierciedlają te interesy; oraz*
	SA-9(4)[3]	*stosuje zdefiniowane organizacyjnie zabezpieczenia, zapewniające, że interesy zdefiniowanego usługodawcy zewnętrznego są spójne z interesami organizacji oraz odzwierciedlają jej interesy.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące usług zewnętrznego systemu informacyjnego; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); organizacyjne środki bezpieczeństwa / zabezpieczenia stosowane wobec zewnętrznych dostawców usług; polityka bezpieczeństwa osobowego stosowana wobec zewnętrznych dostawców usług; oceny przeprowadzane wobec zewnętrznych dostawców usług; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; zewnętrzni dostawcy usług systemów informacyjnych]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące definiowania i stosowania zabezpieczeń zapewniających spójność interesów z usługodawcą zewnętrznym; zautomatyzowane mechanizmy wspierające i/lub wdrażające zabezpieczenia zapewniające spójność interesów z usługodawcą zewnętrznym].	

SA-9(5)	**USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMACYJNEGO | *OBSZAR PROCESOWANIA, PRZECHOWYWANIA I OBSŁUGI TECHNICZNEJ***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-9(5)[1]	*określa miejsca, w których dostęp do zdefiniowanych przez organizację usług przetwarzania informacji, informacji/danych i/lub usług systemu informacyjnego ma być ograniczony;*
	SA-9(5)[2]	*definiuje wymagania lub warunki ograniczające dostęp do lokalizacji przetwarzającej informacje, informacji/danych i/lub usług systemu informacyjnego;*

SA-9(5)	**USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMACYJNEGO | *OBSZAR PROCESOWANIA, PRZECHOWYWANIA I OBSŁUGI TECHNICZNEJ***		
	SA-9(5)[3]	*ogranicza dostęp, w oparciu o zdefiniowane wymagania lub warunki, do jednej lub kilku z poniższych lokalizacji zdefiniowanych przez organizację:*	
		SA-9(5)[3][a]	*przetwarzania informacji;*
		SA-9(5)[3][b]	*przechowywania informacji/danych; i/lub*
		SA-9(5)[3][c]	*usług systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące usług zewnętrznego systemu informacyjnego; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); miejsca o ograniczonym dostępie do przetwarzanych informacji; usługi przetwarzania informacji, przechowywania informacji/danych i/lub usługi systemu informacyjnego, które mają być świadczone w miejscach o ograniczonym dostępie; organizacyjne wymogi bezpieczeństwa lub warunki dotyczące dostawców zewnętrznych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; zewnętrzni dostawcy usług systemów informacyjnych]. **Test**: [*wybierz spośród:* Procesy organizacyjne określające wymagania dotyczące ograniczenia lokalizacji przetwarzania informacji, informacji/danych lub usług informacyjnych; procesy organizacyjne mające na celu zapewnienie ograniczenia lokalizacji zgodnie z wymaganiami lub warunkami].		

SA-10	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA**		
	CEL OCENY: *Określić, czy organizacja:*		
	SA-10(a)	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego zarządzał konfiguracją w fazie:*	
		SA-10(a)[1]	*projektowania systemu, komponentu lub usługi;*
		SA-10(a)[2]	*rozwoju systemu, komponentu lub usługi;*
		SA-10(a)[3]	*wdrożenie systemu, komponentu lub usługi; i/lub*

SA-10	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA**			
		SA-10(a)[4]	*eksploatacji systemu, komponentów lub usług;*	
	SA-10(b)	**SA-10(b)[1]**	*definiuje pozycje konfiguracyjne, które mają zostać umieszczone w systemie zarządzania konfiguracją;*	
		SA-10(b)[2]	*wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego:*	
			SA-10(b)[2][a]	*dokumentowania integralności zmian w elementach zdefiniowanych przez organizację w ramach zarządzania konfiguracją;*
			SA-10(b)[2][b]	*zarządzania integralnością zmian w elementach zdefiniowanych w organizacji w ramach zarządzania konfiguracją;*
			SA-10(b)[2][c]	*kontrolowania integralności zmian w zdefiniowanych przez organizację elementach w ramach zarządzania konfiguracją;*
	SA-10(c)	wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego wprowadzał tylko zatwierdzone przez organizację zmiany w systemie, komponencie lub usłudze;		
	SA-10(d)	wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego sporządził dokumentację:		
		SA-10(d)[1]	*zatwierdzonych zmian w systemie, komponencie lub usłudze;*	
		SA-10(d)[2]	*potencjalnego wpływu tych zmian na bezpieczeństwo;*	
	SA-10(e)	**SA-10(e)[1]**	*wskazuje personel, któremu należy zgłaszać przypadki wykrycia błędów w zakresie bezpieczeństwa, wynikających z nieprawidłowości w systemie, komponencie lub usłudze;*	
		SA-10(e)[2]	*wymaga od twórcy systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego:*	

SA-10	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA**			
			SA-10(e)[2][a]	*śledzenia błędów w zakresie bezpieczeństwa w systemie, komponencie lub usłudze;*
			SA-10(e)[2][b]	*rozwiązywania problemów związanych z błędami w zakresie bezpieczeństwa systemu, komponentu lub usługi; oraz*
			SA-10(e)[2][c]	*zgłaszania nieprawidłowości personelowi określonemu przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące zarządzania konfiguracją dewelopera systemu; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plan zarządzania konfiguracją dewelopera systemu; usterki bezpieczeństwa oraz zapisy śledzenia usterek; zapisy autoryzacji zmian w systemie; rejestry zabezpieczeń zmian; rejestry zarządzania konfiguracją; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie konfiguracją; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu zarządzania konfiguracją dewelopera; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie zarządzania konfiguracją dewelopera].			

SA-10(1)	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | *WERYFIKACJA INTEGRALNOŚCI PROGRAMÓW / OPROGRAMOWANIA UKŁADOWEGO***
	CEL OCENY: *Ustalić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego, aby umożliwiał weryfikację integralności komponentów aplikacji i oprogramowania układowego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące systemu zarządzania konfiguracją dewelopera; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA);

SA-10(1)	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | *WERYFIKACJA INTEGRALNOŚCI PROGRAMÓW / OPROGRAMOWANIA UKŁADOWEGO***
	umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plan zarządzania konfiguracją systemu dewelopera; zapisy dotyczące weryfikacji integralności aplikacji i oprogramowania układowego; zapisy dotyczące autoryzacji zmian w systemie; rejestry zabezpieczeń zmian; rejestry zarządzania konfiguracją; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie konfiguracją; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu zarządzania konfiguracją dewelopera; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie zarządzania konfiguracją dewelopera].

SA-10(2)	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | *ALTERNATYWNE PROCESY ZARZĄDZANIA KONFIGURACJĄ***
	CEL OCENY: *Ustalić, czy organizacja zapewnia alternatywny proces zarządzania konfiguracją z udziałem personelu organizacji, w przypadku braku dedykowanego zespołu programistów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące systemu zarządzania konfiguracją dewelopera; procedury dotyczące zarządzania konfiguracją; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plan zarządzania konfiguracją systemu dewelopera; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie konfiguracją; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu zarządzania konfiguracją dewelopera; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie zarządzania konfiguracją dewelopera].

SA-10(3)	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | *WERYFIKACJA INTEGRALNOŚCI SPRZĘTU***
	CEL OCENY: *Ustalić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego, aby umożliwiał weryfikację integralności komponentów sprzętowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące systemu zarządzania konfiguracją dewelopera; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plan zarządzania konfiguracją systemu dewelopera; protokoły weryfikacji integralności sprzętu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie konfiguracją; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu zarządzania konfiguracją dewelopera; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie zarządzania konfiguracją dewelopera].

SA-10(4)	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | *ZAUFANA GENERACJA***	
	CEL OCENY: *Ustalić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego zastosowania narzędzi do porównywania nowo wygenerowanych wersji z poprzednimi wersjami:*	
	SA-10(4)[1]	*opisów urządzeń istotnych dla bezpieczeństwa; oraz*
	SA-10(4)[2]	*źródeł oprogramowania/oprogramowania układowego i kodu obiektu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące systemu zarządzania konfiguracją dewelopera; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plan zarządzania konfiguracją systemu dewelopera; rejestry zabezpieczeń zmian; rejestry zarządzania konfiguracją; zapisy z audytu kontroli konfiguracji; inne odpowiednie dokumenty lub rejestry].	

SA-10(4)	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | *ZAUFANA GENERACJA***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie konfiguracją; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu zarządzania konfiguracją dewelopera; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie zarządzania konfiguracją dewelopera].

SA-10(5)	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | *INTEGRALNOŚĆ MAPOWANIA KONTROLI WERSJI***
	CEL OCENY: *Określić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego utrzymania integralności mapowania między danymi kompilacji głównej (sprzęt i programy/ oprogramowanie układowe) opisującymi aktualną wersję istotnego dla bezpieczeństwa sprzętu, aplikacji i oprogramowania układowego oraz zaktualizowaną kopią głównej wersji danych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące systemu zarządzania konfiguracją dewelopera; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plan zarządzania konfiguracją systemu dewelopera; rejestry zabezpieczeń zmian; rejestry zarządzania konfiguracją; zapisy dotyczące kontroli wersji/aktualizacji; zapisy dotyczące weryfikacji integralności między głównymi kopiami sprzętu, programów i oprogramowania układowego istotnych dla bezpieczeństwa (w tym projektów i kodu źródłowego); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie konfiguracją; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu zarządzania konfiguracją dewelopera; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie zarządzania konfiguracją dewelopera].

SA-10(6)	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | *ZAUFANA DYSTRYBUCJA***
	CEL OCENY: *Określić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego wykonania procedur mających na celu zapewnienie, że sprzęt, aplikacje oraz aktualizacje oprogramowania układowego związane z bezpieczeństwem, które są rozpowszechniane w organizacji, są dokładnie takie, jak określono w egzemplarzach głównych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące systemu zarządzania konfiguracją dewelopera; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plan zarządzania konfiguracją systemu dewelopera; rejestry zabezpieczeń zmian; rejestry zarządzania konfiguracją; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie konfiguracją; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu zarządzania konfiguracją dewelopera; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie zarządzania konfiguracją dewelopera].

SA-11	**TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA**	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-11(a)	*wymaga od twórcy systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego stworzenia i wdrożenia planu bezpieczeństwa;*
	SA-11(b)	**SA-11(b)[1]** *określa szczegółowość testów/oceny, które mają być przeprowadzone przez dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego;*
		SA-11(b)[2] *definiuje zakres testów/oceny, które mają być wykonane przez dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego;*

SA-11	**TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA**			
		SA-11(b)[3]	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego wykonał jeden lub więcej z poniższych testów/oceny, z uwzględnieniem określonej przez organizację szczegółowości i zakresu:*	
			SA-11(b)[3][a]	*jednostkowy;*
			SA-11(b)[3][b]	*konsolidacyjny;*
			SA-11(b)[3][c]	*systemowy; i/lub*
			SA-11(b)[3][d]	*zredukowany;*
	SA-11(c)	*wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego przedstawienia dowodów:*		
		SA-11(c)[1]	*wykonania planu oceny bezpieczeństwa;*	
		SA-11(c)[2]	*uzyskania wyników testów/oceny bezpieczeństwa;*	
	SA-11(d)	*wymaga od dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego wdrożenia możliwego do zweryfikowania procesu usuwania usterek; oraz*		
	SA-11(e)	*wymaga od twórcy systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego usunięcia nieprawidłowości wykrytych podczas testowania/oceny bezpieczeństwa.*		
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące testowania bezpieczeństwa przez deweloperów systemów; procedury dotyczące usuwania usterek; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plany testowania bezpieczeństwa przez dewelopera systemu; zapisy wyników testów bezpieczeństwa systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego przeprowadzonych przez dewelopera; zapisy śledzenia usterek bezpieczeństwa i usuwania awarii; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za testowanie bezpieczeństwa przez dewelopera; deweloperzy systemów].			

SA-11	**TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA**
	Test: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu testów i oceny bezpieczeństwa przez deweloperów; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie testów i oceny bezpieczeństwa przez deweloperów].

SA-11(1)	**TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | *ANALIZA KODU STATYCZNEGO***
	CEL OCENY: *Ustalić, czy organizacja wymaga od developera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego zastosowania narzędzi do analizy kodu statystycznego, w celu identyfikacji typowych błędów oraz udokumentowania wyników analizy.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące testowania bezpieczeństwa przez deweloperów systemów; procedury dotyczące usuwania usterek; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plany testów bezpieczeństwa przez dewelopera systemu; wyniki testów bezpieczeństwa przeprowadzonych przez dewelopera systemu; błędy w zakresie bezpieczeństwa oraz zapisy śledzenia działań naprawczych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za testowanie bezpieczeństwa przez dewelopera; personel organizacji odpowiedzialny za zarządzanie konfiguracją; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu testów i oceny bezpieczeństwa przez deweloperów; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie testów i oceny bezpieczeństwa przez deweloperów; narzędzia do analizy kodu statycznego].

SA-11(2)	**TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | *ANALIZA ZAGROŻENIA I WRAŻLIWOŚCI***	
	CEL OCENY: *Ustalić, czy organizacja wymaga wykonania przez dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego:*	
	SA-11(2)[1]	*analizy zagrożeń związanych z budową, komponentem systemu lub usługą;*
	SA-11(2)[2]	*analizy podatności wykonanego systemu, komponentu systemu lub usługi; oraz*
	SA-11(2)[3]	*dalszych testów/oceny powykonawczej systemu, komponentu systemu lub usługi.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące testów bezpieczeństwa przez dewelopera systemu; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plany testów bezpieczeństwa przez dewelopera systemu; zapisy wyników testów bezpieczeństwa przeprowadzonych przez dewelopera w odniesieniu do systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego; wyniki skanowania podatności; raporty z szacowania ryzyka systemu informacyjnego; raporty z analizy zagrożeń i podatności na zagrożenia; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za testowanie bezpieczeństwa przez dewelopera; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu testów i oceny bezpieczeństwa przez deweloperów; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie testów i oceny bezpieczeństwa przez deweloperów].	

<table>
<tr><th colspan="5">SA-11(3) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | NIEZALEŻNA WERYFIKACJA PLANÓW OCENY / EWIDENCJA</th></tr>
<tr><td></td><td colspan="4">CEL OCENY:
Określić, czy organizacja:</td></tr>
<tr><td></td><td>SA-11(3)(a)</td><td>SA-11(3)(a)[1]</td><td colspan="2">określa kryteria niezależności, które musi spełniać niezależny organ;</td></tr>
<tr><td></td><td></td><td>SA-11(3)(a)[2]</td><td colspan="2">wymaga od niezależnego organu spełnienia określonych przez organizację kryteriów niezależności w celu weryfikacji:</td></tr>
<tr><td></td><td></td><td></td><td>SA-11(3)(a)[2][a]</td><td>prawidłowego wdrożenia planu oceny bezpieczeństwa przez dewelopera;</td></tr>
<tr><td></td><td></td><td></td><td>SA-11(3)(a)[2][b]</td><td>dowodów uzyskanych podczas testów/oceny bezpieczeństwa;</td></tr>
<tr><td></td><td>SA-11(3)(b)</td><td colspan="3">zapewnia, że niezależny organ uzyskał:</td></tr>
<tr><td></td><td></td><td>SA-11(3)(b)[1]</td><td colspan="2">wystarczające informacje pozwalające na zakończenie procesu weryfikacji; lub</td></tr>
<tr><td></td><td></td><td>SA-11(3)(b)[2]</td><td colspan="2">upoważnienia do otrzymania takich informacji.</td></tr>
<tr><td></td><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka nabywania systemów i usług; procedury dotyczące testów bezpieczeństwa przez dewelopera systemu; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; sprawozdania z niezależnej weryfikacji i oceny; testy bezpieczeństwa i plany oceny; testy bezpieczeństwa i wyniki oceny systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za testowanie bezpieczeństwa przez dewelopera; deweloperzy systemów; niezależny organ weryfikujący].
Test: [wybierz spośród: Procesy organizacyjne służące monitorowaniu testów i oceny bezpieczeństwa przez deweloperów; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie testów i oceny bezpieczeństwa przez deweloperów].</td></tr>
</table>

SA-11(4)	**TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | *MANUALNY PRZEGLĄD KODU***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-11(4)[1]	*definiuje określony kod, w odniesieniu do którego deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego jest zobowiązany do wykonania ręcznego przeglądu kodu;*
	SA-11(4)[2]	*definiuje procesy, procedury i/lub techniki, które mają być stosowane podczas wykonywania przez dewelopera ręcznego przeglądu kodu określonego przez organizację; oraz*
	SA-11(4)[3]	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego dokonał ręcznego przeglądu kodu określonego przez organizację, przy użyciu zdefiniowanych przez nią procesów, procedur i/lub technik.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące testów bezpieczeństwa przez dewelopera systemu; procesy, procedury i/lub techniki wykonywania ręcznego przeglądu kodu; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plany testowania i oceny bezpieczeństwa systemu przez dewelopera; wyniki testowania i oceny bezpieczeństwa systemu przez dewelopera; lista kodów wymagających przeglądu ręcznego; zapisy przeglądu ręcznego kodu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za testowanie bezpieczeństwa przez dewelopera; deweloperzy systemów; niezależny organ weryfikujący]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu testów i oceny bezpieczeństwa przez deweloperów; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie testów i oceny bezpieczeństwa przez deweloperów].	

<table>
<tr><th colspan="4">SA-11(5) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | TESTOWANIE PENETRACYJNE / ANALIZA</th></tr>
<tr><td></td><td colspan="3">CEL OCENY:
Określić, czy organizacja:</td></tr>
<tr><td></td><td>SA-11(5)[1]</td><td colspan="2">definiuje w wymaganiach dla dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego:</td></tr>
<tr><td></td><td></td><td>SA-11(5)[1][a]</td><td>zakres testów penetracyjnych, które mają być wykonane przez dewelopera;</td></tr>
<tr><td></td><td></td><td>SA-11(5)[1][b]</td><td>szczegółowość testów penetracyjnych, które mają być wykonane przez dewelopera;</td></tr>
<tr><td></td><td>SA-11(5)[2]</td><td colspan="2">określa ograniczenia, w ramach których deweloper ma wykonywać testy penetracyjne; oraz</td></tr>
<tr><td></td><td>SA-11(5)[3]</td><td colspan="2">wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego wykonywał testy penetracyjne na określonym przez organizację zakresie/szczegółowości oraz z określonymi przez organizację ograniczeniami.</td></tr>
<tr><td></td><td colspan="3">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka nabywania systemów i usług; procedury dotyczące testów bezpieczeństwa przez dewelopera systemu; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; testowanie penetracyjne i ocena systemów przez deweloperów; wyniki badań penetracyjnych i oceny systemów przez deweloperów; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za testowanie bezpieczeństwa przez dewelopera; deweloperzy systemów; niezależny organ weryfikujący].
Test: [wybierz spośród: Procesy organizacyjne służące monitorowaniu testów i oceny bezpieczeństwa przez deweloperów; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie testów i oceny bezpieczeństwa przez deweloperów].</td></tr>
</table>

SA-11(6)	**TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | *PRZEGLĄD PŁASZCZYZNY ATAKU***
	CEL OCENY: *Ustalić, czy organizacja wymaga od producenta systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego przeprowadzenia przeglądu płaszczyzny ataku.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące testów bezpieczeństwa przez dewelopera systemu; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plany testowania i oceny bezpieczeństwa systemu przez dewelopera; wyniki testowania i oceny bezpieczeństwa systemu przez dewelopera; wyniki przeglądu płaszczyzny ataku; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za testowanie bezpieczeństwa przez dewelopera; personel organizacji odpowiedzialny za zarządzanie konfiguracją; deweloperzy systemów]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu testów i oceny bezpieczeństwa przez deweloperów; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie testów i oceny bezpieczeństwa przez deweloperów].

SA-11(7)	**TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | *WERYFIKACJA ZAKRESU TESTU / OCENA***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-11(7)[1]	*określa szczegółowość testów/oceny w celu zapewnienia, że zakres testów / oceny bezpieczeństwa zapewnia pełne pokrycie wymaganych środków bezpieczeństwa; oraz*
	SA-11(7)[2]	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego zweryfikował, czy zakres testów/oceny bezpieczeństwa zapewnia pełne pokrycie wymaganych środków bezpieczeństwa na określonym przez organizację poziomie szczegółowości testów/oceny.*

SA-11(7) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | *WERYFIKACJA ZAKRESU TESTU / OCENA*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące testów bezpieczeństwa przez dewelopera systemu; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; plany testowania i oceny bezpieczeństwa systemu przez dewelopera; wyniki testowania i oceny bezpieczeństwa systemu przez dewelopera; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za testowanie bezpieczeństwa przez dewelopera; deweloperzy systemów; niezależny organ weryfikujący]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu testów i oceny bezpieczeństwa przez deweloperów; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie testów i oceny bezpieczeństwa przez deweloperów].

SA-11(8) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | *DYNAMICZNA ANALIZA KODU*	
	CEL OCENY: *Ustalenie, czy organizacja wymaga od developera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego zastosowania narzędzi dynamicznej analizy kodu w celu identyfikacji typowych błędów oraz udokumentowania wyników analizy.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące testowania bezpieczeństwa przez deweloperów systemów; procedury dotyczące usuwania usterek; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; testowanie bezpieczeństwa przez dewelopera systemu oraz plany oceny; test bezpieczeństwa oraz wyniki oceny; raporty ze śledzenia błędów bezpieczeństwa oraz raporty z działań naprawczych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za testowanie bezpieczeństwa przez dewelopera; personel organizacji odpowiedzialny za zarządzanie konfiguracją; deweloperzy systemów].

SA-11(8)	**TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | *DYNAMICZNA ANALIZA KODU***
	Test: [*wybierz spośród:* Procesy organizacyjne służące monitorowaniu testów i oceny bezpieczeństwa przez deweloperów; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie testów i oceny bezpieczeństwa przez deweloperów].

SA-12	**BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW**	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-12[1]	*określa środki bezpieczeństwa, które należy stosować w celu ochrony przed zagrożeniami łańcuch dostaw systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego; oraz*
	SA-12[2]	*chroni przed zagrożeniami występującymi w łańcuchu dostaw systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego, poprzez zastosowanie zdefiniowanych przez organizację zabezpieczeń w ramach kompleksowej, wielostopniowej strategii bezpieczeństwa informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; procedury dotyczące włączenia wymogów bezpieczeństwa informacji do procesu nabycia; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; wykaz zagrożeń łańcucha dostaw; wykaz środków bezpieczeństwa, jakie należy podjąć w przypadku wystąpienia zagrożeń łańcucha dostaw; dokumentacja cyklu życia systemu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne mające na celu określenie zabezpieczeń oraz ochronę przed zagrożeniami dotyczącymi łańcucha dostaw; zautomatyzowane mechanizmy wspierające i/lub wdrażające zabezpieczenia przed zagrożeniami dotyczącymi łańcucha dostaw].	

<table>
<tr><th colspan="4">SA-12(1) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | STRATEGIE ZAKUPÓW / NARZĘDZIA / METODY</th></tr>
<tr><td></td><td colspan="3">CEL OCENY:
Określić, czy organizacja:</td></tr>
<tr><td></td><td>SA-12(1)[1]</td><td colspan="2">definiuje zastosowanie przy zakupie systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego od dostawców:</td></tr>
<tr><td></td><td></td><td>SA-12(1)[1][a]</td><td>zindywidualizowane strategie nabycia;</td></tr>
<tr><td></td><td></td><td>SA-12(1)[1][b]</td><td>narzędzia kontraktowe;</td></tr>
<tr><td></td><td></td><td>SA-12(1)[1][c]</td><td>metody przeprowadzania zamówień; oraz</td></tr>
<tr><td></td><td>SA-12(1)[2]</td><td colspan="2">stosuje zdefiniowane organizacyjnie, dostosowane do potrzeb klienta, strategie nabywania, narzędzia kontraktowe oraz metody nabywania systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego od dostawców.</td></tr>
<tr><td></td><td colspan="3">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; procedury dotyczące włączenia wymogów bezpieczeństwa informacji do procesu nabycia; procedury dotyczące integracji strategii nabywania, narzędzi kontraktowych, oraz metod pozyskiwania w procesie nabywania; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy zakupu systemów informacyjnych lub usług; zamówienia/warunki zakupu systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego od dostawców; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw].
Test: [wybierz spośród: Procesy organizacyjne służące definiowaniu i stosowaniu spersonalizowanych strategii nabywania, narzędzi kontraktowych oraz metod przeprowadzania zamówień; zautomatyzowane mechanizmy wspierające i/lub wdrażające definiowanie i stosowanie spersonalizowanych strategii nabywania, narzędzi kontraktowych oraz metod przeprowadzania zamówień].</td></tr>
</table>

SA-12(2) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *PRZEGLĄD DOSTAWCÓW*	
	CEL OCENY: *Ustalić, czy organizacja przeprowadza weryfikację dostawcy przed zawarciem umowy dotyczącej nabycia systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; procedury dotyczące włączenia wymogów bezpieczeństwa informacji do procesu nabycia; zapisy przeglądów należytej staranności („due diligence") dostawcy w celu jego weryfikacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne przeprowadzania przeglądów dostawców; zautomatyzowane mechanizmy wspierające i/lub wdrażające przeglądy dostawców].

SA-12(3) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *ZAUFANA WYSYŁKA I MAGAZYNOWANIE*
[Włączone do: SA-12(1)].

SA-12(4)BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *DYWERSYFIKACJA DOSTAWCÓW*
[Włączone do: SA-12(13)].

SA-12(5) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *OGRANICZENIE SZKODY*		
	CEL OCENY: *Określić, czy organizacja:*	
	SA-12(5)[1]	*określa środki bezpieczeństwa, które mają być stosowane w celu ograniczania szkód wyrządzanych przez potencjalnych przeciwników, rozpoznających i atakujących organizacyjny łańcuch dostaw; oraz*

SA-12(5)	**BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *OGRANICZENIE SZKODY***	
	SA-12(5)[2]	*stosuje określone przez organizację zabezpieczenia w celu ograniczenia szkód wyrządzanych przez potencjalnych przeciwników, którzy rozpoznają i atakują organizacyjny łańcuch dostaw.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; polityka zarządzania konfiguracją; procedury dotyczące bezpieczeństwa łańcucha dostaw; procedury dotyczące włączenia wymogów bezpieczeństwa informacji do procesu nabycia; procedury dotyczące konfiguracji podstawowej systemu informacyjnego; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego oraz związana z nią dokumentacja konfiguracyjna; dokumentacja przetargowa; dokumentacja nabycia; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; wykaz środków bezpieczeństwa, które należy podjąć w celu ochrony organizacyjnego łańcucha dostaw przed potencjalnymi zagrożeniami łańcucha dostaw; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące definiowaniu i stosowaniu środków bezpieczeństwa ograniczających szkody wyrządzone przez przeciwników organizacyjnego łańcucha dostaw; zautomatyzowane mechanizmy wspierające i/lub wdrażające zdefiniowanie oraz stosowanie środków bezpieczeństwa w celu ochrony organizacyjnego łańcucha dostaw].	

SA-12(6)	**BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *MINIMALIZACJA CZASU ZAMÓWIENIA***
[Włączone do: SA-12(1)].	

SA-12(7)	**BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *OCENY PRZED WYBOREM / ODBIOREM / AKTUALIZACJĄ***	
	CEL OCENY: *Ustalić, czy organizacja dokonuje oceny systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego przed:*	
	SA-12(7)[1]	*wyborem;*

SA-12(7)	**BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *OCENY PRZED WYBOREM / ODBIOREM / AKTUALIZACJĄ***	
	SA-12(7)[2]	*akceptacją; lub*
	SA-12(7)[3]	*aktualizacją.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; procedury dotyczące włączenia wymogów bezpieczeństwa informacji do procesu nabycia; test bezpieczeństwa i wyniki oceny; wyniki oceny podatności na zagrożenia; wyniki testów penetracyjnych; wyniki organizacyjnego szacowania ryzyka; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące do przeprowadzania ocen przed wyborem, przyjęciem lub aktualizacją systemu; zautomatyzowane mechanizmy wspomagające i/lub wdrażające przeprowadzanie ocen przed wyborem, przyjęciem lub aktualizacją systemu.].	

SA-12(8)	**BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *WYKORZYSTANIE DOSTĘPNYCH ANALIZ WYWIADOWCZYCH***	
	CEL OCENY: *Ustalić, czy organizacja wykorzystuje dostępne analizy wywiadowcze dotyczące:*	
	SA-12(8)[1]	*dostawców systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego; oraz*
	SA-12(8)[2]	*potencjalnych dostawców systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; dokumentacja przetargowa; dokumentacja nabycia; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; rejestry dostępnych analiz wywiadowczych; inne odpowiednie dokumenty lub rejestry].	

SA-12(8)	**BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *WYKORZYSTANIE DOSTĘPNYCH ANALIZ WYWIADOWCZYCH***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z wykorzystaniem dostępnych analiz wszystkich źródeł informacji dotyczących dostawców i potencjalnych dostawców; zautomatyzowane mechanizmy wspierające i/lub wdrażające wykorzystanie dostępnych analiz wszystkich źródeł informacji dotyczących dostawców i potencjalnych dostawców].

SA-12(9)	**BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *BEZPIECZEŃSTWO OPERACYJNE***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-12(9)[1]	*określa środki bezpieczeństwa operacyjnego (OPSEC), które należy stosować zgodnie z rekomendacjami wydawanymi na podstawie przepisów prawa w celu ochrony informacji związanych z łańcuchem dostaw; oraz*
	SA-12(9)[2]	*stosuje określone przez organizację zabezpieczenia operacyjne zgodne z rekomendacjami wydawanymi na podstawie przepisów prawa w celu ochrony informacji związanych z łańcuchem dostaw.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; dokumentacja przetargowa; dokumentacja nabycia; umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; rejestry dostępnych analiz wywiadowczych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące definiowania i stosowania zabezpieczeń OPSEC; zautomatyzowane mechanizmy wspierające i/lub wdrażające definiowanie i stosowanie zabezpieczeń OPSEC].	

SA-12(10) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *OCENA ORYGINALNOŚCI I NIEZMIENNOŚCI*		
	CEL OCENY: *Określić, czy organizacja:*	
	SA-12(10)[1]	*określa środki bezpieczeństwa, które należy stosować w celu potwierdzenia, że nabyty system informacyjny lub jego komponent są autentyczne i nie zostały zmienione; oraz*
	SA-12(10)[2]	*stosuje określone przez organizację środki bezpieczeństwa w celu potwierdzenia, że nabyty system informacyjny lub jego elementy są autentyczne i nie zostały zmienione.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; procedury uwzględniające włączenie wymogów bezpieczeństwa informacji do procesu nabycia; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja dowodowa (w tym odpowiednie konfiguracje) wskazująca, że system informacyjny, komponent systemu, lub usługa systemu informacyjnego są autentyczne i nie zostały zmienione; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące definiowaniu i ocenie zabezpieczeń; zautomatyzowane mechanizmy wspierające i/lub wdrażające definiowanie i ocenę zabezpieczeń].	

SA-12(11) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *TESTOWANIE PENETRACYJNE / ANALIZA ELEMENTÓW, PROCESÓW I WYKONAWCÓW*			
	CEL OCENY: *Określić, czy organizacja:*		
	SA-12(11)[1]	*definiuje łańcuch dostaw:*	
		SA-12(11)[1][a]	*elementów, które mają być analizowane i/lub testowane;*

SA-12(11) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *TESTOWANIE PENETRACYJNE / ANALIZA ELEMENTÓW, PROCESÓW I WYKONAWCÓW*			
		SA-12(11)[1][b]	*procesów, które mają być analizowane i/lub testowane;*
		SA-12(11)[1][c]	*podmiotów, które mają być analizowane i/lub testowane;*
	SA-12(11)[2]	*stosuje jedno lub więcej z poniższych rozwiązań do analizy i/lub testowania zdefiniowanych przez organizację elementów łańcucha dostaw, procesów oraz podmiotów związanych z systemem informacyjnym, komponentem systemu lub usługą systemu informacyjnego:*	
		SA-12(11)[2][a]	*analizę organizacyjną;*
		SA-12(11)[2][b]	*niezależną, zewnętrzną analizę;*
		SA-12(11)[2][c]	*organizacyjne testy penetracyjne; i/lub*
		SA-12(11)[2][d]	*niezależne zewnętrzne testy penetracyjne.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; dowody analizy organizacyjnej, analizy niezależnej strony trzeciej, organizacyjnych testów penetracyjnych i/lub niezależnych testów penetracyjnych strony trzeciej; lista elementów łańcucha dostaw, procesów oraz podmiotów (związanych z systemem informacyjnym, komponentem systemu, lub usługą systemu informacyjnego) będących przedmiotem analizy i/lub testów; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw; personel organizacji odpowiedzialny za analizę i/lub badanie elementów, procesów i podmiotów łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące definiowania i stosowania metod analizy/testowania elementów, procesów i podmiotów łańcucha dostaw; zautomatyzowane mechanizmy wspierające i/lub wdrażające analizę/testowanie elementów, procesów i podmiotów łańcucha dostaw].		

SA-12(12) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *UMOWY MIĘDZYORGANIZACYJNE*		
	CEL OCENY: *Ustalić, czy organizacja podpisuje z podmiotami uczestniczącymi w łańcuchu dostaw systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego:*	
	SA-12(12)[1]	*umowy międzyorganizacyjne; oraz*
	SA-12(12)[2]	*procedury międzyorganizacyjne.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; umowy praz procedury międzyorganizacyjne; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne tworzenia umów oraz procedur międzyorganizacyjnych z podmiotami łańcucha dostaw].	

SA-12(13) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *KOMPONENTY KRYTYCZNE SYSTEMU* INFORMACYJNEGO		
	CEL OCENY: *Określić, czy organizacja:*	
	SA-12(13)[1]	*definiuje komponenty krytyczne s sytemu informacyjnego w których mają być zastosowane środki bezpieczeństwa w celu zapewnienia prawidłowej dostawy takich komponentów;*
	SA-12(13)[2]	*definiuje środki bezpieczeństwa, które należy zastosować w celu zapewnienia właściwego dostarczania zdefiniowanych przez organizację elementów krytycznych systemu informacyjnego; oraz*
	SA-12(13)[3]	*stosuje określone organizacyjnie zabezpieczenia w celu zapewnienia odpowiedniego zaopatrzenia w określone organizacyjnie komponenty krytyczne systemu informacyjnego.*

SA-12(13) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *KOMPONENTY KRYTYCZNE SYSTEMU* INFORMACYJNEGO	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; spis z natury krytycznych elementów systemu informacyjnego; spis krytycznych elementów systemu informacyjnego; wykaz środków bezpieczeństwa zapewniających właściwe zaopatrzenie w krytyczne elementy systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące definiowania i stosowania środków bezpieczeństwa w celu zapewnienia odpowiedniej dostawy komponentów krytycznego systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające środki bezpieczeństwa, które zapewniają odpowiednią dostawę komponentów krytycznego systemu informacyjnego].

SA-12(14) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *IDENTYFIKACJA I ŚLEDZENIE*			
	CEL OCENY: *Określić, czy organizacja:*		
	SA-12(14)[1]	*definiuje, ustanawia i zachowuje unikalną identyfikację:*	
		SA-12(14)[1][a]	*elementów łańcucha dostaw;*
		SA-12(14)[1][b]	*procesów w łańcuchu dostaw;*
		SA-12(14)[1][c]	*uczestników łańcucha dostaw; oraz*
	SA-12(14)[2]	*ustanawia i zachowuje unikalną identyfikację zdefiniowanych przez organizację elementów łańcucha dostaw, procesów i podmiotów dla systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; procedury dotyczące włączenia wymogów bezpieczeństwa informacji do procesu nabycia; wykaz elementów,		

SA-12(14) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *IDENTYFIKACJA I ŚLEDZENIE*	
	procesów i podmiotów łańcucha dostaw (związanych z systemem informacyjnym, komponentem systemu lub usługą systemu informacyjnego) wymagających wdrożenia procesów jednoznacznej identyfikacji, procedur, narzędzi, sprzętu, mechanizmów, technik lub konfiguracji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw; ; personel organizacji odpowiedzialny za ustanowienie i utrzymanie unikalnej identyfikacji elementów, procesów i podmiotów łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące definiowaniu, ustanawianiu i zachowywaniu jednoznacznej identyfikacji elementów, procesów i podmiotów łańcucha dostaw; zautomatyzowane mechanizmy wspierające lub wdrażające definiowanie, ustanawianie i zachowywanie jednoznacznej identyfikacji elementów, procesów i podmiotów łańcucha dostaw].

SA-12(15) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | *MECHANIZMY ADRESOWANIA SŁABYCH STRON LUB WAD*	
	CEL OCENY: *Ustalenie, czy organizacja ustanawia proces mający na celu usunięcie słabych stron lub wad elementów łańcucha dostaw zidentyfikowanych podczas niezależnych lub organizacyjnych ocen tych elementów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące bezpieczeństwa łańcucha dostaw; procedury dotyczące podatności lub wad elementów łańcucha dostaw; wyniki niezależnych lub organizacyjnych ocen zabezpieczeń i procesów w łańcuchu dostaw; umowy nabycia, umowa gwarancji świadczenia usług (SLA); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za bezpieczeństwo łańcucha dostaw]. **Test**: [*wybierz spośród:* Procesy organizacyjne mające na celu wyeliminowanie słabych stron lub wad elementów łańcucha dostaw; zautomatyzowane mechanizmy wspierające lub wdrażające eliminowanie słabości lub wad elementów łańcucha dostaw].

SA-13	**WIARYGODNOŚĆ**		
	CEL OCENY: *Określić, czy organizacja:*		
	SA-13(a)	**SA-13(a)[1]**	*definiuje system informacyjny, komponent systemu lub usługę systemu informacyjnego, dla których ma być opisana wymagana wiarygodność;*
		SA-13(a)[2]	*opisuje wiarygodność wymaganą w zdefiniowanym przez organizację systemie informacyjnym, komponencie systemu informacyjnego lub usłudze systemu informacyjnego wspierającej jego krytyczne funkcje misyjne/biznesowe;*
	SA-13(b)	**SA-13(b)[1]**	*definiuje nakładkę poświadczającą, która ma być wdrożona w celu osiągnięcia takiej wiarygodności; oraz*
		SA-13(b)[2]	*wdraża zdefiniowaną przez organizację nakładkę poświadczającą, pozwalającą na osiągnięcie takiej wiarygodności.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące wymagań w zakresie wiarygodności systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; Dokumentacja/wyniki kategoryzacji bezpieczeństwa; pakiet autoryzacji bezpieczeństwa systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; osoba autoryzująca].		

SA-14	**ANALIZA KRYTYCZNOŚCI**	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-14[1]	*definiuje systemy informacyjne, komponenty systemów informacyjnych lub usługi systemów informacyjnych wymagające analizy krytyczności w celu określenia krytycznych komponentów i funkcji systemu informacyjnego;*

SA-14	**ANALIZA KRYTYCZNOŚCI**	
	SA-14[2]	*definiuje punkty decyzyjne w cyklu życia systemu, w których ma być przeprowadzona analiza krytyczności dla zdefiniowanych przez organizację systemów informacyjnych, komponentów systemów informacyjnych lub usług systemów informacyjnych; oraz*
	SA-14[3]	*identyfikuje krytyczne części składowe i funkcje systemu informacyjnego poprzez przeprowadzenie analizy krytyczności dla zdefiniowanych przez organizację systemów informacyjnych, części składowych systemu informacyjnego lub usług systemów informacyjnych w zdefiniowanych przez organizację punktach cyklu życia systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące wymagań w zakresie analizy krytyczności systemów informacyjnych; plan bezpieczeństwa; plan awaryjny; wykaz systemów informacyjnych, elementów systemu informacyjnego lub usług systemu informacyjnego wymagających analizy krytyczności; wykaz krytycznych elementów systemu informacyjnego i funkcji zidentyfikowanych w wyniku analizy krytyczności; dokumentacja analizy krytyczności; dokumentacja analizy wpływu na działalność gospodarczą; dokumentacja cyklu życia systemu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za przeprowadzanie analizy krytyczności systemu informacyjnego].	

SA-14(1)	**ANALIZA KRYTYCZNOŚCI | *KRYTYCZNE KOMPONENTY POZBAWIONE REALNYCH ALTERNATYWNYCH ŹRÓDEŁ ZAOPATRZENIA***
[Włączone do: SA-20].	

SA-15	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA**		
	CEL OCENY: *Określić, czy organizacja:*		
	SA-15(a)	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego postępował zgodnie z udokumentowanym procesem rozwoju, który:*	
		SA-15(a)(1)	*jednoznacznie odnosi się do wymogów bezpieczeństwa;*

SA-15	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA**			
		SA-15(a)(2)	*określa standardy i narzędzia wykorzystywane w procesie rozwoju;*	
		SA-15(a)(3)	**SA-15(a)(3)[1]**	*dokumentuje określone opcje narzędzi wykorzystywane w procesie rozwoju;*
			SA-15(a)(3)[2]	*dokumentuje określone konfiguracje narzędzi używanych w procesie rozwoju;*
		SA-15(a)(4)	**SA-15(a)(4)[1]**	*dokumentuje zmiany w procesie i/lub narzędziach użytych w procesie rozwoju;*
			SA-15(a)(4)[2]	*zarządza zmianami w procesie i/lub narzędziami wykorzystywanymi w procesie rozwoju;*
			SA-15(a)(4)[3]	*zapewnia integralność zmian w procesie i/lub narzędziach użytych w procesie rozwoju;*
	SA-15(b)	**SA-15(b)[1]**	*definiuje częstotliwość przeglądów procesu rozwoju, standardów, narzędzi oraz opcji/konfiguracji narzędzi;*	
		SA-15(b)[2]	*definiuje wymagania bezpieczeństwa, które musi spełniać proces, standardy, narzędzia oraz wybrane i zastosowane opcje/konfiguracje narzędziowe; oraz*	
		SA-15(b)[3]	**SA-15(b)[3][a]**	*dokonuje przeglądu procesu rozwoju z częstotliwością zdefiniowaną przez organizację, w celu określenia, czy wybrany i zastosowany proces spełnia wymagania bezpieczeństwa zdefiniowane przez organizację;*
			SA-15(b)[3][b]	*dokonuje przeglądu standardów rozwoju z częstotliwością określoną przez organizację w celu ustalenia, czy wybrane i zastosowane standardy spełniają określone przez organizację wymagania bezpieczeństwa;*

SA-15	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA**			
			SA-15(b)[3][c]	*dokonuje przeglądu narzędzi rozwojowych z częstotliwością określoną przez organizację w celu ustalenia, czy wybrane i zastosowane narzędzia spełniają określone przez organizację wymagania w zakresie bezpieczeństwa; oraz*
			SA-15(b)[3][d]	*przegląda opcje/konfiguracje narzędzi programistycznych z częstotliwością zdefiniowaną przez organizację w celu określenia, czy wybrane i zastosowane opcje/konfiguracje narzędzi spełniają wymagania bezpieczeństwa zdefiniowane przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; procedury dotyczące integracji wymogów bezpieczeństwa w procesie rozwoju; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja deweloperska zawierająca wykaz opcji narzędzi/przewodników konfiguracyjnych; rejestry zarządzania konfiguracją; rejestry zabezpieczeń zmian; zapisy kontroli konfiguracji; udokumentowane przeglądy procesu rozwoju, standardów, narzędzi oraz opcji/konfiguracji narzędzi; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu].			

SA-15(1)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *METRYKI JAKOŚCI***		
	CEL OCENY: *Określić, czy organizacja:*		
	SA-15(1)(a)	*wymaga od dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego zdefiniowania metryki jakości na początku procesu rozwoju;*	
	SA-15(1)(b)	**SA-15(1)(b)[1]**	*definiuje częstotliwość przedstawiania potwierdzenia spełnienia metryki jakości;*

SA-15(1)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *METRYKI JAKOŚCI***			
		SA-15(1)(b)[2]	*definiuje etapy przeglądu programu zdefiniowane przez organizację w celu dostarczenia dowodów na spełnienie wymogów metryki jakości;*	
		SA-15(1)(b)[3]	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego dostarczył dowody potwierdzające spełnienie wymogów metryki jakości jednego lub kilku z poniższych elementów:*	
			SA-15(1)(b)[3][a]	*z częstotliwością określoną przez organizację;*
			SA-15(1)(b)[3][b]	*zgodnie ze zdefiniowanymi przez organizację etapami przeglądu; i/lub*
			SA-15(1)(b)[3][c]	*po dostarczeniu systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; procedura dotycząca włączenia wymogów bezpieczeństwa do procesów zakupu; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; wykaz wskaźników jakości; dokumentacja potwierdzająca spełnienie wymogów wskaźników jakości; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu].			

SA-15(2)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *NARZĘDZIA ŚLEDZENIA BEZPIECZEŃSTWA***
	CEL OCENY: *Określić, czy organizacja wymaga, aby deweloper systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego wybrał i zastosował narzędzie do śledzenia bezpieczeństwa do wykorzystania w procesie rozwoju.*

SA-15(2)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *NARZĘDZIA ŚLEDZENIA BEZPIECZEŃSTWA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; procedura dotycząca włączenia wymogów bezpieczeństwa do procesów zakupu; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; wykaz wskaźników jakości; dokumentacja potwierdzająca spełnienie wymogów wskaźników jakości; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu].

SA-15(3)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *ANALIZA KRYTYCZNOŚCI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-15(3)[1]	*określa zakres analizy krytyczności, którą ma wykonać deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego;*
	SA-15(3)[2]	*definiuje szczegółowość analizy krytyczności wykonywanej przez dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego;*
	SA-15(3)[3]	*definiuje punkty decyzyjne w cyklu życia systemu, w których ma być przeprowadzona analiza krytyczności systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego; oraz*
	SA-15(3)[4]	*wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego przeprowadzenia analizy krytyczności w zdefiniowanym przez organizację zakresie/szczegółowości oraz w zdefiniowanych przez organizację punktach decyzyjnych w cyklu życia systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; procedury dotyczące wymagań w zakresie analizy krytyczności systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego; dokumentacja	

SA-15(3)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *ANALIZA KRYTYCZNOŚCI***
	przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja analizy krytyczności; dokumentacja analizy wpływu na działalność biznesową; dokumentacja cyklu życia oprogramowania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za przeprowadzanie analizy krytyczności; deweloper systemu]. **Test**: [*wybierz spośród:* Procesy organizacyjne do przeprowadzania analizy krytyczności; zautomatyzowane mechanizmy wspierające i/lub wdrażające analizę krytyczności].

SA-15(4)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *MODELOWANIE ZAGROŻEŃ / ANALIZA PODATNOŚCI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-15(4)[1]	*definiuje zakres modelowania zagrożeń i analizy podatności, które mają być wykonywane przez deweloperów na potrzeby systemu informacyjnego;*
	SA-15(4)[2]	*definiuje szczegółowość modelowania zagrożeń i analizy podatności, które mają być wykonywane przez deweloperów na potrzeby systemu informacyjnego;*
	SA-15(4)[3]	*definiuje informacje dotyczące wpływu, środowiska działania, znanych lub zakładanych zagrożeń oraz dopuszczalnych poziomów ryzyka do wykorzystania w modelowaniu zagrożeń i analizie podatności;*
	SA-15(4)[4]	*definiuje narzędzia i metody do zastosowania w modelowaniu zagrożeń i analizie podatności;*
	SA-15(4)[5]	*definiuje kryteria akceptacji materiału dowodowego powstającego w wyniku modelowania zagrożeń i analizy podatności na zagrożenia;*
	SA-15(4)[6]	*wymaga, aby deweloperzy przeprowadzali modelowanie zagrożeń i analizę podatności systemu informacyjnego w określonym przez organizację zakresie/szczegółowości:*

SA-15(4)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *MODELOWANIE ZAGROŻEŃ / ANALIZA PODATNOŚCI***		
		SA-15(4)[6](a)	*wykorzystując zdefiniowane przez organizację informacje dotyczące wpływu, środowiska działania, znanych lub zakładanych zagrożeń oraz dopuszczalnych poziomów ryzyka;*
		SA-15(4)[6](b)	*stosując definiowane przez organizację narzędzia i metody; oraz*
		SA-15(4)[6](c)	*przedstawiająca dowody, które spełniają określone przez organizację kryteria akceptacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja modelowania zagrożeń; wyniki analizy podatności; szacowanie ryzyka organizacyjnego; kryteria akceptacji dowodów uzyskanych z modelowania zagrożeń oraz analizy podatności; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Procesy organizacyjne do przeprowadzania modelowania zagrożeń rozwojowych oraz analizy podatności; zautomatyzowane mechanizmy wspierające i/lub wdrażające modelowanie zagrożeń rozwojowych oraz analizę podatności].		

SA-15(5)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *OGRANICZENIE PŁASZCZYZNY ATAKU***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-15(5)[1]	*określa progi, do których należy zmniejszyć powierzchnie ataku; oraz*
	SA-15(5)[2]	*wymaga od dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego zmniejszenia powierzchni ataku do zdefiniowanych przez organizację progów.*

SA-15(5)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *OGRANICZENIE PŁASZCZYZNY ATAKU***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; procedury dotyczące ograniczania płaszczyzny ataku; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego lub usługi systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; schemat sieciowy; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja ustanowienie/wymuszenie zdefiniowanych przez organizację progów zmniejszenia powierzchni ataku; wykaz portów, protokołów, funkcji i usług podlegających ograniczeniom; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za ograniczanie powierzchni ataku; deweloper systemu]. **Test**: [*wybierz spośród:* Procesy organizacyjne mające na celu określenie progów ograniczenie płaszczyzny ataku].

SA-15(6)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *CIĄGŁE DOSKONALENIE***
	CEL OCENY: *Ustalić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego wdrożenia przejrzystego mechanizmu ciągłego doskonalenia procesu rozwoju.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; cele jakościowe oraz metryki doskonalenia procesu rozwoju systemu; ocena bezpieczeństwa i/lub przeglądy kontroli jakości procesu rozwoju systemu; plany działania oraz etapy doskonalenia procesu rozwoju systemu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu].

SA-15(7)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *AUTOMATYCZNA ANALIZA WRAŻLIWOŚCI***		
	CEL OCENY: *Określić, czy organizacja:*		
	SA-15(7)(a)	**SA-15(7)(a)[1]**	*definiuje narzędzia, które mają być wykorzystywane do zautomatyzowanej analizy podatności systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego;*
		SA-15(7)(a)[2]	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub serwisu systemu informacyjnego przeprowadził automatyczną analizę podatności przy użyciu narzędzi zdefiniowanych przez organizację;*
	SA-15(7)(b)	*wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego określenia potencjalnego wykorzystania odkrytych podatności;*	
	SA-15(7)(c)	*wymaga, aby deweloper systemu informacyjnego, komponent systemu lub usługi systemu informacyjnego określił potencjalne sposoby ograniczania ryzyka wystąpienia wykrytych podatności;*	
	SA-15(7)(d)	**SA-15(7)(d)[1]**	*określa personel lub role, którym mają zostać dostarczone uzyskane rezultaty i wyniki analizy; oraz*
		SA-15(7)(d)[2]	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego dostarczył uzyskane dane wyjściowe oraz wyniki analizy do zdefiniowanego przez organizację personelu lub ról.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; narzędzia do analizy podatności oraz towarzysząca im dokumentacja; raporty szacowanie ryzyka; wyniki analizy podatności; raporty na temat ograniczania podatności; dokumentacja dotycząca strategii ograniczania ryzyka; inne odpowiednie dokumenty lub rejestry].		

SA-15(7)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *AUTOMATYCZNA ANALIZA WRAŻLIWOŚCI***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji przeprowadzający automatyczną analizę podatności na zagrożenia występujące w systemie informacyjnym]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące analizy podatności opracowywanych systemów informacyjnych, komponentów systemu lub usług systemów informacyjnych; zautomatyzowane mechanizmy wspierające i/lub wdrażające analizę podatności opracowywanych systemów informacyjnych, komponentów systemu lub usług systemów informacyjnych].

SA-15(8)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *PONOWNIE UŻYCIE INFORMACJI O ZAGROŻENIACH / WRAŻLIWOŚCI***
	CEL OCENY: *Określenie, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego wykorzystania modelowania zagrożeń i analiz podatności z adekwatnych systemów, komponentów lub usług, w celu informowania o bieżącym procesie rozwoju zagrożeń.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; modelowanie zagrożeń i analiza podatności z analogicznych systemów informacyjnych, komponentów systemu lub usług systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu].

SA-15(9)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *KREATYWNE WYKORZYSTANIE DANYCH***
	CEL OCENY: *Ustalić, czy organizacja, w odniesieniu do systemu informacyjnego, komponentu systemu, oraz usługi systemu informacyjnego:*

SA-15(9)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *KREATYWNE WYKORZYSTANIE DANYCH***	
	SA-15(9)[1]	*zezwala na wykorzystanie rzeczywistych danych w środowiskach rozwojowych i testowych;*
	SA-15(9)[2]	*dokumentuje wykorzystanie rzeczywistych danych w środowiskach rozwojowych i testowych; oraz*
	SA-15(9)[3]	*kontroluje wykorzystanie rzeczywistych danych w środowiskach rozwojowych i testowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja zezwalająca na wykorzystanie danych rzeczywistych w środowiskach rozwojowych i testowych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące zatwierdzania, dokumentowania i kontroli wykorzystania rzeczywistych danych w środowiskach rozwojowych i testowych; zautomatyzowane mechanizmy wspierające i/lub wdrażające zatwierdzanie, dokumentowanie i kontrolę wykorzystania rzeczywistych danych w środowiskach rozwojowych i testowych].	

SA-15(10)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *PLAN REAGOWANIA NA INCYDENTY***
	CEL OCENY: *Ustalić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego opracowania planu reagowania na incydenty.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego lub usług; dokumentacja zakupowa;

SA-15(10)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *PLAN REAGOWANIA NA INCYDENTY***
	dokumentacja przetargowa, umowa gwarancji świadczenia usług (SLA); plan reagowania na incydenty deweloperskie; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu].

SA-15(11)	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA | *SYSTEM ARCHIWIZACJI INFORMACJI / KOMPONENTY***
	CEL OCENY: *Określenie, czy organizacja wymaga, aby deweloper systemu informacyjnego lub komponentu systemu zarchiwizował system lub komponent, który ma być udostępniony lub dostarczony wraz z odpowiednimi dokumentami potwierdzającymi końcowy przegląd bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące procesu rozwoju, stosowanych standardów i narzędzi; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego lub usług; dokumentacja zakupowa; dokumentacja przetargowa, umowa gwarancji świadczenia usług (SLA); plan reagowania na incydenty deweloperskie; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu].

SA-16	**SZKOLENIA PROWADZONE PRZEZ DEWELOPERA**	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-16[1]	*definiuje szkolenie, które ma być przeprowadzone przez dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego; oraz*

SA-16	**SZKOLENIA PROWADZONE PRZEZ DEWELOPERA**	
	SA-16[2]	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego przeprowadził szkolenie w zakresie prawidłowego użytkowania i obsługi wdrożonych funkcji, kontroli i/lub mechanizmów bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące szkolenia prowadzonego przez dewelopera; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; szkolenia prowadzone przez dewelopera materials; rejestry szkoleniowe; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo systemu informacyjnego; deweloper systemu; organizacyjni lub zewnętrzni deweloperzy odpowiedzialni za szkolenia dotyczące systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego].	

SA-17	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA**		
	CEL OCENY: *Określić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego stworzenia specyfikacji projektowej oraz architektury bezpieczeństwa, która to specyfikacja:*		
	SA-17(a)	*jest spójna z architekturą bezpieczeństwa organizacji, która jest tworzona w ramach struktury organizacyjnej organizacji oraz stanowi jej integralną część;*	
	SA-17(b)	*dokładnie i szczegółowo opisuje:*	
		SA-17(b)[1]	*wymagane funkcje bezpieczeństwa;*
		SA-17(b)[2]	*podział środków bezpieczeństwa na komponenty fizyczne i logiczne; oraz*
	SA-17(c)	*określa sposób, w jaki poszczególne funkcje, mechanizmy i usługi w zakresie bezpieczeństwa współpracują ze sobą w celu zapewnienia wymaganych zdolności w zakresie bezpieczeństwa oraz jednolitego podejścia do ochrony.*	

SA-17	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; zasady architektury organizacyjnej; procedury dotyczące architektury bezpieczeństwa dewelopera i specyfikacji projektowej systemu informacyjnego; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; specyfikacja projektowa oraz dokumentacja architektury bezpieczeństwa systemu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za architekturę bezpieczeństwa i projektowanie].

SA-17(1)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *MODEL POLITYKI***		
	CEL OCENY: *Określić, czy organizacja:*		
	SA-17(1)(a)	**SA-17(1)(a)[1]**	*definiuje elementy polityki bezpieczeństwa organizacyjnego, które mają być egzekwowane w ramach modelu polityki, opracowanego przez dewelopera, jako integralna część procesu rozwoju systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego;*
		SA-17(1)(a)[2]	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego opracował, jako integralną część procesu rozwoju, modelową politykę opisującą określone przez organizację elementy polityki bezpieczeństwa organizacyjnego, które mają być egzekwowane; oraz*
	SA-17(1)(b)	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego wykazał, że modelowa polityka jest wewnętrznie spójna oraz wystarczająca do egzekwowania określonych elementów polityki bezpieczeństwa organizacji w momencie jej wdrożenia.*	

SA-17(1)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *MODEL POLITYKI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; zasady architektury organizacyjnej; procedury dotyczące architektury bezpieczeństwa dewelopera i specyfikacji projektowej systemu informacyjnego; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; specyfikacja projektowa oraz dokumentacja architektury bezpieczeństwa systemu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za architekturę bezpieczeństwa i projektowanie].

SA-17(2)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *BAZOWE ELEMENTY BEZPIECZEŃSTWA***		
	CEL OCENY: *Ustalić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego:*		
	SA-17(2)(a)	**SA-17(2)(a)[1]**	*zdefiniowania sprzętu mającego znaczenie dla bezpieczeństwa;*
		SA-17(2)(a)[2]	*zdefiniowania oprogramowania mającego znaczenie dla bezpieczeństwa;*
		SA-17(2)(a)[3]	*zdefiniowania oprogramowania układowego mającego znaczenie dla bezpieczeństwa; oraz*
	SA-17(2)(b)	*przedstawienia uzasadnienia, że zdefiniowany sprzęt, oprogramowanie i programowanie układowe istotne dla bezpieczeństwa są kompletne.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; zasady architektury organizacyjnej; procedury dotyczące architektury bezpieczeństwa dewelopera i specyfikacji projektowej systemu informacyjnego; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; wykaz sprzętu, aplikacji i oprogramowania układowego mających		

SA-17(2)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *BAZOWE ELEMENTY BEZPIECZEŃSTWA***
	znaczenie dla bezpieczeństwa; udokumentowane uzasadnienie kompletności dotyczące specyfikacji sprzętu, aplikacji i oprogramowania układowego mających znaczenie dla bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów; personel organizacji odpowiedzialny za architekturę bezpieczeństwa i projektowanie].

SA-17(3)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *FORMALNA SPECYFIKACJA***	
	CEL OCENY: *Ustalić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego:*	
	SA-17(3)(a)	*opracowania, jako integralnej części procesu rozwoju, formalnej specyfikacji najwyższego poziomu, które określa interfejsy sprzętowe, aplikacje i oprogramowanie układowe istotne z punktu widzenia bezpieczeństwa, powiązane merytorycznie z:*
	SA-17(3)(a)[1]	*wyjątkami;*
	SA-17(3)(a)[2]	*komunikatami o błędach;*
	SA-17(3)(a)[3]	*skutkami;*
	SA-17(3)(b)	*wykazania za pomocą możliwego do przeprowadzenia dowodu, a w razie potrzeby dodatkowo z nieformalną prezentacją, że istniejąca specyfikacja najwyższego poziomu jest zgodna z formalnym modelem polityki;*
	SA-17(3)(c)	*wykazania poprzez nieformalną prezentację, że formalna specyfikacja najwyższego poziomu obejmuje interfejsy z istotnym dla bezpieczeństwa sprzętem, aplikacjami, oprogramowaniem układowym;*
	SA-17(3)(d)	*wykazania, że formalna specyfikacja najwyższego poziomu jest dokładnym opisem zaimplementowanego, związanego z bezpieczeństwem sprzętu, aplikacji i oprogramowania układowego; oraz*

SA-17(3)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *FORMALNA SPECYFIKACJA***	
	SA-17(3)(e)	*opisania mechanizmów związanych z bezpieczeństwem sprzętu, aplikacji i oprogramowania układowego, które nie zostały uwzględnione w formalnej specyfikacji najwyższego poziomu, ale ściśle dotyczą sprzętu, aplikacji i oprogramowania układowego związanego z bezpieczeństwem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; polityka w zakresie architektury organizacyjnej; oficjalny model polityki; procedury dotyczące architektury bezpieczeństwa dewelopera i specyfikacji projektu systemu informacyjnego; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; formalna dokumentacja techniczna najwyższego poziomu; architektura bezpieczeństwa systemu informacyjnego oraz dokumentacja projektowa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja opisująca sprzęt, oprogramowanie i mechanizmy oprogramowania układowego istotne z punktu widzenia bezpieczeństwa, które nie zostały uwzględnione w formalnej dokumentacji specyfikacji najwyższego poziomu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za architekturę bezpieczeństwa i projektowanie].	

SA-17(4)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *NIEFORMALNE SPECYFIKACJE***		
	CEL OCENY: *Ustalić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego:*		
	SA-17(4)(a)	*opracowania, jako integralnej części procesu rozwoju, nieformalnej, opisowej specyfikacji najwyższego poziomu, która określa interfejsy sprzętowe, aplikacje i oprogramowanie układowe istotne z punktu widzenia bezpieczeństwa, powiązane merytorycznie z:*	
		SA-17(4)(a)[1]	*wyjątkami;*
		SA-17(4)(a)[2]	*komunikatami o błędach;*

SA-17(4)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *NIEFORMALNE SPECYFIKACJE***		
		SA-17(4)(a)[3]	*skutkami;*
	SA-17(4)(b)	*wykazania za pomocą nieformalnej prezentacji i/lub, w miarę możliwości formalnych, przekonujących argumentów, że opisowa specyfikacja najwyższego poziomu jest zgodna z polityką modelową;*	
	SA-17(4)(c)	*wykazania, poprzez nieformalną prezentację, że opisowa specyfikacja najwyższego poziomu kompleksowo obejmuje interfejsy sprzętowe, aplikacje i oprogramowanie układowe mające istotne znaczenie dla bezpieczeństwa;*	
	SA-17(4)(d)	*wykazania, że opisowa specyfikacja najwyższego poziomu stanowi dokładny opis interfejsów sprzętowych, aplikacji i oprogramowania układowego, mających istotne znaczenie dla bezpieczeństwa; oraz*	
	SA-17(4)(e)	*opisania mechanizmów związanych ze sprzętem, aplikacjami i oprogramowaniem układowym istotnych z punktu widzenia bezpieczeństwa, które nie zostały uwzględnione w opisowej specyfikacji najwyższego poziomu, ale są ściśle związane z tym sprzętem, aplikacjami i oprogramowaniem układowym, istotnych z punktu widzenia bezpieczeństwa.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; polityka w zakresie architektury organizacyjnej; oficjalny model polityki; procedury dotyczące architektury bezpieczeństwa dewelopera i specyfikacji projektu systemu informacyjnego; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; nieformalna opisowa dokumentacja specyfikacji najwyższego poziomu; architektura bezpieczeństwa systemu informacyjnego oraz dokumentacja projektowa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja opisująca sprzęt, aplikacje i oprogramowanie układowe mające znaczenie dla bezpieczeństwa, nieuwzględnione w nieformalnej, opisowej dokumentacji technicznej najwyższego poziomu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za architekturę bezpieczeństwa i projektowanie].		

SA-17(5)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *PROSTY KONCEPCYJNIE PLAN***	
	CEL OCENY: *Ustalić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu, lub usługi systemu informacyjnego, aby:*	
	SA-17(5)(a)	*projektował i konstruował istotny dla bezpieczeństwa sprzęt, aplikacje i oprogramowanie układowe w celu wykorzystania kompletnego, koncepcyjnie prostego mechanizmu ochronnego z precyzyjnie zdefiniowaną semantyką, oraz*
	SA-17(5)(b)	*ustrukturyzował wewnętrznie istotny dla bezpieczeństwa sprzęt, aplikacje i oprogramowanie układowe, ze szczególnym uwzględnieniem tego mechanizmu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; zasady architektury organizacyjnej; procedury dotyczące architektury bezpieczeństwa dewelopera i specyfikacji projektowej systemu informacyjnego; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja architektury bezpieczeństwa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dokumentacja deweloperska opisująca projekt oraz strukturę sprzętu, oprogramowania oraz oprogramowania układowego, istotnych z punktu widzenia bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za architekturę bezpieczeństwa i projektowanie].	

SA-17(6)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *STRUKTURA DO TESTOWANIA***
	CEL OCENY: *Określić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego, ustrukturyzowania sprzętu, aplikacji i oprogramowania sprzętowego mającego znaczenie dla bezpieczeństwa, w celu usprawnienia testowania.*

SA-17(6)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *STRUKTURA DO TESTOWANIA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; zasady architektury organizacyjnej; procedury dotyczące architektury bezpieczeństwa dewelopera i specyfikacji projektowej systemu informacyjnego; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja architektury bezpieczeństwa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dokumentacja deweloperska opisująca projekt oraz strukturę sprzętu, oprogramowania oraz oprogramowania układowego, dokumentacja deweloperska opisująca projekt i strukturę sprzętu, aplikacji i oprogramowania układowego istotnych z punktu widzenia bezpieczeństwa, w celu usprawnienia testowania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za architekturę bezpieczeństwa i projektowanie].

SA-17(7)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *STRUKTURA DLA NAJNIŻSZYCH UPRAWNIEŃ***
	CEL OCENY: *Określić, czy organizacja wymaga od dewelopera systemu informacyjnego, komponentu systemowego lub usługi systemu informacyjnego, strukturyzacji sprzętu, oprogramowania oraz oprogramowania układowego, w celu usprawnienia kontroli dostępu zgodnie z zasadą wiedzy koniecznej (najniższych uprawnień).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; zasady architektury organizacyjnej; procedury dotyczące architektury bezpieczeństwa dewelopera i specyfikacji projektowej systemu informacyjnego; dokumentacja przetargowa; dokumentacja nabycia; umowa gwarancji świadczenia usług (SLA); umowy nabycia systemu informacyjnego, komponentu systemu lub usług systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja architektury bezpieczeństwa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dokumentacja deweloperska opisująca projekt i strukturę sprzętu, aplikacji i oprogramowania układowego, istotnych z punktu widzenia bezpieczeństwa,

SA-17(7)	**ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | *STRUKTURA DLA NAJNIŻSZYCH UPRAWNIEŃ***
	w celu usprawnienia kontroli dostępu stosując zasadę najniższych uprawnień; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za architekturę bezpieczeństwa i projektowanie].

SA-18	**ODPORNOŚĆ NA SABOTAŻ I *WYKRYWANIE MANIPULACJI***
	CEL OCENY: *Ustalić, czy organizacja wdraża program ochrony przed manipulacją systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące odporności na sabotaż i wykrywanie manipulacji; dokumentacja oprogramowania ochrony przed manipulacją; dokumentacja narzędzi i technik ochrony przed manipulacją; dokumentacja narzędzi i technik ochrony przed manipulacją i wykrywania manipulacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za program ochrony przed manipulacją]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z wdrażaniem programu ochrony przed manipulacją; zautomatyzowane mechanizmy wspierające i/lub wdrażające program ochrony przed manipulacją].

SA-18(1)	**ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI | *WIELOFAZOWOŚĆ CYKLU ŻYCIA SYSTEMU***	
	CEL OCENY: *Ustalenie, czy organizacja stosuje technologie i techniki zapobiegania manipulacjom podczas wielu faz cyklu życia systemu (SDLC), w tym:*	
	SA-18(1)[1]	*projektowania;*
	SA-18(1)[2]	*rozwoju;*

SA-18(1)	**ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI | *WIELOFAZOWOŚĆ CYKLU ŻYCIA SYSTEMU***	
	SA-18(1)[3]	*integracji;*
	SA-18(1)[4]	*operacji; oraz*
	SA-18(1)[5]	*utrzymania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące odporności na sabotaż i wykrywanie manipulacji; dokumentacja programów ochrony przed manipulacją; dokumentacja narzędzi i technik ochrony przed manipulacją; dokumentacja narzędzi (technologii) i technik ochrony przed manipulacją; dokumentacja cyklu życia systemu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za program ochrony przed manipulacją; personel organizacji odpowiedzialny za SDLC]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące stosowania technologii zabezpieczających przed nieuprawnionym manipulowaniem; zautomatyzowane mechanizmy wspierające i/lub wdrażające technologie zabezpieczające przed nieuprawnionym manipulowaniem].	

SA-18(2)	**ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI | *KONTROLA SYSTEMÓW* INFORMACYJNYCH, *KOMPONENTÓW LUB URZĄDZEŃ***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-18(2)[1]	*definiuje systemy informacyjne, elementy systemu lub urządzenia, które mają być kontrolowane w celu wykrycia manipulacji;*
	SA-18(2)[2]	*określa częstotliwość kontroli zdefiniowanych przez organizację systemów informacyjnych, elementów systemu lub urządzeń służących do wykrywania manipulacji;*
	SA-18(2)[3]	*definiuje wskazówki dotyczące potrzeby przeprowadzania inspekcji zdefiniowanych przez organizację systemów informacyjnych, komponentów systemu lub urządzeń, w celu wykrycia nieuprawnionych manipulacji;*

SA-18(2)	**ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI | *KONTROLA SYSTEMÓW* INFORMACYJNYCH, *KOMPONENTÓW LUB URZĄDZEŃ***		
	SA-18(2)[4]	*dokonuje inspekcji zdefiniowanych przez organizację systemów informacyjnych, komponentów systemu lub urządzeń w celu wykrycia nieuprawnionych manipulacji, wybierając jedną lub więcej z poniższych opcji:*	
		SA-18(2)[4][a]	*wyrywkowo;*
		SA-18(2)[4][b]	*z częstotliwością określoną przez organizację; i/lub*
		SA-18(2)[4][c]	*po zdefiniowanych przez organizację okolicznościach wskazujących na potrzebę kontroli.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące odporności na sabotaż i wykrywanie manipulacji; rejestry inspekcji wyrywkowych; sprawozdania z inspekcji/rezultatów; sprawozdania z oceny/rezultatów; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za program ochrony przed manipulacją]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące kontroli systemów informacyjnych, komponentów systemu lub urządzeń służących do wykrywania prób manipulacji; zautomatyzowane mechanizmy wspomagające lub wdrażające wykrywanie prób manipulacji].		

SA-19	**AUTENTYCZNOŚĆ KOMPONENTÓW**		
	CEL OCENY: *Określić, czy organizacja:*		
	SA-19(a)	*opracowuje i wdraża politykę i procedury zwalczania obrotu towarami nieautentycznymi, które obejmują środki wykrywania i zapobiegania przedostawaniu się podrobionych składników do systemu informacyjnego;*	
	SA-19(b)	**SA-19(b)[1]**	*definiuje zewnętrzne organy ścigania, do których mają być zgłaszane podrobione elementy systemu informacyjnego;*
		SA-19(b)[2]	*definiuje personel lub role, którym mają być zgłaszane podrobione elementy systemu informacyjnego;*

SA-19	**AUTENTYCZNOŚĆ KOMPONENTÓW**			
		SA-19(b)[3]	*zgłasza podrobione elementy systemu informacyjnego do jednego lub więcej z poniższych podmiotów:*	
			SA-19(b)[3][a]	*źródło fałszywego komponentu;*
			SA-19(b)[3][b]	*określone przez organizację zewnętrzne organy ścigania; i/lub*
			SA-19(b)[3][c]	*personel lub role określone przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; polityka i procedury zwalczania podrabiania; polityka usuwania nośników; polityka ochrony nośników; polityka reagowania na incydenty; materiały szkoleniowe dotyczące podrabianych komponentów systemów informacyjnych; rejestry szkoleniowe dotyczące wykrywania i zapobiegania wprowadzaniu podrabianych komponentów do systemu informacyjnego; sprawozdania powiadamiające deweloperów / producentów / sprzedawców / wykonawców i/lub zewnętrzne organy ścigania o podrabianych komponentach systemów informacyjnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za politykę, procedury i sprawozdawczość w zakresie zwalczania obrotu towarami nieautentycznymi]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania, zapobiegania i raportowania zjawisk podrabiania; zautomatyzowane mechanizmy wspierające i/lub wdrażające wykrywanie, zapobieganie i raportowanie zjawisk podrabiania].			

SA-19(1)	**AUTENTYCZNOŚĆ KOMPONENTÓW | *SZKOLENIE / ROZPOZNAWANIE AUTENTYCZNOŚCI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-19(1)[1]	*określa personel lub role, które należy przeszkolić w zakresie wykrywania nieautentycznych elementów systemów informacyjnych (w tym sprzętu, aplikacji i oprogramowania układowego); oraz*

SA-19(1)	**AUTENTYCZNOŚĆ KOMPONENTÓW | *SZKOLENIE / ROZPOZNAWANIE AUTENTYCZNOŚCI***	
	SA-19(1)[2]	*szkoli zdefiniowany przez organizację personel lub role w celu wykrywania nieautentycznych elementów systemu informacyjnego (w tym sprzętu, aplikacji i oprogramowania układowego).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; polityka i procedury zapobiegania podrabianiu towarów; polityka utylizacji nośników; polityka ochrony nośników; polityka reagowania na incydenty; materiały szkoleniowe dotyczące nieautentycznych elementów systemów informacyjnych; rejestry szkoleniowe dotyczące wykrywania nieautentycznych elementów systemów informacyjnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za politykę, procedury i szkolenia w zakresie przeciwdziałania podrabianiu towarów]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie szkoleń z zakresu walki z fałszerstwami].	

SA-19(2)	**AUTENTYCZNOŚĆ KOMPONENTÓW | *KONTROLA KONFIGURACJI NA POTRZEBY SERWISOWANIA / NAPRAWY KOMPONENTÓW***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-19(2)[1]	*definiuje komponenty systemu informacyjnego wymagające kontroli konfiguracji, które mają być utrzymywane w oczekiwaniu na serwis/naprawę;*
	SA-19(2)[2]	*definiuje komponenty systemu informacyjnego wymagające kontroli konfiguracji, które mają być utrzymywane w oczekiwaniu na zwrot z serwisu; oraz*
	SA-19(2)[3]	*utrzymuje kontrolę konfiguracji nad zdefiniowanymi przez organizację komponentami systemu informacyjnego czekającymi na serwis/naprawę oraz serwisowanymi/naprawionym i komponentami oczekującymi na powrót do eksploatacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; polityka i procedury przeciwdziałania podrabianiu towarów; polityka ochrony nośników	

SA-19(2)	**AUTENTYCZNOŚĆ KOMPONENTÓW | *KONTROLA KONFIGURACJI NA POTRZEBY SERWISOWANIA / NAPRAWY KOMPONENTÓW***
	informacji; plan zarządzania konfiguracją; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy kontroli konfiguracji komponentów oczekujących na serwis/na naprawę; zapisy kontroli konfiguracji komponentów serwisowanych/naprawionych oczekujących na powrót do eksploatacji; zapisy dotyczące konserwacji systemu informacyjnego; zapisy z audytu systemu informacyjnego; dokumentacja dotycząca zarządzania inwentaryzacją; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za politykę, procedury i szkolenia w zakresie przeciwdziałania podrabianiu towarów; personel organizacji odpowiedzialny za zarządzanie konfiguracją]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania konfiguracją; zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie konfiguracją].

SA-19(3)	**AUTENTYCZNOŚĆ KOMPONENTÓW | *UTYLIZACJA KOMPONENTÓW***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-19(3)[1]	*określa techniki i metody utylizacji komponentów systemu informacyjnego; oraz*
	SA-19(3)[2]	*utylizuje elementy systemu informacyjnego przy użyciu techniki metod zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; polityka i procedury przeciwdziałania podrabianiu towarów; polityka utylizacji nośników danych; polityka ochrony nośników danych osobowych; zapisy dotyczące utylizacji komponentów systemu informacyjnego; dokumentacja technik oraz metod utylizacji komponentów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za politykę i procedury przeciwdziałania podrabianiu towarów; personel organizacji odpowiedzialny za utylizację komponentów systemu informacyjnego].	

SA-19(3)	**AUTENTYCZNOŚĆ KOMPONENTÓW |** ***UTYLIZACJA KOMPONENTÓW***
	Test: [*wybierz spośród:* Techniki organizacyjne oraz metody utylizacji komponentów systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające utylizację komponentów systemu].

SA-19(4)	**AUTENTYCZNOŚĆ KOMPONENTÓW |** ***SKANOWANIE AUTENTYCZNOŚCI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-19(4)[1]	*określa częstotliwość skanowania w poszukiwaniu nieautentycznych komponentów systemu informacyjnego; oraz*
	SA-19(4)[2]	*wyszukuje podrobione elementy systemu informacyjnego z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; polityka i procedury przeciwdziałania podrabianiu towarów; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia skanujące i związana z nimi dokumentacja; wyniki skanowania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za politykę i procedury przeciwdziałania podrabianiu towarów; personel organizacji odpowiedzialny za skanowanie autentyczności]. **Test**: [*wybierz spośród:* Procesy organizacyjne skanowania autentyczności; zautomatyzowane mechanizmy wspierające i/lub wdrażające skanowanie autentyczności].	

SA-20	**NIESTANDARDOWA (NA ZAMÓWIENIE) ROZBUDOWA KOMPONENTÓW KRYTYCZNYCH**	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-20[1]	*definiuje komponenty krytyczne systemu informacyjnego, które mają być ponownie wdrożone lub opracowane na zamówienie; oraz*

SA-20	**NIESTANDARDOWA (NA ZAMÓWIENIE) ROZBUDOWA KOMPONENTÓW KRYTYCZNYCH**	
	SA-20[2]	*ponownie wdraża lub opracowuje na zamówienie, zdefiniowane przez organizację komponenty systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące personalizowania komponentów krytycznych systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja cyklu życia systemu dotycząca niestandardowej (spersonalizowanej) rozbudowy komponentów krytycznych systemu informacyjnego; rejestry zarządzania konfiguracją; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za przebudowę lub indywidualne opracowanie komponentów krytycznych systemu informacyjnego]. **Test**: [*wybierz spośród:* procesy organizacyjne związane z re-implementacją lub niestandardowym rozwojem komponentów krytycznych systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające re-implementację lub niestandardowy rozwój komponentów krytycznych systemu informacyjnego].	

SA-21	**DOBÓR DEWELOPERÓW**		
	CEL OCENY: *Określić, czy organizacja:*		
	SA-21[1]	*definiuje system informacyjny, komponent systemu, lub usługę systemu informacyjnego, wymagające doboru dewelopera;*	
	SA-21[2]	*definiuje obowiązki, w celu określenia odpowiedniego upoważnienia dostępu dla dewelopera;*	
	SA-21[3]	*definiuje dodatkowe kryteria doboru personelu, które mają być spełnione przez dewelopera;*	
	SA-21[4]	**SA-21[4][a]**	*wymaga, aby deweloper zdefiniowanego przez organizację systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego, posiadał odpowiednie upoważnienia dostępu określone zdefiniowane przez organizację, zgodnie z obowiązującymi przepisami; oraz*

SA-21	**DOBÓR DEWELOPERÓW**		
		SA-21[4][b]	*wymaga, aby deweloper zdefiniowanego organizacyjnie systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego, spełniał zdefiniowane organizacyjnie dodatkowe kryteria doboru personelu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; polityka i procedury w zakresie bezpieczeństwa osobowego; procedury dotyczące doboru personelu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz stosownych upoważnień dostępu wymaganych przez deweloperów systemu informacyjnego; kryteria doboru personelu oraz związana z nimi dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za dobór deweloperów]. **Test**: [*wybierz spośród:* Procesy organizacyjne doboru deweloperów; zautomatyzowane mechanizmy wspierające dobór deweloperów].		

SA-21(1)	**DOBÓR DEWELOPERÓW | *OCENA PRZEGLĄDU***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-21(1)[1]	*określa działania, które mają zostać podjęte przez dewelopera systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego, w celu zapewnienia, że zostały spełnione wymagane kryteria uprawień dostępu i kryteria kontroli; oraz*
	SA-21(1)[2]	*wymaga, aby deweloper systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego, podjął określone organizacyjnie działania w celu zapewnienia, że spełnione są wymagane kryteria upoważnienia dostępu oraz kontroli.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; polityka i procedury w zakresie bezpieczeństwa osobowego; procedury dotyczące doboru personelu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz stosownych upoważnień dostępu wymaganych przez deweloperów systemu informacyjnego; kryteria doboru personelu oraz związana z nimi dokumentacja; wykaz działań	

SA-21(1)	**DOBÓR DEWELOPERÓW | *OCENA PRZEGLĄDU***
	gwarantujących spełnienie wymaganych kryteriów upoważnienia do dostępu oraz badań sprawdzających zgodność z przepisami; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za dobór deweloperów; deweloper systemu]. **Test**: [*wybierz spośród:* procesy organizacyjne doboru deweloperów; zautomatyzowane mechanizmy wspierające dobór deweloperów].

SA-22	**KOMPONENTY SYSTEMU BEZ WSPARCIA**	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-22(a)	*zastępuje komponenty systemu informacyjnego, gdy wsparcie dla tych komponentów nie jest już dostępne u dewelopera, sprzedawcy lub producenta;*
	SA-22(b)	**SA-22(b)[1]** *przedstawia uzasadnienie dalszego stosowania komponentów systemu bez wymaganego wsparcia, celem zaspokojenia potrzeb misyjnych/biznesowych; oraz*
		SA-22(b)[2] *dokumentuje zgodę na dalsze korzystanie z komponentów systemu bez wymaganego wsparcia, celem zaspokojenia potrzeb misyjnych/biznesowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedury dotyczące wymiany lub dalszego użytkowania nieobsługiwanych komponentów systemu informacyjnego; udokumentowane dowody na wymianę nieobsługiwanych komponentów systemu informacyjnego; udokumentowane zezwolenia (w tym uzasadnienie) na dalsze użytkowanie nieobsługiwanych komponentów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za cykl życia systemu; personel organizacji odpowiedzialny za zarządzanie konfiguracją].	

SA-22	**KOMPONENTY SYSTEMU BEZ WSPARCIA**
	Test: [*wybierz spośród:* Procesy organizacyjne dotyczące wymiany komponentów systemu nieposiadających wsparcia; zautomatyzowane mechanizmy wspierające i/lub wdrażające wymianę komponentów systemu bez wsparcia].

SA-22(1)	**KOMPONENTY SYSTEMU BEZ WSPARCIA | *ALTERNATYWNE ŹRÓDŁA STAŁEGO WSPARCIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	SA-22(1)[1]	*definiuje wsparcie ze strony zewnętrznych dostawców, które ma być zapewnione dla nieobsługiwanych komponentów systemu informacyjnego;*
	SA-22(1)[2]	*zapewnia i/lub uzyskuje wsparcie nieobsługiwanych komponentów systemu informacyjnego od jednego lub kilku z poniższych podmiotów:*
	SA-22(1)[2][a]	*wsparcie wewnętrzne; i/lub*
	SA-22(1)[2][b]	*zdefiniowane organizacyjnie wsparcie ze strony zewnętrznych dostawców.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka nabywania systemów i usług; procedura dotycząca wsparcia nieobsługiwanych komponentów systemu informacyjnego; dokumentacja przetargowa; dokumentacja nabycia; umowy nabycia; umowa gwarancji świadczenia usług (SLA); inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nabywanie systemów i usług; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za cykl życia systemu; personel organizacji lub zewnętrzni dostawcy wspierający komponenty systemu informacyjnego, które nie są już wspierane przez pierwotnych deweloperów, sprzedawców lub producentów]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące obsługi komponentów systemu, które nie są już obsługiwane przez pierwotnych deweloperów, dostawców lub producentów; zautomatyzowane mechanizmy zapewniające obsługę komponentów systemu, które nie są już obsługiwane przez pierwotnych deweloperów, dostawców lub producentów].	

KATEGORIA SC - OCHRONA SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH

SC-1	**POLITYKA I PROCEDURY OCHRONY SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH**			
	CEL OCENY: *Określić, czy organizacja:*			
	SC-1(A)(1)	**SC-1(A)(1)[1]**	*opracowuje i dokumentuje politykę ochrony systemów i sieci telekomunikacyjnych, która dotyczy:*	
			SC-1(A)(1)[1][A]	*celu;*
			SC-1(A)(1)[1][B]	*zakresu stosowania;*
			SC-1(A)(1)[1][C]	*ról;*
			SC-1(A)(1)[1][D]	*odpowiedzialności;*
			SC-1(A)(1)[1][E]	*zaangażowania kierownictwa;*
			SC-1(A)(1)[1][F]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			SC-1(A)(1)[1][G]	*przestrzegania zgodności z przepisami;*
		SC-1(A)(1)[2]	*określa personel lub role, wśród których ma być rozpowszechniana polityka ochrony systemów i sieci telekomunikacyjnych;*	
		SC-1(A)(1)[3]	*rozpowszechnia politykę ochrony systemów i sieci telekomunikacyjnych wśród personelu lub ról zdefiniowanych w organizacji;*	
	SC-1(A)(2)	**SC-1(A)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wdrażanie polityki ochrony systemów i sieci telekomunikacyjnych oraz związanych z nimi systemów i środków ochrony;*	
		SC-1(a)(2)[2]	*określa personel lub role, wśród których procedury mają być rozpowszechniane;*	
		SC-1(a)(2)[3]	*rozpowszechnia procedury wśród personelu i ról określonych w organizacji;*	

SC-1	**POLITYKA I PROCEDURY OCHRONY SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH**		
	SC-1(b)(1)	**SC-1(b)(1)[1]**	*określa częstotliwość przeglądów i aktualizacji aktualnej polityki ochrony środowiska i komunikacji;*
		SC-1(b)(1)[2]	*opiniuje i aktualizuje obowiązującą politykę ochrony systemów i sieci telekomunikacyjnych z częstotliwością określoną przez organizację;*
	SC-1(b)(2)	**SC-1(b)(2)[1]**	*definiuje częstotliwość przeglądów i aktualizacji bieżącej polityki ochrony systemów i sieci telekomunikacyjnych; oraz*
		SC-1(b)(2)[2]	*opiniuje i aktualizuje istniejący system oraz procedury ochrony systemów i sieci telekomunikacyjnych z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury ochrony systemów i sieci telekomunikacyjnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę systemów i sieci telekomunikacyjnych; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

SC-2	**SEPARACJA**
	CEL OCENY: *Ustalić, czy system informacyjny separuje funkcje użytkownika (w tym usługi interfejsu użytkownika) od funkcji zarządzania systemem informacyjnym.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące separacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Odseparowanie funkcji użytkownika od funkcji zarządzania systemem informacyjnym].

SA-22(1)	**SEPARACJA | *INTERFEJSY DLA UŻYTKOWNIKÓW NIEUPRZYWILEJOWANYCH***
	CEL OCENY: *Ustalić, czy system informacyjny uniemożliwia prezentację funkcji związanych z zarządzaniem systemem informacyjnym w interfejsie dedykowanym dla użytkowników nieuprzywilejowanych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące separacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; nieuprzywilejowani użytkownicy systemu informacyjnego; deweloper systemu]. **Test**: [*wybierz spośród:* Odseparowanie funkcji użytkownika od funkcji zarządzania systemem informacyjnym].

SC-3	**IZOLACJA FUNKCJI BEZPIECZEŃSTWA**
	CEL OCENY: *Ustalić, czy system informacyjny izoluje funkcje bezpieczeństwa od funkcji niezwiązanych z bezpieczeństwem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące izolacji funkcji bezpieczeństwa; wykaz funkcji bezpieczeństwa, które należy odizolować od funkcji niezwiązanych z bezpieczeństwem; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Separacja funkcji bezpieczeństwa od funkcji niezwiązanych z bezpieczeństwem w ramach systemu informacyjnego].

SC-3(1)	**IZOLACJA FUNKCJI BEZPIECZEŃSTWA | *SEPARACJA PODZESPOŁÓW***
	CEL OCENY: *Ustalenie, czy system informacyjny wykorzystuje podstawowe mechanizmy separacji sprzętowej w celu wdrożenia izolacji funkcji bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące izolacji funkcji bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; mechanizmy separacji podzespołów; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Separacja funkcji bezpieczeństwa od funkcji niezwiązanych z bezpieczeństwem w ramach systemu informacyjnego].

SC-3(2)	**IZOLACJA FUNKCJI BEZPIECZEŃSTWA | *FUNKCJE KONTROLI DOSTĘPU / PRZEPŁYWU***	
	CEL OCENY: *Ustalić, czy system informacyjny izoluje funkcje bezpieczeństwa wymuszające:*	
	SC-3(2)[1]	*kontrolę dostępu z funkcji niezwiązanych z bezpieczeństwem;*
	SC-3(2)[2]	*kontrolę przepływu informacji z niezabezpieczonych funkcji;*
	SC-3(2)[3]	*kontrolę dostępu z innych funkcji bezpieczeństwa; oraz*
	SC-3(2)[4]	*kontrolę przepływu informacji z innych funkcji bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące izolacji funkcji bezpieczeństwa; wykaz krytycznych funkcji bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Izolacja funkcji bezpieczeństwa wymuszających kontrolę dostępu i przepływu informacji].	

SC-3(3)	**IZOLACJA FUNKCJI BEZPIECZEŃSTWA | *MINIMALIZACJA FUNKCJONALNOŚCI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM***
	CEL OCENY: *Ustalenie, czy organizacja wprowadziła granicę izolacji systemu informacyjnego w celu zminimalizowania liczby funkcji niezwiązanych z ochroną, zawartych w granicach zawierających funkcje ochrony.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące izolacji funkcji bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające granicę izolacji].

SC-3(4)	**IZOLACJA FUNKCJI BEZPIECZEŃSTWA | *MODUŁ SPRZĘŻENIA I SPÓJNOŚCI***	
	CEL OCENY: *Ustalić, czy organizacja wdraża funkcje bezpieczeństwa jako niezależne moduły, które:*	
	SC-3(4)[1]	*maksymalizują wewnętrzną spójność wewnątrz modułów; oraz*
	SC-3(4)[2]	*minimalizują sprzężenie między modułami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące izolacji funkcji bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne mające na celu maksymalizację wewnętrznej spójności wewnątrz modułów oraz minimalizację sprzężenia między modułami; zautomatyzowane mechanizmy wspierające i/lub implementujące funkcje bezpieczeństwa jako niezależne moduły].	

SC-3(5)	**IZOLACJA FUNKCJI BEZPIECZEŃSTWA | *STRUKTURY WARSTWOWE***	
	CEL OCENY: *Ustalić, czy organizacja realizuje funkcje bezpieczeństwa jako strukturę warstwową:*	
	SC-3(5)[1]	*minimalizując interakcje między warstwami projektu; oraz*
	SC-3(5)[2]	*unikając uzależnienia niższych warstw od funkcjonalności lub poprawności wyższych warstw.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące izolacji funkcji bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne wdrażania funkcji bezpieczeństwa, jako struktury warstwowej, która minimalizuje interakcje pomiędzy warstwami oraz eliminuje zależność niższych warstw od funkcjonalności/korekty wyższych warstw; zautomatyzowane mechanizmy wspierające i/lub implementujące funkcje bezpieczeństwa, jako strukturę warstwową].	

SC-4	**INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH**
	CEL OCENY: *Ustalić, czy system informacyjny zapobiega nieautoryzowanemu i niezamierzonemu przekazywaniu informacji za pośrednictwem współdzielonych zasobów systemowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony informacji znajdujących się we wspólnych zasobach systemowych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu].

SC-4	**INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH**
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy zapobiegające nieautoryzowanemu i niezamierzonemu przekazywaniu informacji za pośrednictwem współdzielonych zasobów systemowych].

SC-4(1)	**INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH | *POZIOMY BEZPIECZEŃSTWA***
[Włączone do: SC-4].	

SC-4(2)	**INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH | *PRZETWARZANIE OKRESOWE***	
	CEL OCENY: *Określić, czy*:	
	SC-4(2)[1]	*organizacja określa procedury, które mają być stosowane w celu zapewnienia, że nieautoryzowany transfer informacji za pośrednictwem wspólnych zasobów jest uniemożliwiony, gdy system przetwarzający informacje jednoznacznie przełącza się między różnymi poziomami klauzuli lub kategoriami bezpieczeństwa; oraz*
	SC-4(2)[2]	*system informacyjny zapobiega nieautoryzowanemu przekazywaniu informacji za pośrednictwem współdzielonych zasobów zgodnie z procedurami określonymi przez organizację, gdy system przetwarzający informacje jednoznacznie przełącza się między różnymi poziomami klauzuli lub kategoriami bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony informacji znajdujących się we wspólnych zasobach systemowych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zapobiegające nieautoryzowanemu przekazywaniu informacji za pośrednictwem współdzielonych zasobów systemowych].	

SC-5	**OCHRONA PRZED BLOKADĄ USŁUG (DoS)**	
	CEL OCENY: *Określić, czy:*	
	SC-5[1]	*organizacja określa rodzaje ataków typu blokada usługi (DoS) lub wskazuje źródła takich informacji, aby chronić lub ograniczać ich skutki;*
	SC-5[2]	*organizacja określa środki bezpieczeństwa jakie mają być stosowane przez system informacyjny w celu ochrony przed zdefiniowanymi przez organizację atakami typu "DoS, lub w celu ograniczenia ich skutków"; oraz*
	SC-5[3]	*system informacyjny chroni przed lub ogranicza skutki zdefiniowanych przez organizację ataków typu DoS (lub wskazanie źródła takiej informacji) poprzez zastosowanie zdefiniowanych przez organizację środków bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony przed blokadą usług (DoS); dokumentacja projektowa systemu informacyjnego; plan bezpieczeństwa; wykaz ataków typu DoS wymagających stosowania środków bezpieczeństwa w celu ochrony przed / lub ograniczenia skutków takich ataków; wykaz środków bezpieczeństwa chroniących przed atakami typu DoS lub ograniczających ich skutki; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za procedury reagowania na incydenty; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy chroniące przed atakami typu DoS lub ograniczające ich skutki].	

SC-5(1)	**OCHRONA PRZED BLOKADĄ USŁUG (DoS) | *OGRANICZENIE UŻYTKOWNIKÓW WEWNĘTRZNYCH***	
	CEL OCENY: *Określić, czy:*	
	SC-5(1)[1]	*organizacja ustala ataki typu DoS, w przypadku których wymagane jest, aby system informacyjny ograniczał zdolność osób do przeprowadzania takich ataków na inne systemy informacyjne; oraz*

SC-5(1)	**OCHRONA PRZED BLOKADĄ USŁUG (DoS) | *OGRANICZENIE UŻYTKOWNIKÓW WEWNĘTRZNYCH***	
	SC-5(1)[2]	*system informacyjny ogranicza zdolność osób do przeprowadzania zdefiniowanych przez organizację ataków typu DoS na inne systemy informacyjne.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony przed blokadą usług (DoS); dokumentacja projektowa systemu informacyjnego; plan bezpieczeństwa; wykaz ataków typu DoS przeprowadzanych przez osoby na systemy informacyjne; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za procedury reagowania na incydenty; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy ograniczające możliwość przeprowadzania ataków typu DoS przeciwko innym systemom informacyjnym].	

SC-5(2)	**OCHRONA PRZED BLOKADĄ USŁUG (DoS) | *NADMIAROWOŚĆ / SZEROKOŚĆ PASMA / REDUNDANCJA***	
	CEL OCENY: *Ustalić, czy system informacyjny, w celu ograniczenia skutków typu DoS, zarządza:*	
	SC-5(2)[1]	*nadmiarowością pasma;*
	SC-5(2)[2]	*szerokością pasma; lub*
	SC-5(2)[3]	*innym tożsamym zabezpieczeniem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony przed blokadą usług (DoS); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za procedury reagowania na incydenty; deweloper systemu].	

SC-5(2)	**OCHRONA PRZED BLOKADĄ USŁUG (DoS) | *NADMIAROWOŚĆ / SZEROKOŚĆ PASMA / REDUNDANCJA***
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające zarządzanie przepustowością, pojemnością i redundancją systemów informacyjnych w celu ograniczenia skutków ataków typu DoS.].

SC-5(3)	**OCHRONA PRZED BLOKADĄ USŁUG (DoS) | *WYKRYWANIE / MONITOROWANIE***		
	CEL OCENY: *Określić, czy organizacja:*		
	SC-5(3)(a)	**SC-5(3)(a)[1]**	*definiuje narzędzia monitorujące, które mają być stosowane do wykrywania wskaźników ataków na system informacyjny typu DoS;*
		SC-5(3)(a)[2]	*stosuje zdefiniowane przez organizację narzędzia monitorujące do wykrywania wskaźników ataków typu DoS na system informacyjny;*
	SC-5(3)(b)	**SC-5(3)(b)[1]**	*definiuje zasoby systemu informacyjnego, które mają być monitorowane w celu ustalenia, czy istnieją wystarczające zasoby, aby zapobiec skutecznym atakom typu DoS; oraz*
		SC-5(3)(b)[2]	*monitoruje zasoby systemu informacyjnego zdefiniowanego przez organizację w celu ustalenia, czy istnieją wystarczające zabezpieczenia, aby zapobiec skutecznym atakom typu DoS.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony przed blokadą usług (DoS); dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za wykrywanie i monitorowanie]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy/narzędzia wdrażające monitorowanie systemu informacyjnego w zakresie ataków typu DoS].		

SC-6	**DOSTĘPNOŚĆ ZASOBÓW**		
	CEL OCENY: *Określić, czy:*		
	SC-6[1]	*organizacja określa sposoby, jakie należy zastosować w celu ochrony dostępności zasobów;*	
	SC-6[2]	*organizacja określa środki bezpieczeństwa, które mają być stosowane w celu ochrony dostępności zasobów;*	
	SC-6[3]	*system informacyjny chroni dostępność zasobów, przydzielając zasoby zdefiniowane przez organizację wg:*	
		SC-6[3][a]	*priorytetu;*
		SC-6[3][b]	*przydziału; lub*
		SC-6[3][c]	*zabezpieczeń zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedura dotycząca ustalania priorytetów w ramach zasobów systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające lub wdrażające zdolność do przydzielania zasobów; zabezpieczenia stosowane w celu ochrony dostępności zasobów].		

SC-7	**OCHRONA POŁĄCZEŃ BRZEGOWYCH**		
	CEL OCENY: *Ustalić, czy system informacyjny:*		
	SC-7(a)	**SC-7(a)[1]**	*monitoruje komunikację na zewnętrznej granicy systemu informacyjnego;*

SC-7	**OCHRONA POŁĄCZEŃ BRZEGOWYCH**		
		SC-7(a)[2]	*monitoruje komunikację w obrębie kluczowych granic wewnętrznych systemu;*
		SC-7(a)[3]	*kontroluje komunikację na zewnętrznych granicach systemu informacyjnego;*
		SC-7(a)[4]	*kontroluje komunikację w obrębie kluczowych granic wewnętrznych systemu;*
	SC-7(b)	*implementuje podsieci dla publicznie dostępnych komponentów systemu, które są albo:*	
		SC-7(b)[1]	*fizycznie oddzielone od wewnętrznych sieci organizacyjnych; i/lub*
		SC-7(b)[2]	*logicznie oddzielone od wewnętrznych sieci organizacyjnych; oraz*
	SC-7(c)	*łączy się z sieciami zewnętrznymi lub systemami informacyjnymi tylko poprzez zarządzane interfejsy zawierające zabezpieczenia połączeń urządzeń brzegowych rozmieszczonych zgodnie z architekturą bezpieczeństwa organizacyjnego.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; wykaz kluczowych granic wewnętrznych systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; sprzętowa i programowa ochrona połączeń brzegowych; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dokumentacja architektury bezpieczeństwa przedsiębiorstwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Automatyzowane mechanizmy wdrażania ochrony połączeń brzegowych].		

SC-7(1)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *FIZYCZNIE ODDZIELONE PODSIECI***
[Włączone do: SC-7].	

SC-7(2)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *DOSTĘP PUBLICZNY***
[Włączone do: SC-7].	

SC-7(3)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *PUNKTY DOSTĘPOWE***
	CEL OCENY: *Ustalić, czy organizacja ogranicza liczbę zewnętrznych połączeń sieciowych do systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzętowa i programowa ochrona połączeń brzegowych; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; logi komunikacji i monitorowania ruchu w sieci; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje ochrony połączeń brzegowych; zautomatyzowane mechanizmy ograniczające liczbę zewnętrznych połączeń sieciowych do systemu informacyjnego].

SC-7(4)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ZEWNĘTRZNE USŁUGI TELEKOMUNIKACYJNE***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-7(4)(a)	*wdraża zarządzany interfejs dla każdej zewnętrznej usługi telekomunikacyjnej;*
	SC-7(4)(b)	*ustanawia politykę przepływu ruchu dla każdego zarządzanego interfejsu;*
	SC-7(4)(c)	*zapewnia poufność i integralność informacji przekazywanych za pośrednictwem każdego interfejsu;*
	SC-7(4)(d)	*dokumentuje każdy wyjątek od polityki przepływu informacji:*

SC-7(4)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ZEWNĘTRZNE USŁUGI TELEKOMUNIKACYJNE***		
		SC-7(4)(d)[1]	*wspiera misję / potrzebę biznesową;*
		SC-7(4)(d)[2]	*określa czas trwania tej potrzeby;*
	SC-7(4)(e)	**SC-7(4)(e)[1]**	*określa częstotliwość przeglądu wyjątków od polityki przepływu informacji;*
		SC-7(4)(e)[2]	*dokonuje przeglądu wyjątków od polityki przepływu informacji z częstotliwością określoną przez organizację; oraz*
		SC-7(4)(e)[3]	*usuwa wyjątki, które nie są już wymagane przez misję / potrzebę biznesową.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; polityka przepływu informacji; polityka kontroli przepływu informacji; procedury dotyczące ochrony połączeń brzegowych; architektura bezpieczeństwa systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; sprzętowa i programowa ochrona połączeń brzegowych; architektura systemu informacyjnego i dokumentacja konfiguracyjna; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry wyjątków w zakresie polityki przepływu informacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Procesy organizacyjne dokumentowania i przeglądania wyjątków od polityki przepływu informacji; procesy organizacyjne usuwania wyjątków od polityki przepływu informacji; zautomatyzowane mechanizmy realizujące funkcje ochrony połączeń brzegowych; zarządzane interfejsy realizujące politykę przepływu informacji.].		

SC-7(5)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ODRZUĆ DOMYŚLNIE / POZWÓL NA WYJĄTEK***	
	CEL OCENY: *Ustalić, czy system informacyjny, na zarządzanych interfejsach:*	
	SC-7(5)[1]	*domyślnie odrzuca ruch sieciowy; oraz*

SC-7(5)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ODRZUĆ DOMYŚLNIE / POZWÓL NA WYJĄTEK***	
	SC-7(5)[2]	*zezwala na ruch sieciowy w drodze wyjątku.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające zarządzanie ruchem danych na zarządzanych interfejsach].	

SC-7(6)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ODPOWIEDŹ NA ROZPOZNANE AWARIE***
[Włączone do: SC-7(18)].	

SC-7(7)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ZAPOBIEGANIE PODZIAŁOWI TUNELOWANIA ZDALNYCH URZĄDZEŃ***
	CEL OCENY: *Ustalić, czy system informacyjny, połączony ze zdalnym urządzeniem, zapobiega równoczesnemu nawiązywaniu przez to urządzenie połączenia z tym systemem i komunikowania się za pośrednictwem innego połączenia z zasobami sieci zewnętrznych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

SC-7(7)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ZAPOBIEGANIE PODZIAŁOWI TUNELOWANIA ZDALNYCH URZĄDZEŃ***
	Wywiad: [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje ochrony połączeń brzegowych; zautomatyzowane mechanizmy wspierające/ograniczające połączenia niebędące połączeniami zdalnymi].

SC-7(8)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *RUCH TELEKOMUNIKACYJNY DO AUTORYZOWANYCH SERWERÓW PROXY***	
	CEL OCENY: *Określić, czy*:	
	SC-7(8)[1]	*organizacja określa wewnętrzny ruch sieciowy, który ma być kierowany do sieci zewnętrznych;*
	SC-7(8)[2]	*organizacja określa sieci zewnętrzne, do których ma być kierowany określony przez organizację wewnętrzny ruch sieciowy; oraz*
	SC-7(8)[3]	*system informacyjny kieruje zdefiniowany przez organizację wewnętrzny ruch sieciowy do zdefiniowanych przez organizację sieci zewnętrznych poprzez uwierzytelnione serwery proxy na zarządzanych interfejsach.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementujące zarządzanie ruchem poprzez uwierzytelnione serwery proxy na zarządzanych interfejsach].	

SC-7(9)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *OGRANICZENIE ZAGROŻEŃ WYJŚCIOWEGO RUCHU TELEKOMUNIKACYJNEGO***		
	CEL OCENY: *Ustalić, czy system informacyjny:*		
	SC-7(9)(a)	**SC-7(9)(a)[1]**	*rozpoznaje wychodzący ruch telekomunikacyjny stanowiący zagrożenie dla zewnętrznych systemów informacyjnych; oraz*
		SC-7(9)(a)[2]	*odrzuca wychodzący ruch komunikacyjny stanowiący zagrożenie dla zewnętrznych systemów informacyjnych; oraz*
	SC-7(9)(b)	*kontroluje tożsamość użytkowników wewnętrznych skojarzonych z odmową komunikacji.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje ochrony połączeń brzegowych; zautomatyzowane mechanizmy realizujące wykrywanie i odrzucanie wychodzącego ruchu komunikacyjnego stanowiącego zagrożenie; zautomatyzowane mechanizmy realizujące audyt wychodzącego ruchu telekomunikacyjnego].		

SC-7(10)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ZAPOBIEGANIE NIEAUTORYZOWANEJ EKSFILTRACJI***
	CEL OCENY: *Ustalić, czy organizacja zapobiega nieautoryzowanej eksfiltracji informacji pomiędzy zarządzanymi interfejsami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu

SC-7(10)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ZAPOBIEGANIE NIEAUTORYZOWANEJ EKSFILTRACJI***
	informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące funkcje ochrony połączeń brzegowych; zapobieganie nieautoryzowanej eksfiltracji informacji pomiędzy zarządzanymi interfejsami].

SC-7(11)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *OGRANICZENIE DOTYCZĄCE RUCHU WEJŚCIOWEGO***	
	CEL OCENY: *Określić, czy:*	
	SC-7(11)[1]	*organizacja określa wewnętrzny ruch telekomunikacyjny, który ma być kierowany do sieci zewnętrznych;*
	SC-7(11)[2]	*organizacja określa autoryzowane miejsca docelowe, do których może być kierowany tylko ruch przychodzący ze zdefiniowanych przez organizację autoryzowanych źródeł; oraz*
	SC-7(11)[3]	*system informacyjny pozwala wyłącznie na kierowanie ruchu przychodzącego ze zdefiniowanych przez organizację autoryzowanych źródeł do zdefiniowanych przez organizację autoryzowanych miejsc docelowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy realizujące możliwości ochrony połączeń brzegowych w oparciu o pary adresowe źródło/przeznaczenie].	

SC-7(12)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *SYSTEM OCHRONY KOMPUTERA GŁÓWNEGO***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-7(12)[1]	*definiuje mechanizmy ochrony połączeń brzegowych oparte na komputerze głównym typu Host;*
	SC-7(12)[2]	*definiuje komponenty systemu informacyjnego, w których mają być zaimplementowane mechanizmy ochrony połączeń brzegowych oparte na komputerze głównym typu Host, zdefiniowane organizacyjnie; oraz*
	SC-7(12)[3]	*implementuje organizacyjnie zdefiniowane mechanizmy ochrony połączeń brzegowych na zdefiniowanych organizacyjnie komponentach systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzętowa i programowa ochrona połączeń brzegowych; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za ochronę połączeń brzegowych; użytkownicy systemu informacyjnego]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wdrażające możliwości ochrony połączeń brzegowych oparte na komputerze głównym typu host].	

SC-7(13)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *IZOLACJA NARZĘDZI BEZPIECZEŃSTWA / MECHANIZMÓW / KOMPONENTÓW WSPARCIA***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-7(13)[1]	*definiuje narzędzia, mechanizmy i komponenty wspierające bezpieczeństwo informacji, które mają być odizolowane od innych wewnętrznych komponentów systemu informacyjnego; oraz*

SC-7(13)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *IZOLACJA NARZĘDZI BEZPIECZEŃSTWA / MECHANIZMÓW / KOMPONENTÓW WSPARCIA***	
	SC-7(13)[2]	*izoluje zdefiniowane przez organizację narzędzia, mechanizmy i komponenty bezpieczeństwa informacji od innych wewnętrznych komponentów systemu informacyjnego, poprzez wdrożenie fizycznie oddzielnych podsieci z zarządzanymi interfejsami do innych komponentów systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; wykaz narzędzi bezpieczeństwa i elementów wsparcia, które należy odizolować od innych wewnętrznych elementów systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające izolację narzędzi, mechanizmów i komponentów wspierających bezpieczeństwo informacji].	

SC-7(14)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *OCHRONA PRZED NIEAUTORYZOWANYMI POŁĄCZENIAMI FIZYCZNYMI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-7(14)[1]	*definiuje zarządzane interfejsy, które mają być chronione przed nieautoryzowanymi połączeniami fizycznymi; oraz*
	SC-7(14)[2]	*chroni przed nieautoryzowanymi połączeniami fizycznymi do zdefiniowanych przez organizację interfejsów zarządzanych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego	

SC-7(14)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *OCHRONA PRZED NIEAUTORYZOWANYMI POŁĄCZENIAMI FIZYCZNYMI***
	i związana z tym dokumentacja; schemat okablowania i sieci telekomunikacyjnej; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające ochronę przed nieautoryzowanymi połączeniami fizycznymi].

SC-7(15)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *DOSTĘP DO SIECI UPRAWNIONEJ***	
	CEL OCENY: *Ustalić, czy system informacyjny kieruje uprzywilejowane połączenia sieciowe poprzez dedykowany, zarządzany interfejs, w celu:*	
	SC-7(15)[1]	*kontroli dostępu; oraz*
	SC-7(15)[2]	*audytu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dzienniki audytów; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące kierowanie uprzywilejowanych połączeń sieciowych poprzez dedykowany, zarządzany interfejs].	

SC-7(16)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ZAPOBIEGANIE WYKRYWANIU KOMPONENTÓW / URZĄDZEŃ***
	CEL OCENY: *Ustalić, czy system informacyjny uniemożliwia wykrycie określonych komponentów systemu tworzących zarządzany interfejs.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zapobieganie wykrywaniu komponentów systemu tworzących zarządzane interfejsy].

SC-7(17)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *AUTOMATYCZNE EGZEKWOWANIE FORMATÓW PROTOKOŁU***
	CEL OCENY: *Ustalić, czy system informacyjny wymusza przestrzeganie formatów protokołów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające egzekwowanie przestrzegania formatów protokołów].

SC-7(18)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *BŁĄD BEZPIECZEŃSTWA***		
	CEL OCENY: *Ustalić, czy w przypadku awarii urządzenia brzegowego zabezpieczającego granicę systemu informacyjnego system przechodzi do stanu bezpiecznego.*		
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające rozwiązania zabezpieczające przed błędem bezpieczeństwa].		

SC-7(19)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *BLOKOWANIE KOMUNIKACJI Z HOSTAMI SPOZA ORGANIZACJI***		
	CEL OCENY: *Określić, czy organizacja:*		
	SC-7(19)[1]	*definiuje klienckie urządzenia komunikacyjne, które są niezależnie konfigurowane przez użytkowników końcowych oraz usługodawców zewnętrznych; oraz*	
	SC-7(19)[2]	*blokuje, pomiędzy zdefiniowanymi przez organizację klienckimi urządzeniami komunikacyjnymi, które są niezależnie konfigurowane przez użytkowników końcowych oraz usługodawców zewnętrznych:*	
		SC-7(19)[2][a]	*przychodzący ruch sieciowy; oraz*
		SC-7(19)[2][b]	*wychodzący ruch sieciowy.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; lista klienckich urządzeń komunikacyjnych konfigurowanych samodzielnie przez użytkowników końcowych oraz		

SC-7(19)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *BLOKOWANIE KOMUNIKACJI Z HOSTAMI SPOZA ORGANIZACJI***
	usługodawców zewnętrznych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące blokowanie przychodzącego i wychodzącego ruchu sieciowego pomiędzy klienckimi urządzeniami komunikacyjnymi konfigurowanymi samodzielnie przez użytkowników końcowych oraz usługodawcę zewnętrznego].

SC-7(20)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *DYNAMICZNA IZOLACJA / SEGREGACJA***	
	CEL OCENY: *Określić, czy:*	
	SC-7(20)[1]	*organizacja określa komponenty systemu informacyjnego, które mają być dynamicznie odizolowane/segregowane od innych komponentów systemu; oraz*
	SC-7(20)[2]	*system informacyjny zapewnia możliwość dynamicznego odizolowania/segregacji komponentów systemu informacyjnego zdefiniowanych przez organizację, od innych komponentów systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; wykaz komponentów systemu informacyjnego, które mają być dynamicznie odizolowane/segregowane od innych komponentów systemu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające lub implementujące możliwość dynamicznego izolowania/segregowania komponentów systemu informacyjnego].	

SC-7(21)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *IZOLACJA KOMPONENTÓW SYSTEMU* INFORMACYJNEGO**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-7(21)[1]	*definiuje elementy systemu informacyjnego, które mają być rozdzielone przez mechanizmy ochrony połączeń brzegowych;*
	SC-7(21)[2]	*definiuje misje i/lub funkcje biznesowe, wspierane przez zdefiniowane organizacyjnie elementy systemu informacyjnego, rozdzielone przez mechanizmy ochrony połączeń brzegowych; oraz*
	SC-7(21)[3]	*wykorzystuje mechanizmy ochrony połączeń brzegowych do rozdzielania zdefiniowanych przez organizację komponentów systemu informacyjnego wspierających zdefiniowane przez organizację misje i/lub funkcje biznesowe.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; dokumentacja struktury organizacyjnej; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwość wyodrębnienia komponentów systemu informacyjnego wspierających misje organizacyjne i/lub funkcje biznesowe].	

SC-7(22)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ODDZIELNE PODSIECI DO PODŁĄCZENIA DO RÓŻNYCH DOMEN BEZPIECZEŃSTWA***
	CEL OCENY: *Ustalić, czy system informacyjny implementuje odrębne adresy sieciowe (tj. różne podsieci), aby połączyć się z systemami w różnych domenach bezpieczeństwa.*

SC-7(22)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *ODDZIELNE PODSIECI DO PODŁĄCZENIA DO RÓŻNYCH DOMEN BEZPIECZEŃSTWA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające odrębne adresy sieciowe/różne podsieci].

SC-7(23)	**OCHRONA POŁĄCZEŃ BRZEGOWYCH | *WYŁĄCZENIE INFORMACJI ZWROTNEJ NADAWCY W PRZYPADKU AWARII PROTOKOŁU UWIERZYTELNIAJĄCEGO***
	CEL OCENY: *Ustalić, czy system informacyjny wyłącza wysyłanie do nadawców informacji zwrotnych o niepowodzeniu uwierzytelniania formatu protokołu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony połączeń brzegowych; dokumentacja projektowa systemu informacyjnego; sprzęt i oprogramowanie systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę połączeń brzegowych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub implementujące wyłączenie informacji zwrotnych wysyłanych do nadawców o niepowodzeniu uwierzytelniania formatu protokołu].

SC-8	**POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI**	
	CEL OCENY: *Ustalić, czy system informacyjny chroni jedno lub więcej z poniższych:*	
	SC-8[1]	*poufność przekazywanych informacji; i/lub*
	SC-8[2]	*integralność przekazywanych informacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące poufności i integralności przekazu danych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające poufność i/lub integralność przekazu danych].	

SC-8(1)	**POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | *KRYPTOGRAFICZNA LUB ALTERNATYWNA OCHRONA FIZYCZNA***		
	CEL OCENY: *Określić, czy:*		
	SC-8(1)[1]	*organizacja określa fizyczne zabezpieczenia, które należy wdrożyć w celu ochrony informacji podczas transmisji, jeśli mechanizmy kryptograficzne nie są wdrożone; oraz*	
	SC-8(1)[2]	*system informacyjny wdraża mechanizmy kryptograficzne w celu wykonania jednego lub więcej z poniższych działań podczas transmisji, chyba, że są one chronione przez określone przez organizację alternatywne zabezpieczenia fizyczne:*	
		SC-8(1)[2][a]	*zapobiega nieuprawnionemu ujawnieniu informacji; i/lub*
		SC-8(1)[2][b]	*wykrywa zmiany w informacjach.*

SC-8(1)	**POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | *KRYPTOGRAFICZNA LUB ALTERNATYWNA OCHRONA FIZYCZNA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące poufności i integralności przekazu danych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficzne wspierające i/lub wdrażające poufność i/lub integralność transmisji; zautomatyzowane mechanizmy wspierające i/lub wdrażające alternatywne zabezpieczenia fizyczne; procesy organizacyjne służące definiowaniu i wdrażaniu alternatywnych zabezpieczeń fizycznych].

SC-8(2)	**POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | *OBSŁUGA „PRZED" I „PO" TRANSMISJI***	
	CEL OCENY: *Ustalić, czy system informacyjny utrzymuje jedno lub więcej z poniższych:*	
	SC-8(2)[1]	*poufność informacji podczas przygotowania do przekazania;*
	SC-8(2)[2]	*poufność informacji w trakcie ich opracowywania; i/lub*
	SC-8(2)[3]	*integralność informacji podczas przygotowania do transmisji;*
	SC-8(2)[4]	*integralność informacji w trakcie odbierania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące poufności i integralności przekazu danych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające poufność i/lub integralność transmisji].	

SC-8(3)	**POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | *OCHRONA KRYPTOGRAFICZNA ZEWNĘTRZNYCH KOMUNIKATÓW***	
	CEL OCENY: *Określić, czy:*	
	SC-8(3)[1]	*organizacja określa alternatywne zabezpieczenia fizyczne, które należy wdrożyć w celu ochrony zewnętrznych wiadomości; oraz*
	SC-8(3)[2]	*system informacyjny wdraża mechanizmy kryptograficzne w celu ochrony zewnętrznych wiadomości, chyba, że są one w inny sposób chronione przez zdefiniowane przez organizację alternatywne zabezpieczenia fizyczne.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące poufności i integralności przekazu danych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficzne wspierające i/lub wdrażające poufność i/lub integralność transmisji wiadomości zewnętrznych; zautomatyzowane mechanizmy wspierające i/lub wdrażające alternatywne zabezpieczenia fizyczne; procesy organizacyjne mające na celu określenie i wdrożenie alternatywnych zabezpieczeń fizycznych].	

SC-8(4)	**POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | *KOMUNIKACJA UKRYTA / LOSOWA***	
	CEL OCENY: *Określić, czy:*	
	SC-8(4)[1]	*organizacja określa alternatywne zabezpieczenia fizyczne, które należy wdrożyć w celu ochrony przed nieuprawnionym ujawnieniem wzorców komunikacji;*
	SC-8(4)[2]	*system informacyjny, o ile nie jest chroniony przez określone przez organizację alternatywne fizyczne środki bezpieczeństwa, wdraża mechanizmy kryptograficzne do:*

SC-8(4)	**POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | *KOMUNIKACJA UKRYTA / LOSOWA***		
		SC-8(4)[2][a]	*ukrytych wzorców komunikacji; lub*
		SC-8(4)[2][b]	*losowych wzorców komunikacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące poufności i integralności przekazu danych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficzne wspierające i/lub implementujące ukrywanie lub losowość wzorców komunikacyjnych; zautomatyzowane mechanizmy wspierające i/lub implementujące alternatywne zabezpieczenia fizyczne; procesy organizacyjne służące definiowaniu i wdrażaniu alternatywnych zabezpieczeń fizycznych].		

SC-9	**POUFNOŚĆ TRANSMISJI**
[Włączone do: SC-8].	

SC-10	**ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO**	
	CEL OCENY: *Określić, czy:*	
	SC-10[1]	*organizacja określa okres braku aktywności, po którym system informacyjny zamyka połączenie sieciowe związane z sesją komunikacyjną; oraz*
	SC-10[2]	*system informacyjny kończy połączenie sieciowe związane z sesją komunikacyjną na koniec sesji lub po upływie określonego przez organizację okresu braku aktywności.*

SC-10	**ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące zakończenia połączenia sieciowego; dokumentacja projektowa systemu informacyjnego; plan bezpieczeństwa; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwości zakańczania połączeń sieciowych].

SC-11	**ZAUFANA ŚCIEŻKA KOMUNIKACYJNA**	
	CEL OCENY: *Określić, czy:*	
	SC-11[1]	*organizacja definiuje funkcje bezpieczeństwa systemu informacyjnego;*
	SC-11[2]	*zdefiniowane przez organizację funkcje bezpieczeństwa obejmują co najmniej podwójne uwierzytelnianie; oraz*
	SC-11[3]	*system informacyjny ustanawia zaufaną ścieżkę komunikacji pomiędzy użytkownikiem, a zdefiniowanymi przez organizację funkcjami bezpieczeństwa systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące zaufanej ścieżki komunikacyjnej; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wyniki oceny niezależnych, sprawdzających organizacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zaufane ścieżki komunikacyjne].	

SC-11(1)	**ZAUFANA ŚCIEŻKA KOMUNIKACYJNA | *IZOLACJA LOGICZNA***	
	CEL OCENY: *Ustalić, czy system informacyjny zapewnia zaufaną ścieżkę komunikacji, czyli:*	
	SC-11(1)[1]	*odizolowaną logicznie; oraz*
	SC-11(1)[2]	*odróżniającą się od innych ścieżek.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące zaufanej ścieżki komunikacyjnej; plan bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wyniki oceny niezależnych, sprawdzających organizacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zaufane ścieżki komunikacyjne].	

SC-12	**GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI**		
	CEL OCENY: *Określić, czy organizacja:*		
	SC-12[1]	*definiuje wymagania dotyczące kluczy kryptograficznych, dotyczące:*	
		SC-12[1][a]	*generowania;*
		SC-12[1][b]	*dystrybucji;*
		SC-12[1][c]	*przechowywania;*
		SC-12[1][d]	*dostępu;*
		SC-12[1][e]	*niszczenia; oraz*
	SC-12[2]	*ustanawia i zarządza kluczami kryptograficznymi stosowanymi w systemie informacyjnym do ochrony kryptograficznej, zgodnie ze zdefiniowanymi przez organizację wymaganiami dotyczącymi generowania, dystrybucji, przechowywania, dostępu i niszczenia kluczy.*	

SC-12	**GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące generowania i zarządzania kluczami kryptograficznymi; dokumentacja projektowa systemu informacyjnego; mechanizmy kryptograficzne; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za generowanie i/lub zarządzanie kluczami kryptograficznymi]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające generowanie i zarządzanie kluczami kryptograficznymi].

SC-12(1)	**GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | *DOSTĘPNOŚĆ***
	CEL OCENY: *Ustalenie, czy organizacja utrzymuje dostępność informacji w przypadku utraty kluczy kryptograficznych przez użytkowników.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące generowania, zarządzania i odtwarzania kluczy kryptograficznych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za generowanie lub zarządzanie kluczami kryptograficznymi]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające generowanie i zarządzanie kluczami kryptograficznymi].

SC-12(2)	**GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | *KLUCZE SYMETRYCZNE***
	CEL OCENY: *Ustalić, czy organizacja generuje, kontroluje i dystrybuuje symetryczne klucze kryptograficzne przy użyciu:*

SC-12(2)	**GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | *KLUCZE SYMETRYCZNE***	
	SC-12(2)[1]	*technologii i procesów zarządzania kluczami, zgodnie z wewnętrzną regulacją organizacji lub przepisami prawa; lub*
	SC-12(2)[2]	*zatwierdzonymi przez upoważniony personel / role organizacji procesami zarządzania kluczami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące generowania i zarządzania kluczami kryptograficznymi; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; lista technologii i procesów zarządzania kluczami, zgodnych z wewnętrzną regulacją organizacji lub przepisami prawa; lista zatwierdzonych, przez upoważniony personel / role w organizacji, procesów zarządzania kluczami; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za generowanie lub zarządzanie kluczami kryptograficznymi]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające generowanie i zarządzanie symetrycznym i kluczami kryptograficznymi].	

SC-12(3)	**GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | *KLUCZE ASYMETRYCZNE***	
	CEL OCENY: *Ustalić, czy organizacja generuje, kontroluje i dystrybuuje asymetryczne klucze kryptograficzne przy użyciu jednego z poniższych sposobów:*	
	SC-12(3)[1]	*technologie i procesy zarządzania kluczami zatwierdzone przez upoważniony personel /role w organizacji;*
	SC-12(3)[2]	*zatwierdzone certyfikaty infrastruktury klucza publicznego klasy 3 lub wstępnie przygotowany materiał klucza; lub*
	SC-12(3)[3]	*zatwierdzone certyfikaty infrastruktury klucza publicznego klasy 3 lub klasy 4 oraz sprzętowe tokeny zabezpieczające, które chronią klucz prywatny użytkownika.*

SC-12(3)	**GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | *KLUCZE ASYMETRYCZNE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące generowania i zarządzania kluczami kryptograficznymi; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; lista zatwierdzonych, przez upoważniony personel / role w organizacji, procesów zarządzania kluczami; wykaz zatwierdzonych świadectw infrastruktury klucza publicznego klasy 3 i 4; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za generowanie lub zarządzanie kluczami kryptograficznymi; personel organizacji odpowiedzialny za certyfikaty infrastruktury klucza publicznego (PKI)]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające generowanie i zarządzanie asymetrycznymi kluczami kryptograficznymi].

SC-12(4)	**GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | *CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO***
[Włączone do: SC-12].	

SC-12(5)	**GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | *CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO / TOKENY SPRZĘTOWE***
[Włączone do: SC-12].	

SC-13	**OCHRONA KRYPTOGRAFICZNA**	
	CEL OCENY: *Określić, czy:*	
	SC-13[1]	*organizacja wdraża zastosowania kryptograficzne; oraz*

SC-13	**OCHRONA KRYPTOGRAFICZNA**	
	SC-13[2]	*organizacja określa rodzaj kryptografii wymaganej dla każdego zastosowania; oraz*
	SC-13[3]	*system informacyjny wdraża zdefiniowane przez organizację zastosowania kryptograficzne oraz rodzaj kryptografii wymagany dla każdego zastosowania zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, zasadami, przepisami i standardami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony kryptograficznej; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; certyfikaty uwierzytelniające moduły kryptograficzne; lista uwierzytelnionych modułów kryptograficznych certyfikowanych przez stosowne organy; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za ochronę kryptograficzną]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające ochronę kryptograficzną].	

SC-13(1)	**OCHRONA KRYPTOGRAFICZNA | *KRYPTOGRAFIA STOSOWANA PRZEZ ORGANIZACJĘ***
[Włączone do: SC-13].	

SC-13(2)	**OCHRONA KRYPTOGRAFICZNA | *KRYPTOGRAFIA ZATWIERDZONA PRZEZ ORGANIZACJĘ***
[Włączone do: SC-13].	

SC-13(3)	**OCHRONA KRYPTOGRAFICZNA | *OSOBY NIEPOSIADAJĄCE FORMALNYCH ZEZWOLEŃ NA DOSTĘP***
[Włączone do: SC-13].	

SC-13(4)	**OCHRONA KRYPTOGRAFICZNA | *PODPISY CYFROWE***
[Włączone do: SC-13].	

SC-14	**OCHRONA DOSTĘPU PUBLICZNEGO**
[Zdolność zapewniona przez: AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].	

SC-15	**WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE**		
	CEL OCENY: *Określić, czy:*		
	SC-15(a)	**SC-15(a)[1]**	*organizacja określa wyjątki, w których dopuszcza się zdalną aktywację współpracujących urządzeń komputerowych;*
		SC-15(a)[2]	*system informacyjny zakazuje zdalnej aktywacji współpracujących urządzeń komputerowych, z wyjątkiem zdefiniowanych przez organizację wyjątków, gdzie zdalna aktywacja ma być dozwolona; oraz*
	SC-15(b)	*system informacyjny zapewnia użytkownikom korzystającym z urządzeń jednoznaczne wskazówki dotyczące użytkowania.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące współpracy informacyjnej; zasady i procedury kontroli dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za zarządzanie współpracującymi urządzeniami komputerowymi]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub implementujące zarządzanie zdalną aktywacją współpracujących urządzeń komputerowych; zautomatyzowane mechanizmy umożliwiające identyfikację użytkowania współpracującego urządzenia komputerowego].		

SC-15(1)	**WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | *ODŁĄCZENIE FIZYCZNE***
	CEL OCENY: *Ustalić, czy system informacyjny zapewnia fizyczne odłączenie współpracujących urządzeń komputerowych w sposób ułatwiający ich użytkowanie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące współpracy informacyjnej; zasady i procedury kontroli dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za zarządzanie współpracującymi urządzeniami komputerowymi]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające lub wdrażające fizyczne odłączanie współpracujących urządzeń komputerowych].

SC-15(2)	**WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | *BLOKOWANIE RUCHU WEJŚCIOWEGO / WYJŚCIOWEGO***
[Włączone do: SC-7].	

SC-15(3)	**WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | *DEZAKTYWACJA / USUWANIE W CHRONIONYCH OBSZARACH PRACY***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-15(3)[1]	*definiuje systemy informacyjne lub komponenty systemów informacyjnych, z których mają być wyłączone lub usunięte współpracujące urządzenia komputerowe;*
	SC-15(3)[2]	*definiuje bezpieczne miejsca pracy, w których współpracujące urządzenia komputerowe mają być wyłączane lub usuwane z systemów informacyjnych lub elementów systemów informacyjnych zainstalowanych w takich miejscach pracy; oraz*

SC-15(3)	**WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | *DEZAKTYWACJA / USUWANIE W CHRONIONYCH OBSZARACH PRACY***	
	SC-15(3)[3]	*wyłącza lub usuwa współpracujące urządzenia komputerowe ze zdefiniowanych w organizacji systemów informacyjnych lub komponentów systemów informacyjnych w zdefiniowanych w organizacji bezpiecznych obszarach pracy.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące współpracy informacyjnej; zasady i procedury kontroli dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; lista bezpiecznych miejsc pracy; systemy informacyjne lub elementy systemów informacyjnych w zabezpieczonych miejscach pracy, w których współpracujące urządzenia komputerowe mają być wyłączone lub usunięte; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie współpracującymi urządzeniami komputerowymi]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące możliwość wyłączenia współpracujących urządzeń komputerowych].	

SC-15(4)	**WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | *WYRAŹNIE WYKAZANIE AKTUALNYCH UŻYTKOWNIKÓW***	
	CEL OCENY: *Określić, czy:*	
	SC-15(4)[1]	*organizacja określa spotkania online oraz telekonferencje, w przypadku których wymagane jest dokładne wskazanie aktualnych uczestników; oraz*
	SC-15(4)[2]	*system informacyjny zapewnia dokładne wskazanie aktualnych uczestników określonych spotkań i telekonferencji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące współpracy informacyjnej; zasady i procedury kontroli dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z audytu systemu informacyjnego; wykaz rodzajów spotkań i telekonferencji wymagających	

SC-15(4)	**WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | *WYRAŹNIE WYKAZANIE AKTUALNYCH UŻYTKOWNIKÓW***
	wyraźnego wskazania aktualnych uczestników; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie współpracującymi urządzeniami komputerowymi]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące możliwość wskazywania poszczególnych uczestników na współpracujących urządzeniach komputerowych].

SC-16	**TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA**	
	CEL OCENY: *Określić, czy:*	
	SC-16[1]	*organizacja określa atrybuty bezpieczeństwa powiązane z wymianą informacji:*
		SC-16[1][a] *pomiędzy systemami informacyjnymi;*
		SC-16[1][b] *między elementami systemu;*
	SC-16[2]	*system informacyjny łączy zdefiniowane przez organizację atrybuty bezpieczeństwa z wymianą informacji:*
		SC-16[2][a] *pomiędzy systemami informacyjnymi; oraz*
		SC-16[2][b] *między elementami systemu;*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące transmisji atrybutów bezpieczeństwa; zasady i procedury kontroli dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające transmisję atrybutów bezpieczeństwa pomiędzy systemami informacyjnymi].	

SC-16(1)	**TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA | *OCENA INTEGRALNOŚCI***
	CEL OCENY: *Ustalić, czy system informacyjny sprawdza integralność transmitowanych atrybutów bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące transmisji atrybutów bezpieczeństwa; zasady i procedury kontroli dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające ocenę integralności przekazywanych atrybutów bezpieczeństwa].

SC-17	**CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-17[1]	*określa politykę w zakresie wydawania certyfikatów klucza publicznego;*
	SC-17[2]	*wydaje certyfikaty klucza publicznego:*
	SC-17[2][a]	*w ramach polityki certyfikacji określonej przez organizację: lub*
	SC-17[2][b]	*uzyskuje certyfikaty klucza publicznego od zatwierdzonego dostawcy usług.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące certyfikatów infrastruktury klucza publicznego; polityka w zakresie certyfikatów klucza publicznego; proces wydawania certyfikatów klucza publicznego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za wydawanie certyfikatów klucza publicznego; dostawcy usług].	

SC-17	**CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO**
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie certyfikatami infrastruktury klucza publicznego].

SC-18	**KOD MOBILNY**		
	CEL OCENY: *Określić, czy organizacja:*		
	SC-18(a)	*definiuje akceptowalny i niedopuszczalny kod mobilny oraz technologie kodu mobilnego;*	
	SC-18(b)	**SC-18(b)[1]**	*ustanawia ograniczenia użytkowania akceptowalnych kodów mobilnych i technologii kodów mobilnych;*
		SC-18(b)[2]	*ustanawia wskazówki dotyczące wdrażania akceptowalnych kodów mobilnych i technologii kodów mobilnych;*
	SC-18(c)	**SC-18(c)[1]**	*zezwala na korzystanie z kodu mobilnego w ramach systemu informacyjnego;*
		SC-18(c)[2]	*monitoruje korzystanie z kodów mobilnych w ramach systemu informacyjnego; oraz*
		SC-18(c)[3]	*kontroluje korzystanie z kodów mobilnych w ramach systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące kodu mobilnego; ograniczenia w korzystaniu z kodu mobilnego, polityka i procedury wdrażania kodu mobilnego; lista akceptowalnych kodów mobilnych i technologii kodów mobilnych; lista niedopuszczalnych kodów mobilnych i technologii mobilnych; rejestry autoryzacji; zapisy z monitoringu systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie kodem mobilnym].		

SC-18	**KOD MOBILNY**
	Test: [*wybierz spośród:* Proces organizacyjny dotyczący kontrolowania, autoryzacji, monitorowania i stosowania ograniczeń w kodach mobilnych; zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie kodami mobilnymi; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie kodów mobilnych].

SC-18(1)	**KOD MOBILNY | *IDENTYFIKACJA NIEDOPUSZCZALNEGO KOD / PODEJMOWANIE DZIAŁAŃ NAPRAWCZYCH***		
	CEL OCENY: *Określić, czy:*		
	SC-18(1)[1]	*organizacja określa niedopuszczalny kod mobilny do identyfikacji przez system informacyjny;*	
	SC-18(1)[2]	*organizacja określa działania korygujące, które należy podjąć, gdy system informacyjny zidentyfikuje zdefiniowany przez organizację niedopuszczalny kod mobilny;*	
	SC-18(1)[3]	*system informacyjny:*	
		SC-18(1)[3][a]	*identyfikuje zdefiniowany przez organizację niedopuszczalny kod mobilny; oraz*
		SC-18(1)[3][b]	*podejmuje określone organizacyjnie działania naprawcze.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące kodu mobilnego; ograniczenia w korzystaniu z kodu mobilnego, polityka i procedury wdrażania kodu mobilnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz niedopuszczalnego kodu mobilnego; wykaz działań naprawczych, które należy podjąć w przypadku stwierdzenia niedopuszczalnego kodu mobilnego; zapisy z monitoringu systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za zarządzanie kodem mobilnym]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wdrażające wykrywanie kodu mobilnego, kontrolę i możliwości naprawcze].		

SC-18(2)	**KOD MOBILNY |** ***NABYCIE / OPRACOWYWANIE / UŻYTKOWANIE***		
	CEL OCENY: *Określić, czy organizacja:*		
	SC-18(2)[1]	*określa wymagania dotyczące:*	
		SC-18(2)[1][a]	*nabycia kodu mobilnego;*
		SC-18(2)[1][b]	*opracowywania kodu mobilnego;*
		SC-18(2)[1][c]	*korzystania z kodu mobilnego; oraz*
	SC-18(2)[2]	*zapewnia, że nabycie, opracowanie i wykorzystanie kodu mobilnego przeznaczonego do wdrożenia w systemie informacyjnym spełnia określone przez organizację wymagania dotyczące kodu mobilnego.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące kodu mobilnego; wymagania na kod mobilny; ograniczenia w korzystaniu z kodu mobilnego, polityka i procedury wdrażania kodu mobilnego; dokumentacja nabycia; umowy nabycia systemu informacyjnego, komponentu systemu lub usługi systemu informacyjnego; dokumentacja cyklu życia systemu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie kodem mobilnym; personel organizacji odpowiedzialny za pozyskiwanie i realizację kontraktów]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z pozyskiwaniem, rozwojem i wykorzystaniem kodu mobilnego].		

SC-18(3)	**KOD MOBILNY |** ***ZAPOBIEGANIE POBIERANIU / WYKONANIU***	
	CEL OCENY: *Określić, czy:*	
	SC-18(3)[1]	*organizacja określa nieakceptowalny kod mobilny, którego pobieranie i wykonywanie należy uniemożliwiać;*
	SC-18(3)[2]	*system informacyjny uniemożliwia:*

SC-18(3) KOD MOBILNY | *ZAPOBIEGANIE POBIERANIU / WYKONANIU*			
		SC-18(3)[2][a]	*pobieranie zdefiniowanego przez organizację niedopuszczalnego kodu mobilnego; oraz*
		SC-18(3)[2][b]	*wykonanie zdefiniowanego przez organizację niedopuszczalnego kodu mobilnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące kodu mobilnego; ograniczenia w korzystaniu z kodu mobilnego, polityka i procedury wdrażania kodu mobilnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za zarządzanie kodem mobilnym]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zapobiegające pobieraniu i wykonywaniu niedopuszczalnego kodu mobilnego].		

SC-18(4) KOD MOBILNY | *ZAPOBIEGANIE AUTOMATYCZNEMU WYKONANIU*		
	CEL OCENY: *Określić, czy:*	
	SC-18(4)[1]	*organizacja określa aplikacje programowe, w których automatyczne wykonywanie kodu mobilnego ma być zabronione;*
	SC-18(4)[2]	*organizacja określa działania, które system informacyjny ma egzekwować przed wykonaniem kodu mobilnego;*
	SC-18(4)[3]	*system informacyjny uniemożliwia automatyczne wykonanie kodu mobilnego w aplikacjach programowych zdefiniowanych przez organizację; oraz*
	SC-18(4)[4]	*system informacyjny wymusza działania zdefiniowane przez organizację przed wykonaniem kodu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące kodu mobilnego; ograniczenia użytkowania kodu mobilnego; polityka i procedury wdrażania kodu mobilnego; dokumentacja projektowa systemu	

SC-18(4)	**KOD MOBILNY | *ZAPOBIEGANIE AUTOMATYCZNEMU WYKONANIU***
	informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz aplikacji programowych, dla których automatyczne wykonywanie kodu mobilnego jest zabronione; wykaz czynności wymaganych przed wykonaniem kodu mobilnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za zarządzanie kodem mobilnym]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy zapobiegające automatycznemu wykonaniu niedopuszczalnego kodu mobilnego; zautomatyzowane mechanizmy egzekwujące działania, które należy podjąć przed wykonaniem kodu mobilnego].

SC-18(5)	**KO MOBILNY | *POZWALANIE NA WYKONANIE TYLKO W OGRANICZONYCH ŚRODOWISKACH***
	CEL OCENY: *Określić, czy organizacja pozwala na wykonanie dozwolonego kodu mobilnego tylko w ograniczonych środowiskach maszyn wirtualnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące kodu mobilnego; uprawnienia do użytkowania kodu mobilnego; ograniczenia użytkowania kodu mobilnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista ograniczonych środowisk maszyn wirtualnych, dla których dozwolone jest wykonanie akceptowalnego organizacyjnie kodu mobilnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji odpowiedzialny za zarządzanie kodem mobilnym]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy pozwalające na wykonanie dozwolonego kodu mobilnego w ograniczonych środowiskach maszyn wirtualnych].

<table>
<tr><th colspan="4">SC-19 PROTOKÓŁ TRANSMISJI PAKIETOWEJ (VoIP)</th></tr>
<tr><td></td><td colspan="3">CEL OCENY:
Określić, czy organizacja:</td></tr>
<tr><td></td><td>SC-19(a)</td><td>SC-19(a)[1]</td><td>ustanawia ograniczenia użytkowania protokołu transmisji pakietowej (VoIP) uwzględniając potencjalne uszkodzenie systemu informacyjnego w przypadku złośliwego użycia;</td></tr>
<tr><td></td><td></td><td>SC-19(a)[2]</td><td>ustanawia wytyczne dotyczące wdrażania protokołu transmisji pakietowej (VoIP) uwzględniając potencjalne uszkodzenie systemu informacyjnego w przypadku złośliwego użycia;</td></tr>
<tr><td></td><td>SC-19(b)</td><td>SC-19(b)[1]</td><td>zezwala na wykorzystanie protokołu VoIP w ramach systemu informacyjnego;</td></tr>
<tr><td></td><td></td><td>SC-19(b)[2]</td><td>monitoruje wykorzystanie VoIP w ramach systemu informacyjnego; oraz</td></tr>
<tr><td></td><td></td><td>SC-19(b)[3]</td><td>kontroluje wykorzystanie VoIP w systemie informacyjnym.</td></tr>
<tr><td></td><td colspan="3">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka ochrony systemu i komunikacji; procedury dotyczące VoIP; ograniczenia w korzystaniu z VoIP; wskazówki dotyczące wdrażania VoIP; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy z monitoringu systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie technologią VoIP].
Test: [wybierz spośród: Proces organizacyjny autoryzacji, monitorowania i kontroli VoIP; zautomatyzowane mechanizmy wspierające i/lub wdrażające autoryzację, monitorowanie i kontrolę VoIP].</td></tr>
</table>

SC-20	**BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)**		
	CEL OCENY: *Ustalić, czy system informacyjny:*		
	SC-20(a)	*zapewnia dodatkowe źródło danych oraz artefakty weryfikujące integralność wraz z autorytatywnymi informacjami o rozpoznawalności nazwy, które system zwraca w odpowiedzi na zewnętrzne zapytania dotyczące rozpoznawalności nazwy/adresu zewnętrznego;*	
	SC-20(b)	*zapewnia środki umożliwiające, w przypadku gdy działają one w ramach rozproszonej, hierarchicznej przestrzeni nazw:*	
		SC-20(b)[1]	*wskazywanie statusu bezpieczeństwa stref podrzędnych (jeśli ta podrzędna strefa zapewnia obsługę środków bezpieczeństwa); oraz*
		SC-20(b)[2]	*weryfikację łańcucha zaufania między domenami nadrzędnymi i podrzędnymi.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące bezpiecznej usługi rozwiązywania problemów związanych z nazwą/adresem (autorytatywne źródło); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie DNS]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające bezpieczną usługę rozwiązywania problemów związanych z nazwą/adresem].		

SC-20(1)	**BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA) | *STREFA PODRZĘDNA (PODPRZESTRZEŃ)***
[Włączone do: SC-20].	

SC-20(2)	**BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA) |** ***INTEGRALNOŚĆ DANYCH***
	CEL OCENY: *Ustalić, czy system informacyjny zapewnia artefakty ochrony pochodzenia i integralności danych wewnętrznych zapytań dotyczących rozpoznawania nazw / adresów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące bezpiecznej usługi rozwiązywania problemów związanych z nazwą/adresem (autorytatywne źródło); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie DNS]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające ochronę pochodzenia danych oraz ochronę integralności dla wewnętrznych zapytań dotyczących usług w zakresie rozróżniania nazw/adresów].

SC-21	**BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP**	
	CEL OCENY: *Ustalić, czy system informacyjny:*	
	SC-21[1]	*żąda uwierzytelnienia pochodzenia danych w odpowiedzi na rozpoznanie nazwy / adresu otrzymanej przez system z wiarygodnych źródeł;*
	SC-21[2]	*żąda weryfikacji integralności danych w odpowiedzi na rozpoznanie nazwy / adresu otrzymanej przez system z wiarygodnych źródeł;*
	SC-21[3]	*dokonuje uwierzytelnienia pochodzenia danych w odpowiedzi na rozpoznanie nazwy / adresu otrzymanej przez system z wiarygodnych źródeł; oraz*
	SC-21[4]	*przeprowadza weryfikację integralności danych w odpowiedzi na rozpoznanie nazwy / adresu otrzymanej przez system z wiarygodnych źródeł.*

SC-21	**BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące bezpiecznej usługi rozwiązywania problemów związanych z nazwą/adresem (rozwiązanie rekurencyjne lub buforowanie); dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie DNS]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające uwierzytelnianie pochodzenia danych oraz weryfikację integralności danych w odniesieniu do usług w zakresie rozdzielczości nazw/adresów].

SC-21(1)	**BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP | *INTEGRALNOŚĆ***
[Włączone do: SC-21].	

SC-22	**ARCHITEKTURA NAZW DOMEN / ADRESÓW IP / ZAMAWIANIE USŁUGI DNS**	
	CEL OCENY: *Ustalić, czy systemy informacyjne, które łącznie zapewniają organizacji usługę rozpoznawania nazw / adresów:*	
	SC-22[1]	*są odporne na błędy; oraz*
	SC-22[2]	*wdrażają wewnętrzny/zewnętrzny rozdział ról.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące architektury i świadczenia usługi rozwiązywania problemów związanych z nazwą/adresem; zasady i procedury kontroli dostępu; dokumentacja projektowa systemu informacyjnego; wyniki oceny niezależnych, sprawdzających organizacji; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

SC-22	**ARCHITEKTURA NAZW DOMEN / ADRESÓW IP / ZAMAWIANIE USŁUGI DNS**
	Wywiad: [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zarządzanie DNS]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące usługę rozpoznawania nazw/adresów w celu zapewnienia odporności na błędy oraz separację ról].

SC-23	**AUTENTYCZNOŚĆ SESJI**
	CEL OCENY: *Ustalić, czy system informacyjny zapewnia ochronę autentyczności sesji komunikacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące autentyczności sesji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające sesję autentyczności].

SC-23(1)	**AUTENTYCZNOŚĆ SESJI | *UNIEWAŻNIENIE IDENTYFIKATORÓW SESJI PO WYLOGOWANIU***
	CEL OCENY: *Ustalić, czy system informacyjny unieważnia identyfikatory sesji po wylogowaniu się użytkownika lub innym zakończeniu sesji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące autentyczności sesji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].

SC-23(1)	**AUTENTYCZNOŚĆ SESJI | *UNIEWAŻNIENIE IDENTYFIKATORÓW SESJI PO WYLOGOWANIU***
	Wywiad: [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające unieważnienie identyfikatora sesji po zakończeniu sesji].

SC-23(2)	**AUTENTYCZNOŚĆ SESJI | *WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA / WYŚWIETLANIE WIADOMOŚCI***
[Włączone do: AC-12(1)].	

SC-23(3)	**AUTENTYCZNOŚĆ SESJI | *LOSOWE UNIKALNE IDENTYFIKATORY SESJI***	
	CEL OCENY: *Określić, czy:*	
	SC-23(3)[1]	*Organizacja, w celu wygenerowania niepowtarzalnego identyfikatora sesji dla każdej poszczególnej sesji, określa wymagania dotyczące losowości;*
	SC-23(3)[2]	*system informacyjny generuje niepowtarzalny identyfikator sesji dla każdej sesji o zdefiniowanych przez organizację wymaganiach dotyczących losowości; oraz*
	SC-23(3)[3]	*system informacyjny rozpoznaje tylko te identyfikatory sesji, które są generowane przez system.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące autentyczności sesji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające generowanie i monitorowanie niepowtarzalnych identyfikatorów sesji; zautomatyzowane mechanizmy wspierające i/lub wdrażające wymagania dotyczące losowości].	

SC-23(4) AUTENTYCZNOŚĆ SESJI | *LOSOWE UNIKALNE IDENTYFIKATORY SESJI*
[Włączone do: SC-23(3)].

SC-23(5) AUTENTYCZNOŚĆ SESJI | *AUTORYZOWANE URZĘDY CERTYFIKACYJNE*		
	CEL OCENY: *Określić, czy:*	
	SC-23(5)[1]	*organizacja określa urzędy wydające certyfikaty, które mają być uprawnione do weryfikacji ustanawiania chronionych sesji; oraz*
	SC-23(5)[2]	*system informacyjny pozwala na wykorzystanie jedynie zdefiniowanych przez organizację organów certyfikacyjnych do weryfikacji ustanowienia chronionych sesji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące autentyczności sesji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz organów certyfikujących dopuszczonych do weryfikacji ustanowienia sesji chronionych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zasady zarządzania wydawanymi certyfikatami wydawanymi przez urzędy certyfikacyjne].	

SC-24 PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE		
	CEL OCENY: *Określić, czy:*	
	SC-24[1]	*organizacja określa znany stan bezpieczny (po błędzie), do którego system informacyjny przechodzi w przypadku awarii systemu;*

SC-24	**PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE**	
	SC-24[2]	*organizacja określa rodzaje awarii, w przypadku których system informacyjny ma zostać uruchomiony w określonym przez organizację znanym stanie bezpiecznym;*
	SC-24[3]	*organizacja określa informacje o stanie systemu, które mają być zachowane w przypadku awarii systemu;*
	SC-24[4]	*system informacyjny przechodzi do zdefiniowanego przez organizację znanego stanu bezpiecznego w przypadku określonych przez organizację rodzajów awarii; oraz*
	SC-24[5]	*system informacyjny zachowuje informacje o stanie systemu zdefiniowanego przez organizację w przypadku awarii systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące awarii systemu informacyjnego w znanym stanie; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz awarii wymagających przejścia systemu informacyjnego do określonego stanu bezpiecznego; informacje o stanie bezpiecznym w przypadku awarii systemu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające lub wdrażające znany stan bezpieczny w przypadku wystąpienia awarii; zautomatyzowane mechanizmy zachowujące informacje o stanie systemu na wypadek awarii systemu].	

SC-25	**THIN NODES / TERMINALOWE STACJE ROBOCZE**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-25[1]	*definiuje komponenty systemu informacyjnego o ograniczonej funkcjonalnością i pamięci; oraz*
	SC-25[2]	*wykorzystuje zdefiniowane przez organizację komponenty systemu informacyjnego o minimalnej funkcjonalności oraz pojemności przechowywania informacji.*

SC-25	**THIN NODES / TERMINALOWE STACJE ROBOCZE**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące używania terminalowych stacji roboczych (Thin Nodes; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające terminalowe stacje robocze (Thin Nodes)].

SC-26	**HONEY POTS**
	CEL OCENY: *Ustalić, czy system informacyjny zawiera komponenty specjalnie zaprojektowane (tzw. wabiki), jako cel złośliwych ataków, w celu wykrywania, odbijania i analizowania takich ataków.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące używania Honey Pots; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające Honey Pots].

SC-26(1)	**HONEY POTS | *WYKRYWANIE ZŁEGO KODU***
[Włączone do: SC-35].	

SC-27	**WIELOPLATFORMOWOŚĆ APLIKACJI**	
	CEL OCENY: *Określić, czy:*	
	SC-27[1]	*organizacja określa aplikacje niezależne od platform (wieloplatformowość aplikacji); oraz*
	SC-27[2]	*system informacyjny zawiera aplikacje niezależne od platformy organizacyjnej (wieloplatformowość aplikacji).*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące wieloplatformowości aplikacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista aplikacji niezależnych od platformy; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące wieloplatformowość aplikacji].	

SC-28	**OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU**		
	CEL OCENY: *Określić, czy:*		
	SC-28[1]	*organizacja określa informacje w stanie spoczynku wymagające jednego lub kilku z poniższych elementów:*	
		SC-28[1][a]	*ochrony poufności; i/lub*
		SC-28[1][b]	*ochrony integralności;*
	SC-28[2]	*system informacyjny chroni:*	
		SC-28[2][a]	*poufność informacji zdefiniowanych przez organizację w stanie spoczynku; i/lub*
		SC-28[2][b]	*integralność informacji zdefiniowanych przez organizację w stanie spoczynku.*

SC-28	**OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony danych w składowaniu / kopii konfiguracji systemu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; mechanizmy kryptograficzne i związana z nimi dokumentacja konfiguracyjna; wykaz informacji w stanie spoczynku wymagających poufności i ochrony integralności; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające ochronę poufności i integralności informacji w stanie spoczynku].

SC-28(1)	**OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU | *OCHRONA KRYPTOGRAFICZNA***	
	CEL OCENY: *Określić, czy:*	
	SC-28(1)[1]	*organizacja określa informacje wymagające ochrony kryptograficznej;*
	SC-28(1)[2]	*organizacja określa komponenty systemu informacyjnego zawierające informacje wymagające ochrony kryptograficznej; oraz*
	SC-28(1)[3]	*system informacyjny wykorzystuje mechanizmy kryptograficzne zapobiegające nieautoryzowanemu ujawnieniu oraz modyfikacji zdefiniowanych przez organizację informacji o komponentach systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony danych w składowaniu / kopii konfiguracji systemu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; mechanizmy kryptograficzne i związana z nimi dokumentacja konfiguracyjna; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające ochronę poufności i integralności informacji w stanie spoczynku].	

SC-28(2)	**OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU | *PRZECHOWYWANIE OFF-LINE***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-28(2)[1]	*definiuje informacje, które mają być usuwane z pamięci masowej online oraz przechowywane off-line w bezpiecznym środowisku; oraz*
	SC-28(2)[2]	*usuwa z pamięci masowej online informacje zdefiniowane przez organizację; oraz*
	SC-28(2)[3]	*przechowuje off-line zdefiniowane organizacyjnie informacje w bezpiecznej lokalizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ochrony danych w składowaniu / kopii konfiguracji systemu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; mechanizmy kryptograficzne i związana z nimi dokumentacja konfiguracyjna; lokalizacje przechowywania off-line informacji w stanie spoczynku; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy obsługujące lub wdrażające usuwanie informacji z systemu przechowywania online; zautomatyzowane mechanizmy obsługujące lub wdrażające przechowywanie informacji w trybie off-line].	

SC-29	**HETEROGENICZNOŚĆ SYSTEMU**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-29[1]	*definiuje komponenty systemu informacyjnego wymagające zastosowania różnorodnego zestawu technologii informacyjnych do wdrożenia systemu informacyjnego; oraz*

SC-29	**HETEROGENICZNOŚĆ SYSTEMU**	
	SC-29[2]	*stosuje różnorodne technologie informacyjne w komponentach systemu informacyjnego zdefiniowanych przez organizację w ramach wdrażania systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz technologii stosowanych w systemie informacyjnym; dokumentacja nabycia; umowy nabycia komponentów lub usług systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za nabywanie, rozwój i wdrażanie systemów informacyjnych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające stosowanie zróżnicowanego zestawu technologii informacyjnych].	

SC-29(1)	**HETEROGENICZNOŚĆ SYSTEMU | *TECHNIKI WIRTUALIZACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-29(1)[1]	*definiuje częstotliwość zmiany różnorodności systemów operacyjnych oraz aplikacji wdrażanych z wykorzystaniem technik wirtualizacji; oraz*
	SC-29(1)[2]	*stosuje techniki wirtualizacji w celu wsparcia wdrażania różnorodnych systemów operacyjnych oraz aplikacji, zmienianych z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; polityka i procedury zarządzanie konfiguracją; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; wykaz systemów operacyjnych i aplikacji wdrożonych z wykorzystaniem techniki wirtualizacji; rejestry zabezpieczeń zmian; rejestry zarządzania konfiguracją; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za wdrożenie zatwierdzonej techniki wirtualizacji do systemu informacyjnego].	

SC-29(1)	**HETEROGENICZNOŚĆ SYSTEMU | *TECHNIKI WIRTUALIZACJI***
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające wykorzystanie zróżnicowanego zestawu technologii informacyjnych; zautomatyzowane mechanizmy wspierające i/lub wdrażające techniki wirtualizacji].

SC-30	**MASKOWANIE I DEZINFORMACJA**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-30[1]	*definiuje techniki maskowania i dezinformacji, które mają być stosowane w celu dezorientacji i wprowadzania w błąd przeciwników potencjalnie ukierunkowanych na organizacyjne systemy informacyjne;*
	SC-30[2]	*definiuje systemy informacyjne, w których mają być stosowane określone przez organizację techniki maskowania i dezinformacji;*
	SC-30[3]	*definiuje okresy czasu, w których należy stosować określone przez organizację techniki maskowania i dezinformacji określonych przez organizację systemów informacyjnych; oraz*
	SC-30[4]	*stosuje zdefiniowane organizacyjnie techniki maskowania i dezinformacji zdefiniowanych organizacyjnie systemów informacyjnych w określonych przedziałach czasowych, w celu dezorientacji i wprowadzania w błąd przeciwników.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące technik maskowania i dezinformacji systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; lista technik maskowania i dezinformacji stosowanych w systemach informacyjnych organizacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za wdrażanie technik maskowania i dezinformacji w systemach informacyjnych]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające techniki maskowania i dezinformacji].	

SC-30(1) MASKOWANIE I DEZINFORMACJA | *TECHNIKI WIRTUALIZACJI*
[Włączone do: SC-29(1)].

SC-30(2) MASKOWANIE I DEZINFORMACJA | *LOSOWOŚĆ*		
	CEL OCENY: *Określić, czy organizacja:*	
	SC-30(2)[1]	*definiuje techniki, które należy stosować w celu wprowadzenia losowości do operacji organizacyjnych oraz zasobów; oraz*
	SC-30(2)[2]	*wykorzystuje zdefiniowane przez organizację techniki wprowadzania losowości do operacji organizacyjnych i zasobów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące technik maskowania i dezinformacji systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; lista technik, które należy stosować w celu wprowadzenia losowości do operacji organizacyjnych oraz zasobów; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za wdrażanie technik maskowania i dezinformacji w systemach informacyjnych. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące losowość, jako technikę maskowania i dezinformacji].	

SC-30(3) MASKOWANIE I DEZINFORMACJA | *ZMIANA LOKALIZACJI PRZETWARZANIA / PRZECHOWYWANIA*		
	CEL OCENY: *Określić, czy organizacja:*	
	SC-30(3)[1]	*definiuje miejsca przetwarzania i/lub przechowywania, które mają być zmieniane w odstępach czasu określonych przez organizację;*
	SC-30(3)[2]	*definiuje częstotliwość zmiany lokalizacji przetwarzania i/lub przechowywania zdefiniowanej przez organizację; oraz*

SC-30(3)	**MASKOWANIE I DEZINFORMACJA | *ZMIANA LOKALIZACJI PRZETWARZANIA / PRZECHOWYWANIA***		
	SC-30(3)[3]	*zmienia lokalizację zdefiniowanego przez organizację przetwarzania i/lub przechowywania w jeden z poniższych sposobów:*	
		SC-30(3)[3][a]	*organizacyjnie określonych przedziałach czasowych; lub*
		SC-30(3)[3][b]	*losowych odstępach czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące technik maskowania i dezinformacji systemu informacyjnego; lista miejsc przetwarzania/magazynowania, które należy zmieniać w organizacyjnie określonych odstępach czasu; rejestry zabezpieczeń zmian; rejestry zarządzania konfiguracją; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za zmianę miejsca przetwarzania i/lub składowania]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zmiany lokalizacji przetwarzania i/lub przechowywania].	

SC-30(4)	**MASKOWANIE I DEZINFORMACJA | *INFORMACJE DEZINFORMUJĄCE***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-30(4)[1]	*definiuje komponenty systemu informacyjnego, w których należy stosować wiarygodne, lecz dezinformujące informacje dotyczące jego stanu bezpieczeństwa lub sposobu funkcjonowania; oraz*
	SC-30(4)[2]	*wykorzystuje wiarygodne, lecz dezinformujące informacje w organizacyjnie zdefiniowanych komponentach systemu informacyjnego dotyczące jego stanu bezpieczeństwa lub sposobu funkcjonowania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące technik maskowania i dezinformacji systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji	

SC-30(4)	**MASKOWANIE I DEZINFORMACJA | *INFORMACJE DEZINFORMUJĄCE***
	systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za definiowanie i wykorzystywanie rzeczywistych, lecz dezinformujących informacji o stanie bezpieczeństwa komponentów systemu informacyjnego]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące wykorzystanie realistycznych, lecz dezinformujących informacji o stanie bezpieczeństwa komponentów systemu informacyjnego].

SC-30(5)	**MASKOWANIE I DEZINFORMACJA | *UKRYWANIE KOMPONENTÓW SYSTEMU***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-30(5)[1]	*definiuje techniki, które należy stosować w celu ukrywania lub maskowania komponentów systemu informacyjnego;*
	SC-30(5)[2]	*definiuje komponenty systemu informacyjnego, które mają być ukryte lub zamaskowane przy użyciu technik zdefiniowanych przez organizację; oraz*
	SC-30(5)[3]	*wykorzystuje zdefiniowane przez organizację techniki ukrywania lub maskowania komponentów systemu informacyjnego opracowanego przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące technik maskowania i dezinformacji systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz technik stosowanych w celu ukrycia lub zamaskowania komponentów systemu informacyjnego; wykaz komponentów systemu informacyjnego, które należy ukryć lub zamaskować; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za ukrywanie/maskowanie komponentów systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające techniki ukrywania/maskowania komponentów systemu].	

SC-31	**ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-31(a)	*wykonuje analizę ukrytego kanału komunikacji w celu zidentyfikowania tych aspektów komunikacji w ramach systemu informacyjnego, które są potencjalnymi drogami dla jednego lub kilku z poniższych:*
	SC-31(a)[1]	*ukrytych kanałów przechowywania; i/lub*
	SC-31(a)[2]	*ukrytych kanałów synchronizacji; oraz*
	SC-31(b)	*szacuje maksymalną przepustowość tych kanałów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące analizy ukrytego kanału komunikacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja analizy ukrytego kanału komunikacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za analizę kanałów ukrytych; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Proces organizacyjny prowadzenia analizy ukrytego kanału komunikacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające analizę ukrytego kanału komunikacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwość oszacowania przepustowości ukrytych kanałów].	

SC-31(1)	**ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | *TESTOWANIE KANAŁÓW UKRYTYCH***
	CEL OCENY: *Ustalenie, czy organizacja testuje podzbiór zidentyfikowanych ukrytych kanałów, aby określić, które z nich są odpowiednie do wyzyskiwania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące analizy ukrytego kanału komunikacji; dokumentacja projektowa

SC-31(1)	**ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | *TESTOWANIE KANAŁÓW UKRYTYCH***
	systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista ukrytych kanałów; dokumentacja analizy ukrytego kanału komunikacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za analizę ukrytych kanałów]. **Test**: [*wybierz spośród:* Proces organizacyjny testowania kanałów ukrytych; zautomatyzowane mechanizmy wspierające i/lub wdrażające testowanie analizy kanałów ukrytych].

SC-31(2)	**ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | *MAKSYMALNA PRZEPUSTOWOŚĆ ŁĄCZA***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-31(2)[1]	*określa maksymalną przepustowość łącza dozwoloną dla zidentyfikowanych ukrytych kanałów; oraz*
	SC-31(2)[2]	*redukuje maksymalną przepustowość łącza do wartości zdefiniowanych organizacyjnie dla jednej lub kilku z poniższych zidentyfikowanych wartości dotyczących ukrytych kanałów:*
		SC-31(2)[2][a] *przechowywania; i/lub*
		SC-31(2)[2][b] *synchronizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące analizy ukrytego kanału komunikacji; umowy nabycia systemów lub usług informacyjnych; dokumentacja nabycia; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja analizy ukrytego kanału komunikacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za analizę kanałów ukrytych; deweloperzy systemów informacyjnych/integratorzy].	

SC-31(2)	**ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | *MAKSYMALNA PRZEPUSTOWOŚĆ ŁĄCZA***
	Test: [*wybierz spośród:* Proces organizacyjny prowadzenia analizy ukrytego kanału komunikacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające analizę ukrytego kanału komunikacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwość zmniejszenia szerokości pasma kanałów ukrytych].

SC-31(3)	**ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | *POMIAR PRZEPUSTOWOŚCI W ŚRODOWISKU OPERACYJNYM***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-31(3)[1]	*definiuje podzbiór zidentyfikowanych ukrytych kanałów, których szerokość pasma ma być mierzona w środowisku operacyjnym systemu informacyjnego; oraz*
	SC-31(3)[2]	*mierzy szerokość pasma określonego przez organizację podzbioru zidentyfikowanych ukrytych kanałów w środowisku operacyjnym systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące analizy ukrytego kanału komunikacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja analizy ukrytego kanału komunikacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za analizę kanałów ukrytych; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Proces organizacyjny prowadzenia analizy ukrytego kanału komunikacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające analizę ukrytego kanału komunikacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające zdolność do pomiaru szerokości pasma kanałów ukrytych].	

SC-32	**DZIELENIE SYSTEMU INFORMACYJNEGO NA PARTYCJE**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-32[1]	*definiuje warunki fizycznego rozdzielenia komponentów systemu informacyjnego na partycje systemu informacyjnego;*
	SC-32[2]	*definiuje komponenty systemu informacyjnego przeznaczone do rezydowania w oddzielnych domenach fizycznych lub środowiskach w oparciu o zdefiniowane przez organizację uwarunkowania fizycznego rozdzielenia komponentów; oraz*
	SC-32[3]	*partycjonuje system informacyjny na zdefiniowane przez organizację komponenty systemu informacyjnego rezydujące w oddzielnych fizycznych domenach lub środowiskach w oparciu o zdefiniowane przez organizację uwarunkowania fizycznego rozdzielenia komponentów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące dzielenie systemu informacyjnego na partycje; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; wykaz fizycznych domen (lub środowisk) systemu informacyjnego; schematy infrastruktury systemu informacyjnego; schematy sieciowe systemów informacyjnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające fizyczne odseparowanie komponentów systemu informacyjnego].	

SC-33	**INTEGRALNOŚĆ TRANSMISJI**
[Włączone do: SC-8].	

<table>
<tr><th colspan="4">SC-34 NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE</th></tr>
<tr><td></td><td colspan="3">CEL OCENY:
Określić, czy:</td></tr>
<tr><td></td><td>SC-34[1]</td><td colspan="2">organizacja określa komponenty systemu informacyjnego, dla których środowisko operacyjne oraz aplikacje zdefiniowane przez organizację mają być ładowane oraz wykonywane z nośników, wymuszonych sprzętowo tylko do odczytu;</td></tr>
<tr><td></td><td>SC-34[2]</td><td colspan="2">organizacja określa aplikacje, które mają być wczytywane i uruchamiane z nośników, wymuszonych sprzętowo tylko do odczytu;</td></tr>
<tr><td></td><td rowspan="3">SC-34[3]</td><td colspan="2">system informacyjny, w którego zdefiniowanych przez organizację komponentach systemu informacyjnego:</td></tr>
<tr><td>SC-34[3](a)</td><td>wczytuje i wykonuje środowisko operacyjne z nośników wymuszonych sprzętowo tylko do odczytu; oraz</td></tr>
<tr><td>SC-34[3](b)</td><td>wczytuje i wykonuje zdefiniowane organizacyjnie aplikacje z nośników wymuszonych sprzętowo tylko do odczytu.</td></tr>
<tr><td></td><td colspan="3">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka ochrony systemu i komunikacji; procedury dotyczące niemodyfikowalnych programów wykonywalnych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; lista komponentów systemu operacyjnego do wczytania z nośnika sprzętowego tylko do odczytu; lista aplikacji do wczytania z nośnika sprzętowego tylko do odczytu; używane nośniki do wczytywania i wykonywania aplikacji systemu informacyjnego; używane nośniki do wczytywania i wykonywania aplikacji systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych/integratorzy].
Test: [wybierz spośród: Zautomatyzowane mechanizmy obsługujące i/lub implementujące ładowanie oraz uruchamianie środowiska operacyjnego z nośników sprzętowych tylko do odczytu; zautomatyzowane mechanizmy obsługujące i/lub implementujące ładowanie oraz uruchamianie aplikacji z nośników sprzętowych tylko do odczytu].</td></tr>
</table>

SC-34(1)	**NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | *NIEZAPISYWALNE PAMIĘCI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-34(1)[1]	*definiuje komponenty systemu informacyjnego z niezapisywalnymi pamięciami; oraz*
	SC-34(1)[2]	*wykorzystuje zdefiniowane przez organizację komponenty systemu informacyjnego z niezapisywalnymi pamięciami, których zawartość pozostaje niezmienna po ponownym uruchomieniu komponentu lub włączeniu / wyłączeniu zasilania.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące niemodyfikowalnych programów wykonywalnych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; wykaz komponentów systemu informacyjnego, które mają być użytkowane bez możliwości zapisu danych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy obsługujące lub wdrażające wykorzystanie komponentów bez możliwości zapisu; zautomatyzowane mechanizmy obsługujące lub wdrażające trwałe przechowywanie bez możliwości zapisu po ponownym uruchomieniu komponentów oraz włączeniu/wyłączeniu zasilania].	

SC-34(2)	**NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | *OCHRONA INTEGRALNOŚCI / MEDIA TYLKO DO ODCZYTU***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-34(2)[1]	*chroni integralność informacji przechowywanej na nośnikach tylko do odczytu; oraz*
	SC-34(2)[2]	*zabezpiecza nośniki po zapisaniu na nich informacji.*

SC-34(2)	**NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | *OCHRONA INTEGRALNOŚCI / MEDIA TYLKO DO ODCZYTU***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące niemodyfikowalnych programów wykonywalnych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy obsługujące lub implementujące funkcje ochrony integralności informacji na nośnikach przeznaczonych tylko do odczytu, przed ich nieautoryzowanym zapisaniem oraz po zapisaniu na nich informacji].

SC-34(3)	**NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | *OCHRONA SPRZĘTOWA***		
	CEL OCENY: *Określić, czy organizacja:*		
	SC-34(3)(a)	**SC-34(3)(a)[1]**	*definiuje składniki oprogramowania układowego systemu informacyjnego, które mają być zabezpieczone sprzętowo przed zapisem;*
		SC-34(3)(a)[2]	*stosuje sprzętową, zabezpieczającą przed zapisem, ochronę zdefiniowanych przez organizację składników oprogramowania układowego systemu informacyjnego;*
	SC-34(3)(b)	**SC-34(3)(b)[1]**	*definiuje osoby upoważnione do ręcznego wyłączania ochrony przed zapisem sprzętowym w przypadku modyfikacji oprogramowania sprzętowego oraz ponownego włączania ochrony przed zapisem przed powrotem do trybu operacyjnego; oraz*

SC-34(3)	**NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | *OCHRONA SPRZĘTOWA***		
		SC-34(3)(b)[2]	*wprowadza określone procedury wśród zdefiniowanych przez organizację osób upoważnionych do ręcznego wyłączania ochrony przed zapisem sprzętu w przypadku modyfikacji oprogramowania sprzętowego oraz ponownego włączania ochrony przed zapisem przed powrotem do trybu operacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące modyfikacji oprogramowania układowego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z modyfikacją oprogramowania układowego; zautomatyzowane mechanizmy wspierające i/lub wdrażające sprzętową ochronę oprogramowania układowego przed zapisem].		

SC-35	**HONEYCLIENTS**
	CEL OCENY: *Ustalić, czy system informacyjny zawiera elementy, które proaktywnie dążą do identyfikacji złośliwych stron internetowych i/lub złośliwego kodu internetowego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące „honeyclients"; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; komponenty systemu informacyjnego stosowane do identyfikacji złośliwych stron internetowych i/lub złośliwego kodu internetowego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych/integratorzy].

SC-35	**HONEYCLIENTS**
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające „honeyclients”].

SC-36	**PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-36[1]	*definiuje procesy przetwarzanie i przechowywanie, które mają być realizowane w wielu fizycznych lokalizacjach; oraz*
	SC-36[2]	*dystrybuuje zdefiniowane przez organizację procesy przetwarzania i przechowywania w wielu rozproszonych fizycznych lokalizacjach.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; polityka i procedury planowania ciągłości działania; plan ciągłości działania; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; wykaz fizycznych lokalizacji (lub środowisk) systemu informacyjnego z rozproszonym przetwarzaniem i przechowywaniem; schematy obiektów systemu informacyjnego; umowy dotyczące miejsc przetwarzania; umowy dotyczące miejsc składowania; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za planowanie ciągłości działania i realizację planów; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące do rozpraszania przetwarzania i przechowywania w wielu fizycznych lokalizacjach; zautomatyzowane mechanizmy obsługujące i/lub wdrażające możliwości rozpraszania przetwarzania i przechowywania w wielu fizycznych lokalizacjach].	

SC-36(1)	**PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE | *PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE***
	CEL OCENY: *Określić, czy organizacja:*

SC-36(1)	**PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE | *PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE***	
	SC-36(1)[1]	*definiuje komponenty przetwarzania i przechowywania rozproszonego, dla których przetwarzanie i przechowywanie rozproszone ma być stosowane do identyfikacji potencjalnych usterek, błędów lub naruszeń; oraz*
	SC-36(1)[2]	*wykorzystuje przetwarzanie i przechowywanie rozproszone do identyfikacji potencjalnych usterek, błędów lub naruszeń zdefiniowanych w organizacji komponentów przetwarzania i przechowywania rozproszonego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; wykaz elementów składowych przetwarzania i przechowywania rozproszonego poddanych badaniu statystycznemu; rozproszony system informacyjny oraz związana z nim dokumentacja lub rejestry; rejestr audytów system informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające przetwarzanie i przechowywanie rozproszone].	

SC-37	**KANAŁY POZAPASMOWE**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-37[1]	*definiuje kanały pozapasmowe jako narzędzie do fizycznego dostarczania lub elektronicznej transmisji informacji, komponentów systemu informacyjnego lub urządzeń do osób lub systemów informacyjnych;*
	SC-37[2]	*definiuje informacje, elementy systemu informacyjnego lub urządzenia, których fizyczne dostarczenie lub elektroniczna transmisja takich informacji, komponentów systemu informacyjnego lub urządzeń do osób fizycznych lub systemów informacyjnych wymaga zastosowania zdefiniowanych organizacyjnie kanałów pozapasmowych;*

SC-37	**KANAŁY POZAPASMOWE**	
	SC-37[3]	*definiuje osoby lub systemy informacyjne, do których fizyczne dostarczenie lub elektroniczna transmisja takich informacji, komponentów systemu informacyjnego lub urządzeń wymaga organizacyjnie zdefiniowanego kanału pozapasmowego; oraz*
	SC-37[4]	*wykorzystuje zdefiniowane organizacyjnie kanały pozapasmowe do fizycznego dostarczania lub elektronicznej transmisji zdefiniowanych organizacyjnie informacji, komponentów systemów informacyjnych lub urządzeń do określonych osób lub systemów informacyjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczą przypadków użycia kanałów pozapasmowych; zasady i procedury kontroli dostępu; polityka i procedury identyfikacji i uwierzytelniania; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; wykaz kanałów pozapasmowych; rodzaje informacji, komponentów systemu informacyjnego lub urządzeń wymagających użycia kanałów pozapasmowych do fizycznego dostarczania lub elektronicznej transmisji do uprawnionych osób lub systemów informacyjnych; fizyczne zapisy dostaw; elektroniczne zapisy transmisji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji autoryzujący, instalujący, konfigurujący, obsługujący i/lub wykorzystujący kanały pozapasmowe; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z wykorzystaniem kanałów pozapasmowych; zautomatyzowane mechanizmy wspierające i/lub wdrażające wykorzystanie kanałów pozapasmowych].	

SC-37(1)	**KANAŁY POZAPASMOWE | *GWARANTOWANA DOSTAWA / TRANSMISJA***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-37(1)[1]	*określa środki bezpieczeństwa, które należy stosować w celu zapewnienia, że tylko wyznaczone osoby lub systemy informacyjne uzyskują określone informacje, składniki systemów informacyjnych lub urządzenia;*

SC-37(1)	**KANAŁY POZAPASMOWE | *GWARANTOWANA DOSTAWA / TRANSMISJA***	
	SC-37(1)[2]	*definiuje osoby lub systemy informacyjne przeznaczone do otrzymywania określonych informacji, komponentów systemów informacyjnych lub urządzeń;*
	SC-37(1)[3]	*definiuje informacje, komponenty systemów informacyjnych lub urządzenia, do których otrzymywania są przeznaczone wyłącznie osoby lub systemy informacyjne określone przez organizację; oraz*
	SC-37(1)[4]	*stosuje określone przez organizację środki bezpieczeństwa w celu zapewnienia, że tylko określone przez organizację osoby lub systemy informacyjne otrzymują określone przez organizację informacje, komponenty systemów informacyjnych lub urządzenia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące użycia kanałów pozapasmowych; zasady i procedury kontroli dostępu; polityka i procedury identyfikacji i uwierzytelniania; dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; wykaz środków bezpieczeństwa, które należy stosować w celu zapewnienia, że wyznaczone osoby lub systemy informacyjne otrzymają informacje, składniki systemów informacyjnych lub urządzenia określone przez organizację; wykaz środków bezpieczeństwa w celu dostarczenia wyznaczonym osobom lub systemom informacyjnym ustalonych informacji, komponentów systemów informacyjnych lub urządzeń; wykaz informacji, komponentów systemów informacyjnych lub urządzeń, które należy dostarczyć wyznaczonym osobom lub systemom informacyjnym; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji autoryzujący, instalujący, konfigurujący, obsługujący i/lub wykorzystujący kanały pozapasmowe; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z użytkowaniem kanałów pozapasmowych; zautomatyzowane mechanizmy wspomagające i/lub implementujące użytkowanie kanałów pozapasmowych; zautomatyzowane mechanizmy wspomagające i/lub implementujące zabezpieczenia zapewniające dostarczenie wskazanych informacji, komponentów systemu lub urządzeń].	

SC-38	**BEZPIECZEŃSTWO OPERACJI**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-38[1]	*określa środki bezpieczeństwa operacji, które należy stosować w celu ochrony kluczowych informacji organizacyjnych w całym cyklu życia systemu; oraz*
	SC-38[2]	*stosuje określone przez organizację zabezpieczenia operacji w celu ochrony kluczowych informacji organizacyjnych w całym cyklu życia systemu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące bezpieczeństwa operacji; plan bezpieczeństwa; wykaz operacyjnych środków bezpieczeństwa; oceny środków bezpieczeństwa; szacowanie ryzyka; oceny zagrożenia i podatności na zagrożenia; plany i etapy działania; dokumentacja cyklu życia systemu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Procesy organizacyjne mające na celu ochronę informacji organizacyjnych w całym cyklu życia systemu (SDLC); zautomatyzowane mechanizmy wspierające i/lub wdrażające zabezpieczenia w celu ochrony informacji organizacyjnych w całym cyklu życia systemu (SDLC)].	

SC-39	**IZOLACJA PROCESÓW**
	CEL OCENY: *Ustalić, czy system informacyjny utrzymuje osobną domenę wykonawczą dla każdego wykonywanego procesu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Dokumentacja projektowa systemu informacyjnego; architektura systemu informacyjnego; dokumentacja niezależnej weryfikacji i oceny; dokumentacja badań i oceny, inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Deweloperzy systemów informacyjnych/integratorzy; architekt bezpieczeństwa systemu informacyjnego].

SC-39	**IZOLACJA PROCESÓW**
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące osobne domeny wykonania dla każdego procesu wykonawczego].

SC-39(1)	**IZOLACJA PROCESÓW | *SEPARACJA SPRZĘTOWA***
	CEL OCENY: *Ustalenie, czy system informacyjny wdraża podstawowe mechanizmy separacji sprzętowej w celu ułatwienia separacji procesów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; dokumentacja systemu informacyjnego dotycząca stosowanych mechanizmów separacji podzespołów; dokumentacja systemu informacyjnego dostawców, producentów lub deweloperów; niezależna dokumentacja weryfikacyjna i oceniająca; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Zdolność systemu informacyjnego do wdrażania podstawowych sprzętowych mechanizmów rozdzielania procesów].

SC-39(2)	**IZOLACJA PROCESÓW | *IZOLACJA WĄTKÓW***	
	CEL OCENY: *Ustalić, czy system informacyjny:*	
	SC-39(2)[1]	*definiuje przetwarzanie wielowątkowe, w przypadku którego dla każdego wątku w przetwarzaniu wielowątkowym ma być utrzymana oddzielna domena wykonania; oraz*
	SC-39(2)[2]	*utrzymuje osobną domenę wykonawczą dla każdego wątku w zdefiniowanym organizacyjnie wielowątkowym przetwarzaniu.*

SC-39(2)	**IZOLACJA PROCESÓW | *IZOLACJA WĄTKÓW***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; lista domen wykonawczych systemu informacyjnego dla każdego wątku w przetwarzaniu wielowątkowym; dokumentacja systemu informacyjnego dla przetwarzania wielowątkowego; dokumentacja systemu informacyjnego dostawców, producentów lub deweloperów; dokumentacja niezależnej weryfikacji i oceny; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; deweloperzy systemów informacyjnych/integratorzy]. **Test**: [*wybierz spośród:* Możliwości systemu informacyjnego implementującego wydzieloną domenę wykonawczą dla każdego wątku w przetwarzaniu wielowątkowym].

SC-40	**OCHRONA ŁĄCZA BEZPRZEWODOWEGO**	
	CEL OCENY: *Określić, czy:*	
	SC-40[1]	*organizacja określa:*
	SC-40[1][a]	*wewnętrzne łącza bezprzewodowe, które mają być chronione przed atakami określonych parametrów sygnału;*
	SC-40[1][b]	*zewnętrzne łącza bezprzewodowe, które mają być chronione przed atakami określonych parametrów sygnału;*
	SC-40[2]	*organizacja określa typy parametrów atakowanych sygnałów lub odniesienia do źródeł takich ataków, które opierają się na wykorzystaniu parametrów sygnału zdefiniowanych przez organizację wewnętrznych i zewnętrznych łączy bezprzewodowych; oraz*
	SC-40[3]	*system informacyjny chroni zdefiniowane przez organizację wewnętrzne i zewnętrzne łącza bezprzewodowe przed ustalonymi przez organizację rodzajami ataków na parametry sygnału lub odniesieniami do źródeł takich ataków.*

SC-40	**OCHRONA ŁĄCZA BEZPRZEWODOWEGO**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; zasady i procedury kontroli dostępu; procedury dotyczące ochrony łącza bezprzewodowego; dokumentacja projektowa systemu informacyjnego; schematy sieci bezprzewodowych; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; architektura systemu informacyjnego; wykaz wewnętrznych i zewnętrznych łączy bezprzewodowych; wykaz ataków na parametry sygnału lub odniesienia do źródeł ataków; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji autoryzujący, instalujący, konfigurujący i/lub utrzymujący wewnętrzne i zewnętrzne łącza bezprzewodowe]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające ochronę połączeń bezprzewodowych].

SC-40(1)	**OCHRONA ŁĄCZA BEZPRZEWODOWEGO | *INTERFERENCJA ELEKTROMAGNETYCZNA***	
	CEL OCENY: *Określić, czy:*	
	SC-40(1)[1]	*organizacja określa poziom ochrony przed skutkami celowych zakłóceń elektromagnetycznych; oraz*
	SC-40(1)[2]	*system informacyjny wykorzystuje mechanizmy kryptograficzne, które zapewniają określony organizacyjnie poziom ochrony przed skutkami celowych zakłóceń elektromagnetycznych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; zasady i procedury kontroli dostępu; procedury dotyczące ochrony łącza bezprzewodowego; dokumentacja projektowa systemu informacyjnego; schematy sieci bezprzewodowych; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; architektura systemu informacyjnego; sprzęt i oprogramowanie telekomunikacyjne systemu informacyjnego; wyniki kategoryzacji bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

SC-40(1)	**OCHRONA ŁĄCZA BEZPRZEWODOWEGO | *INTERFERENCJA ELEKTROMAGNETYCZNA***
	Wywiad: [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji autoryzujący, instalujący, konfigurujący i/lub utrzymujący wewnętrzne i zewnętrzne łącza bezprzewodowe]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficzne wprowadzające zabezpieczenia przed skutkami zamierzonych zakłóceń elektromagnetycznych].

SC-40(2)	**OCHRONA ŁĄCZA BEZPRZEWODOWEGO | *REDUKCJA POTENCJALNEJ DETEKCJI***	
	CEL OCENY: *Określić, czy:*	
	SC-40(2)[1]	*organizacja określa poziom redukcji, jaki należy osiągnąć, aby zmniejszyć potencjał wykrywania połączeń bezprzewodowych; oraz*
	SC-40(2)[2]	*system informacyjny wdraża mechanizmy kryptograficzne w celu zmniejszenia potencjału wykrywalności połączeń bezprzewodowych do określonego organizacyjnie poziomu redukcji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; zasady i procedury kontroli dostępu; procedury dotyczące ochrony łącza bezprzewodowego; dokumentacja projektowa systemu informacyjnego; schematy sieci bezprzewodowych; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; architektura systemu informacyjnego; sprzęt i oprogramowanie telekomunikacyjne systemu informacyjnego; wyniki kategoryzacji bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji autoryzujący, instalujący, konfigurujący i/lub utrzymujący wewnętrzne i zewnętrzne łącza bezprzewodowe]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficzne wprowadzające ochronę w celu zmniejszenia wykrywalności połączeń bezprzewodowych].	

SC-40(3)	**OCHRONA ŁĄCZA BEZPRZEWODOWEGO | *NAŚLADOWCZE LUB MANIPULACYJNE OSZUSTWO TELEKOMUNIKACYJNE***	
	CEL OCENY: *Ustalić, czy system informacyjny wdraża mechanizmy kryptograficzne w celu:*	
	SC-40(3)[1]	*identyfikowania transmisji bezprzewodowych, które są celowymi próbami uwierzytelnienia oszustwa opartego na naśladownictwie lub manipulacji parametrami sygnału; oraz*
	SC-40(3)[2]	*odrzucania transmisji bezprzewodowych, które są celowymi próbami uwierzytelnienia oszustwa opartego na naśladownictwie lub manipulacji parametrami sygnału.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; zasady i procedury kontroli dostępu; procedury dotyczące dokumentacji projektowej systemu informacyjnego; schematy sieci bezprzewodowych; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; architektura systemu informacyjnego; sprzęt i oprogramowanie telekomunikacyjne systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji autoryzujący, instalujący, konfigurujący i/lub utrzymujący wewnętrzne i zewnętrzne łącza bezprzewodowe]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficzne zapewniające ochronę łączy bezprzewodowych przed próbami związanymi z naśladowczymi lub manipulacyjnymi oszustwami telekomunikacyjnymi].	

SC-40(4)	**OCHRONA ŁĄCZA BEZPRZEWODOWEGO | *IDENTYFIKACJA PARAMETRÓW SYGNAŁU***	
	CEL OCENY: *Określić, czy:*	
	SC-40(4)[1]	*organizacja określa nadajnik i bezprzewodowe, w przypadku których należy wdrożyć mechanizmy kryptograficzne uniemożliwiające ich identyfikację przy wykorzystaniu parametrów sygnału nadajnika; oraz*

SC-40(4)	**OCHRONA ŁĄCZA BEZPRZEWODOWEGO | *IDENTYFIKACJA PARAMETRÓW SYGNAŁU***	
	SC-40(4)[2]	*system informacyjny wdraża mechanizmy kryptograficzne uniemożliwiające identyfikację zdefiniowanych organizacyjnie nadajników bezprzewodowych z wykorzystaniem parametrów sygnału nadajnika.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; zasady i procedury kontroli dostępu; procedury dotyczące dokumentacji projektowej systemu informacyjnego; schematy sieci bezprzewodowych; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; architektura systemu informacyjnego; sprzęt i oprogramowanie telekomunikacyjne systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji autoryzujący, instalujący, konfigurujący i/lub utrzymujący wewnętrzne i zewnętrzne łącza bezprzewodowe]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficzne zapobiegające identyfikacji nadajników bezprzewodowych].	

SC-41	**DOSTĘP DO PORTÓW I URZĄDZEŃ WEJŚCIA / WYJŚCIA**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-41[1]	*definiuje połączenia portów lub urządzeń wejściowych/wyjściowych, które mają być fizycznie wyłączone lub usunięte w systemach informacyjnych lub komponentach systemów informacyjnych;*
	SC-41[2]	*definiuje systemy informacyjne lub komponenty systemów informacyjnych ze zdefiniowanymi przez organizację połączonymi portami lub urządzeniami wejściowymi / wyjściowymi, które mają być fizycznie wyłączone lub usunięte; oraz*
	SC-41[3]	*fizycznie wyłącza lub usuwa określone przez organizację porty połączeniowe lub urządzenia wejścia/wyjścia w określonych przez organizację systemach informacyjnych lub komponentach systemu informacyjnego.*

SC-41	**DOSTĘP DO PORTÓW I URZĄDZEŃ WEJŚCIA / WYJŚCIA**		
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; zasady i procedury kontroli dostępu; procedury dotyczące dostępu do portów oraz urządzeń wejściowych/wyjściowych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; wykaz połączonych portów lub urządzeń wejścia/wyjścia systemu informacyjnego lub komponentów systemu informacyjnego, które mają być fizycznie wyłączone lub usunięte w systemach informacyjnych lub komponentach systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy obsługujące lub implementujące wyłączenie portów połączeniowych lub urządzeń wejściowych/wyjściowych].		

SC-42	**CZUJNIKI**	
	CEL OCENY: *Określić, czy:*	
SC-42(a)	**SC-42(a)[1]**	*organizacja określa wyjątki, w których dopuszcza się zdalną aktywację czujników;*
	SC-42(a)[2]	*system informacyjny zakazuje zdalnej aktywacji czujników, z wyjątkiem zdefiniowanych przez organizację wyjątków, w przypadku których zdalna aktywacja czujników jest dozwolona;*
SC-42(b)	**SC-42(b)[1]**	*organizacja określa kategorię użytkowników, którym ma być zapewnione jednoznaczne wskazanie sposobu wykorzystania czujników; oraz*
	SC-42(b)[2]	*system informacyjny zapewnia jednoznaczne wskazanie wykorzystania czujnika do określonej przez organizację kategorii użytkowników.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury uwzględniające możliwości czujników i zbierania danych; zasady i procedury	

SC-42	**CZUJNIKI**
	kontroli dostępu; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za obsługę czujników]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wprowadzające kontrolę dostępu w celu zdalnej aktywacji funkcji czujników systemu informacyjnego; zautomatyzowane mechanizmy wprowadzające funkcję sygnalizowania użycia czujników].

SC-42(1)	**CZUJNIKI | *RAPORTOWANIE DO UPOWAŻNIONYCH OSÓB LUB RÓL***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-42(1)[1]	*określa czujniki, które mają być wykorzystywane do gromadzenia danych lub informacji zgłaszanych tylko upoważnionym osobom lub rolom; oraz*
	SC-42(1)[2]	*zapewnia, że system informacyjny jest skonfigurowany w taki sposób, że dane lub informacje zbierane przez czujniki zdefiniowane przez organizację są zgłaszane tylko upoważnionym osobom lub rolom.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; zasady i procedury kontroli dostępu; procedury uwzględniające możliwości czujników i zbierania danych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za definiowanie czujników]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy ograniczające przekazywanie informacji z czujników tylko do osób upoważnionych; zbieranie danych z czujników oraz możliwość przekazywania raportów do systemu informacyjnego].	

SC-42(2)	**CZUJNIKI |** ***AUTORYZOWANE UŻYCIE***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-42(2)[1]	*definiuje środki, które należy zastosować, aby dane lub informacje gromadzone przez czujniki były wykorzystywane wyłącznie w dozwolonych celach;*
	SC-42(2)[2]	*definiuje czujniki, które mają być wykorzystywane do gromadzenia danych lub informacji wyłącznie w dozwolonych celach; oraz*
	SC-42(2)[3]	*stosuje środki określone przez organizację, tak, aby dane lub informacje zbierane przez czujniki określone przez organizację były wykorzystywane wyłącznie do uprawnionych celów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; zasady i procedury kontroli dostępu; możliwości czujników i gromadzenie danych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; architektura systemu informacyjnego; wykaz środków, które należy zastosować w celu zapewnienia, że dane lub informacje gromadzone przez czujniki są wykorzystywane wyłącznie w dozwolonych celach; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za definiowanie czujników]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub środki wykonawcze zapewniające wykorzystanie informacji z czujników tylko do dozwolonych celów; zbieranie danych z czujników oraz możliwość przekazywania raportów do systemu informacyjnego].	

SC-42(3)	**CZUJNIKI |** ***ZABRONIONE WYKORZYSTANIE URZĄDZEŃ***	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-42(3)[1]	*definiuje właściwości czujników środowiskowych, których stosowanie w obiektach, obszarach lub systemach jest zabronione;*

SC-42(3)	**CZUJNIKI |** ***ZABRONIONE WYKORZYSTANIE URZĄDZEŃ***	
	SC-42(3)[2]	*definiuje obiekty, obszary lub systemy, w których ma być zakazane stosowanie urządzeń posiadających Zdolności detekcji otoczenia; oraz*
	SC-42(3)[3]	*zakazuje stosowania w obiektach, obszarach lub systemach zdefiniowanych organizacyjnie urządzeń posiadających zdolność detekcji otoczenia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; zasady i procedury kontroli dostępu; procedury uwzględniające możliwości czujników i zbierania danych; dokumentacja projektowa systemu informacyjnego; schematy sieci bezprzewodowych; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; architektura systemu informacyjnego; obiekty, obszary lub systemy, w których zabronione jest stosowanie urządzeń posiadających zdolność wykrywania zagrożeń dla środowiska; wykaz urządzeń posiadających zdolność wykrywania zagrożeń dla środowiska w obiektach, obszarach lub systemach, w których zabronione jest stosowanie urządzeń wyposażonych w czujniki środowiskowe; wykaz urządzeń wyposażonych w czujniki środowiskowe; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za definiowanie czujników].	

SC-43	**OGRANICZENIA UŻYCIA**			
	CEL OCENY: *Określić, czy organizacja:*			
	SC-43(a)	**SC-43(a)[1]**	*definiuje komponenty systemu informacyjnego, dla których mają zostać ustanowione ograniczenia użycia oraz wytyczne dotyczące wdrażania;*	
		SC-43(a)[2]	*ustanawia, dla zdefiniowanych przez organizację komponentów systemu informacyjnego:*	
			SC-43(a)[2][a]	*ograniczenie użycia w oparciu o możliwość spowodowania uszkodzenia systemu informacyjnego w przypadku użycia w sposób złośliwy;*

SC-43	**OGRANICZENIA UŻYCIA**			
			SC-43(a)[2][b]	*wytyczne dotyczące wdrażania oparte na możliwości spowodowania uszkodzenia systemu informacyjnego w przypadku jego złośliwego użycia;*
	SC-43(b)	**SC-43(b)[1]**	*upoważnia do korzystania z takich komponentów w ramach systemu informacyjnego;*	
		SC-43(b)[2]	*monitoruje wykorzystanie takich komponentów w ramach systemu informacyjnego; oraz*	
		SC-43(b)[3]	*kontroluje wykorzystanie takich komponentów w systemie informacyjnym.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące ograniczania użycia; ograniczenie użycia; polityka i procedury wdrażania; zapisy dotyczące zezwoleń; zapisy dotyczące monitorowania systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z autoryzacją, monitorowaniem i kontrolą wykorzystania komponentów z ograniczonym użyciem; zautomatyzowane mechanizmy wspierające i/lub wdrażające autoryzację, monitorowanie i kontrolę wykorzystania komponentów z ograniczonym użyciem].			

SC-44	**KOMORY DETONACYJNE**	
	CEL OCENY: *Określić, czy organizacja:*	
	SC-44[1]	*określa system informacyjny, komponent systemu lub miejsce, w którym ma być zastosowana funkcja komory detonacyjnej; oraz*
	SC-44[2]	*wykorzystuje funkcje komory detonacyjnej w ramach zdefiniowanego przez organizację systemu informacyjnego, komponentu systemu lub lokalizacji.*

SC-44	**KOMORY DETONACYJNE**
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka ochrony systemu i komunikacji; procedury dotyczące komory detonacyjnej; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcje komory detonacyjnej].

KATEGORIA SI - INTEGRALNOŚĆ SYSTEMU I INFORMACJI

SI-1	**POLITYKA I PROCEDURY INTEGRALNOŚCI SYSTEMU I INFORMACJI**			
	CEL OCENY: *Określić, czy organizacja:*			
	SI-1(a)(1)	**SI-1(a)(1)[1]**	*opracowuje i dokumentuje politykę integralności systemu i informacji, która dotyczy:*	
			SI-1(a)(1)[1][a]	*celu;*
			SI-1(a)(1)[1][b]	*zakresu stosowania;*
			SI-1(a)(1)[1][c]	*ról;*
			SI-1(a)(1)[1][d]	*odpowiedzialności;*
			SI-1(a)(1)[1][e]	*zaangażowania kierownictwa;*
			SI-1(a)(1)[1][f]	*koordynacji pomiędzy jednostkami organizacyjnymi;*
			SI-1(a)(1)[1][g]	*przestrzegania zgodności z przepisami;*
		SI-1(a)(1)[2]	*określa personel lub role, wśród których ma być rozpowszechniana polityka integralności systemu i informacji;*	
		SI-1(a)(1)[3]	*rozpowszechnia system oraz politykę integralności informacji wśród personelu lub ról zdefiniowanych przez organizację;*	
	SI-1(a)(2)	**SI-1(a)(2)[1]**	*opracowuje i dokumentuje procedury ułatwiające wprowadzenie w życie systemu oraz polityki integralności informacji, a także związanych z nimi zabezpieczeń integralności informacji;*	
		SI-1(a)(2)[2]	*określa personel lub role, wśród których procedury mają być rozpowszechniane;*	
		SI-1(a)(2)[3]	*rozpowszechnia procedury wśród określonego przez organizację personelu lub ról;*	
	SI-1(b)(1)	**SI-1(b)(1)[1]**	*określa częstotliwość przeglądów i aktualizacji bieżącego systemu i polityki integralności informacji;*	

SI-1	**POLITYKA I PROCEDURY INTEGRALNOŚCI SYSTEMU I INFORMACJI**		
		SI-1(b)(1)[2]	*opiniuje i aktualizuje obowiązujący system oraz politykę integralności informacji z częstotliwością określoną przez organizację;*
	SI-1(b)(2)	**SI-1(b)(2)[1]**	*definiuje częstotliwość przeglądów aktualizujących istniejący system oraz procedury integralności informacji; oraz*
		SI-1(b)(2)[2]	*opiniuje i aktualizuje istniejący system i procedury integralności informacji z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka i procedury integralności systemu i informacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za integralność systemu i informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji].		

SI-2	**USUWANIE USTEREK**		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-2(a)	**SI-2(a)[1]**	*identyfikuje niedoskonałości systemu informacyjnego;*
		SI-2(a)[2]	*zgłasza niedoskonałości systemu informacyjnego;*
		SI-2(a)[3]	*koryguje niedoskonałości systemu informacyjnego;*
	SI-2(b)	**SI-2(b)[1]**	*testuje aktualizacje oprogramowania związane z usuwaniem błędów pod kątem ich skuteczności oraz potencjalnych skutków ubocznych przed instalacją;*
		SI-2(b)[2]	*testuje aktualizacje oprogramowania związane z usuwaniem błędów systemowych pod kątem ich skuteczności oraz potencjalnych skutków ubocznych przed instalacją;*
	SI-2(c)	**SI-2(c)[1]**	*określa okres czasu, w którym należy zainstalować aktualizacje oprogramowania związane z bezpieczeństwem po wydaniu aktualizacji;*

SI-2	**USUWANIE USTEREK**		
		SI-2(c)[2]	*definiuje okres czasu, w którym należy zainstalować aktualizacje oprogramowania układowego mające znaczenie dla bezpieczeństwa po wydaniu aktualizacji;*
		SI-2(c)[3]	*instaluje aktualizacje oprogramowania w określonym przez organizację okresie czasu, w którym aktualizacje są wydawane;*
		SI-2(c)[4]	*instaluje aktualizacje oprogramowania układowego w zdefiniowanym przez organizację okresie czasu, w którym wydawane są aktualizacje; oraz*
	SI-2(d)	*włącza usuwanie wad oprogramowania do procesu zarządzania konfiguracją organizacyjną.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące usuwania usterek; procedury dotyczące zarządzania konfiguracją; wykaz niedoskonałości słabych punktów mogących mieć wpływ na system informacyjny; lista wykonanych działań naprawczych dotyczących niedoskonałości systemu informacyjnego (np. lista zainstalowanych poprawek, dodatki Service Pack, hot fixy i inne aktualizacje oprogramowania korygujące niedoskonałości systemu informacyjnego); wyniki testów instalacji oprogramowania i aktualizacji oprogramowania układowego umożliwiających skorygowanie niedoskonałości systemu informacyjnego; zapisy dotyczące kontroli instalacji/zmian oprogramowania i aktualizacji oprogramowania układowego istotnych dla bezpieczeństwa; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za usuwanie usterek; personel organizacji odpowiedzialny za zarządzanie konfiguracją]. **Test**: [*wybierz spośród:* Organizacyjne procesy identyfikacji, raportowania i usuwania usterek systemu informacyjnego; organizacyjny proces instalacji oprogramowania i aktualizacji oprogramowania układowego; zautomatyzowane mechanizmy wspomagające i/lub wdrażające raportowanie oraz korygujące usterki systemu informacyjnego; zautomatyzowane mechanizmy wspomagające i/lub wdrażające testowanie oprogramowania i aktualizacji oprogramowania układowego].		

SI-2(1)	**USUWANIE USTEREK | *ZARZĄDZANIE CENTRALNE***
	CEL OCENY: *Ustalić, czy organizacja centralnie zarządza procesem usuwania usterek.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące usuwania usterek; personel organizacji odpowiedzialny za usuwanie usterek; personel organizacji odpowiedzialny za zautomatyzowane mechanizmy wspomagające scentralizowane zarządzanie usuwaniem usterek; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za usuwanie usterek]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z zarządzaniem centralnym procesem usuwania usterek; zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie centralnym procesem usuwania usterek].

SI-2(2)	**USUWANIE USTEREK | *ZAUTOMATYZOWANE USUWANIA USTEREK***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-2(2)[1]	*określa częstotliwość stosowania zautomatyzowanych mechanizmów określania stanu komponentów systemu informacyjnego w zakresie usuwania usterek; oraz*
	SI-2(2)[2]	*wykorzystuje zautomatyzowane mechanizmy z określoną przez organizację częstotliwością do określenia statusu komponentów systemu informacyjnego w zakresie usuwania usterek.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące usuwania usterek; personel organizacji odpowiedzialny za usuwanie usterek; personel organizacji odpowiedzialny za zautomatyzowane mechanizmy wspomagające scentralizowane zarządzanie usuwaniem usterek; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

SI-2(2)	**USUWANIE USTEREK | *ZAUTOMATYZOWANE USUWANIA USTEREK***
	Wywiad: [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za usuwanie usterek]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy stosowane do określania stanu komponentów systemu informacyjnego w zakresie usuwania usterek].

SI-2(3)	**USUWANIE USTEREK | *CZAS DO USUNIĘCIA USTERKI / STANDARDY DZIAŁAŃ NAPRAWCZYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-2(3)(a)	*mierzy czas pomiędzy identyfikacją i usunięciem usterek;*
	SI-2(3)(b)	**SI-2(3)(b)[1]** *określa wartości referencyjne służące do podejmowania działań naprawczych; oraz*
		SI-2(3)(b)[2] *ustanawia określone organizacyjnie standardy podejmowania działań naprawczych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące usuwania usterek; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz standardów wyznaczających punkty odniesienia do podejmowania działań naprawczych w odniesieniu do zidentyfikowanych usterek; rejestry zapewniające znaczniki czasu identyfikacji usterek oraz wynikające z nich czynności w zakresie usuwania usterek; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za usuwanie usterek]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące do identyfikacji, raportowania i korygowania usterek systemu informacyjnego; zautomatyzowane mechanizmy służące do pomiaru czasu między identyfikacją i usunięciem usterki].	

SI-2(4)	**USUWANIE USTEREK | *AUTOMATYCZNE ŚCIEŻKI ZARZĄDZANIA NARZĘDZIAMI***
[Włączone do: SI-2].	

SI-2(5)	**USUWANIE USTEREK | *AUTOMATYCZNE AKTUALIZACJE APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO***		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-2(5)[1]	**SI-2(5)[1][a]**	*definiuje komponenty systemu informacyjnego wymagające automatycznej instalacji aktualizacji programów istotnych z punktu widzenia bezpieczeństwa;*
		SI-2(5)[1][b]	*definiuje komponenty systemu informacyjnego wymagające automatycznej instalacji aktualizacji oprogramowania układowego istotnych z punktu widzenia bezpieczeństwa;*
	SI-2(5)[2]	**SI-2(5)[2][a]**	*definiuje aktualizacje oprogramowania związane z bezpieczeństwem, które mają być automatycznie instalowane w komponentach systemu informacyjnego zdefiniowanych przez organizację;*
		SI-2(5)[2][b]	*definiuje aktualizacje oprogramowania układowego mające znaczenie dla bezpieczeństwa, które mają być automatycznie instalowane w komponentach systemu informacyjnego zdefiniowanego przez organizację;*
	SI-2(5)[3]	**SI-2(5)[3][a]**	*automatycznie instaluje aktualizacje oprogramowania o istotnym znaczeniu dla bezpieczeństwa, które mają być automatycznie instalowane w zdefiniowanych przez organizację komponentach systemu informacyjnego; oraz*
		SI-2(5)[3][b]	*automatycznie instaluje zdefiniowane przez organizację aktualizacje oprogramowania układowego związane z bezpieczeństwem w komponentach systemu informacyjnego określonych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące usuwania usterek; zautomatyzowane mechanizmy wspomagające usuwanie usterek i automatyczne aktualizacje aplikacji i oprogramowania układowego; dokumentacja projektowa systemu informacyjnego; ustawienia		

SI-2(5)	**USUWANIE USTEREK | *AUTOMATYCZNE AKTUALIZACJE APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO***
	konfiguracyjne systemu informacyjnego i związana z nimi dokumentacja; rejestry ostatnich aktualizacji aplikacji i oprogramowania układowego istotnych z punktu widzenia bezpieczeństwa, zainstalowanych automatycznie do komponentów systemu informacyjnego; rejestry audytów system informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za usuwanie usterek]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy implementujące automatyczne aktualizacje oprogramowania/oprogramowania układowego].

SI-2(6)	**USUWANIE USTEREK | *USUWANIE POPRZEDNICH WERSJI APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO***		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-2(6)[1]	**SI-2(6)[1][a]**	*definiuje komponenty oprogramowania, które mają być usunięte po zainstalowaniu zaktualizowanych wersji;*
		SI-2(6)[1][b]	*definiuje składniki oprogramowania układowego, które mają być usunięte po zainstalowaniu zaktualizowanych wersji;*
	SI-2(6)[2]	**SI-2(6)[2][a]**	*usuwa organizacyjne składniki oprogramowania, które zostaną skasowane po zainstalowaniu zaktualizowanych wersji; oraz*
		SI-2(6)[2][b]	*usuwa składniki oprogramowania układowego zdefiniowane organizacyjnie po zainstalowaniu zaktualizowanych wersji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące usuwania usterek; zautomatyzowane mechanizmy wspierające usuwanie usterek; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry usuwania elementów aplikacji i oprogramowania układowego po zainstalowaniu zaktualizowanych wersji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].		

SI-2(6)	**USUWANIE USTEREK | *USUWANIE POPRZEDNICH WERSJI APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO***
	Wywiad: [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za usuwanie usterek]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające usuwanie wcześniejszych wersji oprogramowania/poprogramowania układowego].

SI-3	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM**				
	CEL OCENY: *Określić, czy organizacja:*				
	SI-3(a)	*wykorzystuje mechanizmy ochrony przed złośliwym kodem w celu wykrycia i wyeliminowania złośliwego kodu w systemie informacyjnym:*			
		SI-3(a)[1]	*w punktach wejścia;*		
		SI-3(a)[2]	*w punktach wyjścia;*		
	SI-3(b)	*aktualizuje mechanizmy ochrony przed złośliwym kodem, gdy tylko dostępne są nowe wydania zgodnie z polityką organizacyjną i procedurą zarządzania konfiguracją (określoną w zabezpieczeniu CM-1);*			
	SI-3(c)	**SI-3(c)[1]**	*definiuje częstotliwość wykonywania przez mechanizmy ochrony przed złośliwym kodem, okresowych skanowań systemu informacyjnego;*		
		SI-3(c)[2]	*określa działania, które mają być inicjowane przez mechanizmy ochrony przed złośliwym kodem w odpowiedzi na wykrycie złośliwego kodu;*		
		SI-3(c)[3]	**SI-3(c)[3](1)**	*konfiguruje mechanizmy ochrony przed złośliwym kodem w celu wykonywania:*	
				SI-3(c)[3](1)[a]	*okresowych skanowań systemu informacyjnego z częstotliwością określoną przez organizację;*

<table>
<tr><td colspan="6">SI-3 ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM</td></tr>
<tr><td rowspan="10"></td><td rowspan="9"></td><td rowspan="9"></td><td rowspan="2"></td><td>SI-3(c)[3](1)[b]</td><td>w czasie rzeczywistym skanowania plików ze źródeł zewnętrznych w punktach końcowych i/lub punktach wejścia/wyjścia z sieci w trakcie ich pobierania, otwierania lub wykonywania, zgodnie z organizacyjną polityką bezpieczeństwa;</td></tr>
<tr><td>SI-3(c)[3](2)</td><td colspan="2">konfiguruje zabezpieczenia przed złośliwym kodem celem implementacji jednego lub kilku z poniższych mechanizmów:</td></tr>
<tr><td></td><td>SI-3(c)[3](2)[a]</td><td>blokowania złośliwego kodu w odpowiedzi na wykrycie złośliwego kodu;</td></tr>
<tr><td></td><td>SI-3(c)[3](2)[b]</td><td>poddania złośliwego kodu kwarantannie w odpowiedzi na wykrycie złośliwego kodu;</td></tr>
<tr><td></td><td>SI-3(c)[3](2)[c]</td><td>wysłania powiadomienia do administratora w odpowiedzi na wykrycie złośliwego kodu; i/lub</td></tr>
<tr><td></td><td>SI-3(c)[3](2)[d]</td><td>inicjowania działań zdefiniowanych przez organizację w odpowiedzi na wykrycie złośliwego kodu;</td></tr>
<tr><td>SI-3(d)</td><td>SI-3(d)[1]</td><td colspan="2">rozwiązuje kwestię uzyskiwania fałszywie pozytywnych wyników podczas wykrywania i zwalczania złośliwego kodu; oraz</td></tr>
<tr><td></td><td>SI-3(d)[2]</td><td colspan="2">rozwiązuje wynikający z tego potencjalny wpływ na dostępność systemu informacyjnego.</td></tr>
<tr><td colspan="5">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka integralności systemu i informacji; polityka i procedury zarządzanie konfiguracją; procedury dotyczące zabezpieczania przed złośliwym kodem; mechanizmy ochrony przed złośliwym kodem; ewidencja aktualizacji zabezpieczenia przed złośliwym kodem; dokumentacja projektowa</td></tr>
</table>

SI-3	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM**
	systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wyniki skanowania pochodzące z mechanizmów zabezpieczenia przed złośliwym kodem; zapis działań inicjowanych przez mechanizmy ochrony przed złośliwym kodem w odpowiedzi na wykrycie złośliwego kodu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za zabezpieczenie przed złośliwym kodem; personel organizacji odpowiedzialny za zarządzanie konfiguracją]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z wykorzystaniem, aktualizacją oraz konfiguracją mechanizmów zabezpieczenia przed złośliwym kodem; proces organizacyjny związany z adresowaniem fałszywych alarmów oraz wynikających z nich potencjalnych skutków; zautomatyzowane mechanizmy wspierające i/lub implementujące wykorzystanie, aktualizację oraz konfigurację mechanizmów zabezpieczania przed złośliwym kodem; zautomatyzowane mechanizmy wspierające i/lub implementujące skanowanie złośliwego kodu oraz wynikające z tego działania.].

SI-3(1)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *ZARZĄDZANIE CENTRALNE***
	CEL OCENY: *Ustalić, czy organizacja centralnie zarządza mechanizmami zabezpieczenia przed złośliwym kodem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące zabezpieczania przed złośliwym kodem; zautomatyzowane mechanizmy wspomagające scentralizowane zarządzanie zabezpieczeniami przed złośliwym kodem; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za zabezpieczenia przed złośliwym kodem].

SI-3(1)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *ZARZĄDZANIE CENTRALNE***
	Test: [*wybierz spośród:* Procesy organizacyjne zarządzania centralnego zabezpieczeniami przed złośliwym kodem; zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie centralne zabezpieczeniami przed złośliwym kodem].

SI-3(2)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *AUTOMATYCZNE AKTUALIZACJE***
	CEL OCENY: *Ustalić, czy system informacyjny automatycznie aktualizuje mechanizmy ochrony przed złośliwym kodem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące zabezpieczania przed złośliwym kodem; zautomatyzowane mechanizmy wspomagające scentralizowane zarządzanie zabezpieczeniami przed złośliwym kodem; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za zabezpieczenia przed złośliwym kodem]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wdrażające automatyczne aktualizacje ochrony przed złośliwym kodem].

SI-3(3)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *NIEUPRZYWILEJOWANI UŻYTKOWNICY***
[Włączone do: AC-6(10)].	

SI-3(4)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *AKTUALIZACJE WYŁĄCZNIE PRZEZ UPRAWNIONYCH UŻYTKOWNIKÓW***
	CEL OCENY: *Ustalić, czy system informacyjny aktualizuje mechanizmy zabezpieczenia przed złośliwym kodem tylko na polecenie personelu wyznaczonego przez kierownika jednostki organizacyjnej.*

SI-3(4)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *AKTUALIZACJE WYŁĄCZNIE PRZEZ UPRAWNIONYCH UŻYTKOWNIKÓW***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące zabezpieczania przed złośliwym kodem; dokumentacja projektowa systemu informacyjnego; mechanizmy ochrony przed złośliwym kodem; rejestry aktualizacji zabezpieczeń przed złośliwym kodem; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za zabezpieczenia przed złośliwym kodem]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące funkcjonalność zabezpieczeń przed złośliwym kodem].

SI-3(5)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE***
[Włączone do: MP-7].	

SI-3(6)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *TESTOWANIE / WERYFIKACJA***		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-3(6)(a)	**SI-3(6)(a)[1]**	*określa częstotliwość testowania mechanizmów ochrony przed złośliwym kodem;*
		SI-3(6)(a)[2]	*testuje mechanizmy ochrony przed złośliwym kodem z częstotliwością określoną przez organizację poprzez wprowadzenie do systemu informacyjnego znanego łagodnego, nierozprzestrzeniającego się przypadku testowego;*
	SI-3(6)(b)	**SI-3(6)(b)[1]**	*weryfikuje, czy ma miejsce wykrycie przypadku testowego; oraz*

SI-3(6)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *TESTOWANIE / WERYFIKACJA***		
		SI-3(6)(b)[2]	*weryfikuje, czy ma miejsce, związane z tym, zgłaszanie incydentów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące zabezpieczania przed złośliwym kodem; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; procesy testowe; rejestry potwierdzające wykonywanie procesów testowych na mechanizmach ochrony przed złośliwym kodem; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za zabezpieczenia przed złośliwym kodem]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub wdrażające testowanie oraz weryfikację możliwości ochrony przed złośliwym kodem].		

SI-3(7)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *WYKRYWANIE BEZSYGNATUROWE***
	CEL OCENY: *Ustalić, czy system informacyjny implementuje mechanizmy wykrywania złośliwego kodu w oparciu o bezsygnaturowe systemy wykrywania zaawansowanych ataków.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące zabezpieczania przed złośliwym kodem; dokumentacja projektowa systemu informacyjnego; mechanizmy ochrony przed złośliwym kodem; rejestry aktualizacji zabezpieczeń przed złośliwym kodem; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za zabezpieczenia przed złośliwym kodem].

SI-3(7)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *WYKRYWANIE BEZSYGNATUROWE***
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące metody ochrony przed złośliwym kodem oparte o wykrywanie bezsygnaturowe].

SI-3(8)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *WYKRYWANIE NIEAUTORYZOWANYCH KOMEND***	
	CEL OCENY: *Określić, czy:*	
	SI-3(8)[1]	*organizacja określa nieautoryzowane polecenia systemu operacyjnego, które powinny być wykrywane przez system informacyjny;*
	SI-3(8)[2]	*organizacja określa komponenty sprzętowe systemu informacyjnego, dla których nieautoryzowane polecenia systemu operacyjnego zdefiniowane przez organizację mają być wykrywane przez interfejs programowania aplikacji jądra;*
	SI-3(8)[3]	*system informacyjny wykrywa nieautoryzowane polecenia systemu operacyjnego zdefiniowane przez organizację poprzez interfejs programowania aplikacji jądra na komponentach sprzętowych systemu informacyjnego zdefiniowanych przez organizację oraz wykonuje jedno lub więcej z poniższych działań:*
		SI-3(8)[3][a] *emituje ostrzeżenie;*
		SI-3(8)[3][b] *kontroluje wykonywanie poleceń; i/lub*
		SI-3(8)[3][c] *uniemożliwia wykonanie polecenia.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące zabezpieczania przed złośliwym kodem; dokumentacja projektowa systemu informacyjnego; mechanizmy ochrony przed złośliwym kodem; komunikaty ostrzegawcze wysyłane w przypadku wykrycia nieautoryzowanego wykonywania poleceń systemu operacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

SI-3(8)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *WYKRYWANIE NIEAUTORYZOWANYCH KOMEND***
	Wywiad: [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za zabezpieczenia przed złośliwym kodem]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub implementujące funkcjonalność ochrony przed złośliwym kodem; zautomatyzowane mechanizmy wspomagające i/lub implementujące wykrywanie nieautoryzowanych poleceń systemu operacyjnego poprzez interfejs programowania aplikacji jądra].

SI-3(9)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *ZDALNE POLECENIA AUTENTYFIKACYJNE***	
	CEL OCENY: *Określić, czy:*	
	SI-3(9)[1]	*organizacja określa środki bezpieczeństwa, które mają być wdrożone przez system informacyjny w celu uwierzytelniania zdalnych poleceń zdefiniowanych przez organizację;*
	SI-3(9)[2]	*organizacja określa zdalne polecenia, które mają być uwierzytelniane przez środki bezpieczeństwa zdefiniowane przez organizację; oraz*
	SI-3(9)[3]	*system informacyjny wdraża środki bezpieczeństwa zdefiniowane przez organizację w celu uwierzytelnienia zdalnych poleceń zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące zabezpieczania przed złośliwym kodem; dokumentacja projektowa systemu informacyjnego; mechanizmy ochrony przed złośliwym kodem; komunikaty ostrzegawcze wysyłane w przypadku wykrycia nieautoryzowanego wykonywania poleceń systemu operacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za zabezpieczenia przed złośliwym kodem].	

SI-3(9)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *ZDALNE POLECENIA AUTENTYFIKACYJNE***
	Test: [*wybierz spośród:* Zautomatyzowane mechanizmy wspomagające i/lub implementujące funkcjonalność ochrony przed złośliwym kodem; zautomatyzowane mechanizmy realizujące uwierzytelnianie zdalnych poleceń; zautomatyzowane mechanizmy wspierające i/lub wdrażające środki bezpieczeństwa w odniesieniu do zdalnych poleceń autentyfikacyjnych].

SI-3(10)	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | *ANALIZA KODU ZŁOŚLIWEGO***		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-3(10)(a)	**SI-3(10)(a)[1]**	*definiuje narzędzia i techniki, które mają być stosowane do analizy cech i zachowania złośliwego kodu;*
		SI-3(10)(a)[2]	*używa zdefiniowanych przez organizację narzędzi i technik do analizy cech i zachowania złośliwego kodu; oraz*
	SI-3(10)(b)	*włącza wyniki z analizy kodu złośliwego do procesów reagowania na incydenty i usuwania wad.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące zabezpieczania przed złośliwym kodem; procedury dotyczące reagowania na incydenty; procedury dotyczące usuwania usterek; dokumentacja projektowa systemu informacyjnego; mechanizmy, narzędzia i techniki ochrony przed złośliwym kodem; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; wyniki analiz złośliwego kodu; zapisy zdarzeń usuwania wad wynikających z analiz złośliwego kodu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za zabezpieczenia przed złośliwym kodem; personel organizacji odpowiedzialny za usuwanie usterek; personel organizacji odpowiedzialny za reagowanie/zarządzanie incydentami]. **Test**: [*wybierz spośród:* Proces organizacyjny dotyczący reakcji na incydent; proces organizacyjny dotyczący usuwania usterek; zautomatyzowane mechanizmy wspomagające i/lub implementujące funkcjonalność ochrony przed złośliwym kodem; narzędzia i techniki analizy charakterystyki i zachowania złośliwego kodu].		

SI-4	**MONITOROWANIE SYSTEMU INFORMACYJNEGO**				
	CEL OCENY: *Określić, czy organizacja:*				
	SI-4(a)	**SI-4(a)(1)**	**SI-4(a)(1)[1]**	*określa cele monitorowania w zakresie wykrywania ataków oraz wskaźniki potencjalnych ataków na system informacyjny;*	
			SI-4(a)(1)[2]	*monitoruje system informacyjny w celu wykrycia, zgodnie ze zdefiniowanymi przez organizację celami monitorowania:*	
				SI-4(a)(1)[2][a]	*ataki;*
				SI-4(a)(1)[2][b]	*wskaźniki potencjalnych ataków;*
		SI-4(a)(2)	*monitoruje system informacyjny w celu wykrycia nieautoryzowanych połączeń:*		
			SI-4(a)(2)[1]	*lokalnych;*	
			SI-4(a)(2)[2]	*sieciowych;*	
			SI-4(a)(2)[3]	*zdalnych;*	
	SI-4(b)	**SI-4(b)(1)**	*definiuje techniki oraz metody identyfikacji nieautoryzowanego użycia systemu informacyjnego;*		
		SI-4(b)(2)	*identyfikuje nieautoryzowane użycie systemu informacyjnego za pomocą techniki metod zdefiniowanych przez organizację;*		
	SI-4(c)	*wdraża urządzenia monitorujące:*			
		SI-4(c)[1]	*długofalowo, do zbierania w ramach systemu informacyjnego istotnych informacji określonych przez organizację;*		
		SI-4(c)[2]	*doraźnie, do śledzenia w ramach systemu informacyjnego określonych rodzajów transakcji będących przedmiotem zainteresowania organizacji;*		
	SI-4(d)	*chroni informacje uzyskane z narzędzi do monitorowania włamań przed nieuprawnionym:*			

SI-4	**MONITOROWANIE SYSTEMU INFORMACYJNEGO**			
		SI-4(d)[1]	*dostępem;*	
		SI-4(d)[2]	*modyfikacją;*	
		SI-4(d)[3]	*skasowaniem;*	
	SI-4(e)	*zwiększa poziom monitorowania systemu informacyjnego, gdy tylko istnieją przesłanki wskazujące na zwiększone ryzyko dla działań organizacyjnych oraz majątku, osób, innych organizacji lub społeczeństwa w oparciu o informacje organów ścigania, informacje wywiadowcze lub inne wiarygodne źródła informacji;*		
	SI-4(f)	*uzyskuje opinię prawną dotyczącą działań związanych z monitorowaniem systemu informacyjnego zgodnie z obowiązującym prawem, rozporządzeniami wykonawczymi, dyrektywami, polityką lub standardami;*		
	SI-4(g)	**SI-4(g)[1]**	*określa personel lub role, którym mają być przekazywane informacje pochodzące z monitorowania systemu informacyjnego;*	
		SI-4(g)[2]	*określa informacje pochodzące z monitorowania systemu informacyjnego, które mają być dostarczane personelowi lub rolom zdefiniowanym przez organizację;*	
		SI-4(g)[3]	*określa częstotliwość dostarczania określonych przez organizację informacji pochodzących z monitorowania systemu informacyjnego, wyznaczonemu przez organizację personelowi lub rolom;*	
		SI-4(g)[4]	*dostarcza wyznaczonemu przez organizację personelowi lub rolom, informacje pochodzące z monitorowania w systemie informacyjnym:*	
			SI-4(g)[4][a]	*w razie potrzeby; i/lub*
			SI-4(g)[4][b]	*z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Strategia ciągłości monitorowania; polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; schemat/układ obiektu; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; lokalizacje w systemie informacyjnym, w których rozmieszczone są urządzenia monitorujące; ustawienia konfiguracji			

SI-4	**MONITOROWANIE SYSTEMU INFORMACYJNEGO**
	systemu informacyjnego i związana z tym dokumentacja; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z monitorowaniem systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwości monitorowania systemu informacyjnego].

SI-4(1)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *SYSTEM WYKRYWANIA WŁAMAŃ***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-4(1)[1]	*łączy poszczególne narzędzia do wykrywania włamań w jeden system informacyjny obejmujący kompleksowy system wykrywania włamań; oraz*
	SI-4(1)[2]	*konfiguruje poszczególne narzędzia do wykrywania włamań do systemu informacyjnego obejmującego kompleksowy system wykrywania włamań.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań/ monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające zdolność wykrywania włamań].	

SI-4(2)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNE NARZĘDZIA ANALIZY W CZASIE RZECZYWISTYM***
	CEL OCENY: *Ustalenie, czy organizacja stosuje zautomatyzowane narzędzia do wspomagania analizy zdarzeń w czasie zbliżonym do rzeczywistego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za reagowanie/zarządzanie incydentami]. **Test**: [*wybierz spośród:* Procesy organizacyjne do analizy zdarzeń w czasie zbliżonym do rzeczywistego; procesy organizacyjne do monitorowania systemów informacyjnych; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie systemów informacyjnych; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające analizę zdarzeń].

SI-4(3)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNA INTEGRACJA NARZĘDZI***	
	CEL OCENY: *Ustalenie, czy organizacja, w celu szybkiej reakcji na ataki, poprzez umożliwienie rekonfiguracji narzędzi do wykrywania włamań w celu wsparcia izolacji eliminacji ataków, stosuje zautomatyzowane środki do integracji narzędzi do wykrywania włamań do:*	
	SI-4(3)[1]	*mechanizmów kontroli dostępu; oraz*
	SI-4(3)[2]	*mechanizmów kontroli przepływu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; zasady i procedury kontroli dostępu; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu	

SI-4(3)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNA INTEGRACJA NARZĘDZI***
	informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań/ monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające Zdolności monitorowania systemu wykrywania włamań/systemów informacyjnych; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające Zdolności kontroli dostępu/ przepływu; zautomatyzowane mechanizmy/narzędzia wspierające i/lub wdrażające integrację narzędzi wykrywania włamań z mechanizmami kontroli dostępu/ przepływu].

SI-4(4)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *PRZYJŚCIOWY / WYJŚCIOWY RUCH TELEKOMUNIKACYJNY***		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-4(4)[1]	*definiuje częstotliwość monitorowania:*	
		SI-4(4)[1][a]	*przychodzącego ruchu telekomunikacyjnego pod kątem nietypowych lub nieautoryzowanych działań lub zachowań;*
		SI-4(4)[1][b]	*wychodzącego ruchu telekomunikacyjnego w związku z nietypowymi lub nieuprawnionymi działaniami lub okolicznościami;*
	SI-4(4)[2]	*monitoruje, z częstotliwością określoną przez organizację:*	
		SI-4(4)[2][a]	*przychodzący ruch telekomunikacyjny pod kątem nietypowych lub nieautoryzowanych działań lub zachowań;*
		SI-4(4)[2][b]	*wychodzący ruch telekomunikacyjny w związku z nietypowymi lub nieuprawnionymi działaniami lub okolicznościami.*

SI-4(4)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *PRZYJŚCIOWY / WYJŚCIOWY RUCH TELEKOMUNIKACYJNY***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; protokoły systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań/ monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające Zdolności wykrywania włamań/ monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające monitorowanie przychodzącego/wychodzącego ruchu telekomunikacyjnego].

SI-4(5)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *ALERTY SYSTEMOWE***	
	CEL OCENY: *Określić, czy:*	
	SI-4(5)[1]	*organizacja określa wskaźniki naruszenia dla systemu informacyjnego;*
	SI-4(5)[2]	*organizacja określa personel lub role, które mają być powiadamiane w przypadku wystąpienia oznak naruszenia lub potencjalnego zagrożenia; oraz*
	SI-4(5)[3]	*system informacyjny alarmuje zdefiniowany przez organizację personel lub role w przypadku wystąpienia zdefiniowanych przez organizację wskaźników naruszeń.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja;	

SI-4(5)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *ALERTY SYSTEMOWE***
	ostrzeżenia/ powiadomienia generowane w oparciu o wskaźniki naruszeń; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań/ monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające Zdolności systemu wykrywania włamań/ monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające alerty dotyczące wskaźników naruszeń].

SI-4(6)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *OGRANICZANIE NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW***
[Włączone do: AC-6(10)].	

SI-4(7)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNA ODPOWIEDŹ NA PODEJRZANE ZDARZENIA***	
	CEL OCENY: *Określić, czy:*	
	SI-4(7)[1]	*organizacja określa personel odpowiedzialny za reagowanie na incydenty (identyfikowany na podstawie nazwiska i/lub roli), który ma być powiadamiany o wykryciu podejrzanych zdarzeń;*
	SI-4(7)[2]	*organizacja określa najmniej zakłócające działania podejmowane przez system informacyjny w celu wyeliminowania podejrzanych zdarzeń;*
	SI-4(7)[3]	*system informacyjny powiadamia określony przez organizację personel reagujący na wykryte podejrzane zdarzenia; oraz*
	SI-4(7)[4]	*system informacyjny podejmuje zdefiniowane przez organizację działania o najmniejszym stopniu zakłóceń w celu wyeliminowania podejrzanych zdarzeń.*

SI-4(7)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNA ODPOWIEDŹ NA PODEJRZANE ZDARZENIA***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; alarmy/ powiadomienia generowane na podstawie wykrytych podejrzanych zdarzeń; rejestry działań podjętych w celu wyeliminowania podejrzanych zdarzeń; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z wykrywaniem włamań/monitorowaniem systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcje wykrywania włamań/monitorowanie systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające powiadomienia personelu reagującego na incydenty; zautomatyzowane mechanizmy wspierające i/lub wdrażające działania zmierzające do wyeliminowania podejrzanych zdarzeń].

SI-4(8)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *OCHRONA INFORMACJI MONITORUJĄCYCH***
[Włączone do: SI-4].	

SI-4(9)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *TESTOWANIE NARZĘDZI MONITORUJĄCYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-4(9)[1]	*określa częstotliwość testowania narzędzi do monitorowania włamań; oraz*
	SI-4(9)[2]	*testuje narzędzia do monitorowania włamań z częstotliwością określoną przez organizację.*

SI-4(9)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *TESTOWANIE NARZĘDZI MONITORUJĄCYCH***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące testowania narzędzi i technik monitorowania systemów informacyjnych; dokumentacja potwierdzająca testowanie narzędzi do monitorowania włamań; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań/monitorowanie systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcje wykrywania włamań/monitorowanie systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające testowanie narzędzi monitorowania włamań.].

SI-4(10)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *INSPEKCJA ZASZYFROWANYCH KOMUNIKATÓW***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-4(10)[1]	*identyfikuje ruch szyfrowanej komunikacji, który musi być widoczny dla narzędzi monitorowania systemu informacyjnego;*
	SI-4(10)[2]	*definiuje narzędzia monitorowania systemu informacyjnego, które mają zapewnić dostęp do określonego przez organizację szyfrowanego ruchu komunikacyjnego; oraz*
	SI-4(10)[3]	*wprowadza przepisy, dzięki którym zdefiniowany przez organizację szyfrowany ruch telekomunikacyjny jest widoczny dla zdefiniowanych przez organizację narzędzi monitorowania systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; protokoły systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

SI-4(10)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *INSPEKCJA ZASZYFROWANYCH KOMUNIKATÓW***
	Wywiad: [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań/ monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwości monitorowania systemu wykrywania włamań/ systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające widoczność zaszyfrowanego ruchu telekomunikacyjnego dla narzędzi monitorowania].

SI-4(11)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *ANALIZA ANOMALII RUCHU TELEKOMUNIKACYJNEGO***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-4(11)[1]	*definiuje punkty wewnętrzne w systemie (np. podsieci, podsystemy), w których ma być analizowany ruch telekomunikacyjny;*
	SI-4(11)[2]	*analizuje wychodzący ruch telekomunikacyjny w celu wykrycia anomalii:*
	SI-4(11)[2][a]	*na zewnętrznej granicy systemu informacyjnego; oraz*
	SI-4(11)[2][b]	*wybranych, zdefiniowanych organizacyjnie punktach wewnętrznych w systemie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; schemat sieciowy; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dzienniki lub rejestry monitorowania systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań].	

SI-4(11)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *ANALIZA ANOMALII RUCHU TELEKOMUNIKACYJNEGO***
	Test: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań/ monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające zdolność wykrywania włamań/ monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające analizę ruchu telekomunikacyjnego].

SI-4(12)	**SYSTEMU INFORMACYJNEGO | *AUTOMATYCZNE ALERTY***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-4(12)[1]	*definiuje działania, które uruchamiają ostrzeżenia dla personelu ochrony na podstawie niewłaściwych lub nietypowych działań mających wpływ na bezpieczeństwo; oraz*
	SI-4(12)[2]	*stosuje zautomatyzowane mechanizmy ostrzegania personelu ochrony o określonych przez organizację czynnościach, które wyzwalają alerty na podstawie niewłaściwych lub nietypowych czynności mających wpływ na bezpieczeństwo.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; wykaz nieprawidłowych lub nietypowych działań (mających wpływ na bezpieczeństwo), które powodują uruchomienie alarmów; alarmy/zawiadomienia przekazywane personelowi ochrony; dzienniki lub rejestry monitorowania systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemów/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloperzy systemów; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie monitorowania systemu wykrywania włamań/systemów informacyjnych; zautomatyzowane mechanizmy wspierające i/lub wdrażające Zdolności monitorowania systemu wykrywania włamań/systemów informacyjnych; zautomatyzowane mechanizmy wspierające i/lub wdrażające zautomatyzowane alerty dla personelu ochrony].	

SI-4(13)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *ANALIZA MODELU RUCHU / ZDARZEŃ TELEKOMUNIKACYJNYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-4(13)(a)	*analizuje schematy ruchu telekomunikacyjnego/zdarzeń danego systemu informacyjnego;*
	SI-4(13)(b)	*opracowuje profile reprezentujące typowe wzorce ruchu i / lub zdarzenia;*
	SI-4(13)(c)	*wykorzystuje profile ruchu telekomunikacyjnego/zdarzeń w urządzeniach monitorujących system, celem zmniejszenia liczby fałszywych i rzeczywistych alarmów.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; lista profil i przedstawiających wspólne schematy ruchu i/lub zdarzenia; dokumentacja protokołów systemu informacyjnego; wykaz dopuszczalnych progów dla wyników fałszywie dodatnich i fałszywie ujemnych; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań/ monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwości monitorowania systemu wykrywania włamań/ systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające analizę schematów ruchu/zdarzeń telekomunikacyjnych].	

SI-4(14)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *WYKRYWANIE ATAKÓW BEZPRZEWODOWYCH***	
	CEL OCENY: *Ustalić, czy organizacja stosuje system wykrywania ataków bezprzewodowych do:*	
	SI-4(14)[1]	*identyfikacji nieautoryzowanych urządzeń bezprzewodowych;*
	SI-4(14)[2]	*wykrywania prób ataków na system informacyjny; oraz*
	SI-4(14)[3]	*wykrywania potencjalnych zagrożeń/zakłóceń w systemie informacyjnym.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; protokoły systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań; zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwości wykrywania ataków bezprzewodowych].	

SI-4(15)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *TELEKOMUNIKACJA BEZPRZEWODOWA / PRZEWODOWA***
	CEL OCENY: *Ustalić, czy organizacja stosuje system wykrywania włamań do monitorowania ruchu telekomunikacyjnego generowanego przez urządzenia bezprzewodowe i nawiązywania połączeń z sieci bezprzewodowych do przewodowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji

SI-4(15)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *TELEKOMUNIKACJA BEZPRZEWODOWA / PRZEWODOWA***
	systemu informacyjnego i związana z tym dokumentacja; dokumentacja protokołów systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z monitorowaniem systemów wykrywania włamań/systemów informacyjnych; zautomatyzowane mechanizmy wspierające i/lub wdrażające Zdolności monitorowania systemów wykrywania włamań/systemów informacyjnych; zautomatyzowane mechanizmy wspierające i/lub wdrażające Zdolności wykrywania włamań bezprzewodowych].

SI-4(16)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *KORELOWANIE INFORMACJI MONITORUJĄCYCH***
	CEL OCENY: *Ustalić, czy organizacja koreluje informacje pochodzące z narzędzi monitorujących stosowanych w całym systemie informacyjnym.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dzienniki lub zapisy korelacji zdarzeń; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań/monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające funkcje wykrywania włamań/monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające korelację informacji uzyskiwanych z narzędzi monitorowania].

SI-4(17)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *ZINTEGROWANA ŚWIADOMOŚĆ SYTUACYJNA***	
	CEL OCENY: *Ustalić, czy organizacja, w celu osiągnięcia zintegrowanej, ogólnoorganizacyjnej świadomości sytuacyjnej, koreluje informacje z monitorowania:*	
	SI-4(17)[1]	*aktywności fizycznej;*
	SI-4(17)[2]	*działalności w cyberprzestrzeni; oraz*
	SI-4(17)[3]	*działalności w ramach łańcucha dostaw.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dzienniki korelacji zdarzeń lub zapisy wynikające z działalności fizycznej, w cyberprzestrzeni łańcucha dostaw; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań/monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające Zdolności wykrywania włamań/ monitorowania systemu; zautomatyzowane mechanizmy wspierające i/lub wdrażające korelację informacji uzyskanych z narzędzi monitorowania].	

SI-4(18)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *ANALIZA RUCHU / ZAPOBIEGANIE EKSFILTRACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-4(18)[1]	*definiuje punkty wewnętrzne w systemie (np. podsystemy, podsieci), w których ma być analizowany ruch telekomunikacyjny;*

SI-4(18)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *ANALIZA RUCHU / ZAPOBIEGANIE EKSFILTRACJI***		
	SI-4(18)[2]	*wykrywa ukrytą eksfiltrację informacji, analizując wychodzący ruch telekomunikacyjny na:*	
		SI-4(18)[2][a]	*zewnętrznej granicy systemu informacyjnego (tj. obszaru obwodu systemu); oraz*
		SI-4(18)[2][b]	*organizacyjnie zdefiniowanych punktach wewnętrznych w systemie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; schemat sieciowy; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dzienniki lub rejestry monitorowania systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego; personel organizacji odpowiedzialny za system wykrywania włamań]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie wykrywania włamań/monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspomagające i/lub wdrażające Zdolności wykrywania włamań/ monitorowania systemu; zautomatyzowane mechanizmy wspomagające i/lub wdrażające analizę wychodzącego ruchu telekomunikacyjnego].		

SI-4(19)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *ZWIĘKSZONE RYZYKO GENEROWANE PRZEZ OSOBY***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-4(19)[1]	*definiuje źródła, które identyfikują osoby stanowiące podwyższony poziom ryzyka;*
	SI-4(19)[2]	*określa dodatkowy monitoring, który należy wdrożyć w odniesieniu do osób, które zostały zidentyfikowane przez źródła określone przez organizację, jako stwarzające zwiększony poziom ryzyka; oraz*

SI-4(19)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *ZWIĘKSZONE RYZYKO GENEROWANE PRZEZ OSOBY***	
	SI-4(19)[3]	*wdraża zdefiniowany organizacyjnie dodatkowy monitoring osób, które zostały zidentyfikowane przez źródła zdefiniowane organizacyjnie, jako stwarzające zwiększony poziom ryzyka.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; lista osób, które zostały zidentyfikowane, jako stwarzające zwiększony poziom ryzyka; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspomagające i/lub wdrażające zdolność monitorowania systemu].	

SI-4(20)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *UPRZYWILEJOWANI UŻYTKOWNICY***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-4(20)[1]	*definiuje dodatkowy monitoring, który należy wdrożyć wobec uprzywilejowanych użytkowników; oraz*
	SI-4(20)[2]	*wdraża zdefiniowany organizacyjnie dodatkowy monitoring uprzywilejowanych użytkowników;*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; wykaz uprzywilejowanych użytkowników; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dzienniki lub rejestry monitorowania systemu informacyjnego;	

SI-4(20)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *UPRZYWILEJOWANI UŻYTKOWNICY***
	rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspomagające i/lub wdrażające zdolność monitorowania systemu].

SI-4(21)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *OKRESY PRÓBNE***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-4(21)[1]	*definiuje dodatkowy monitoring, który ma być realizowany wobec osób podczas okresu próbnego;*
	SI-4(21)[2]	*definiuje okres próbny, podczas którego ma być przeprowadzany dodatkowy monitoring osób, zdefiniowany przez organizację; oraz*
	SI-4(21)[3]	*wprowadza zdefiniowany organizacyjnie dodatkowy monitoring osób podczas określonego organizacyjnie okresu próbnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dzienniki lub rejestry monitorowania systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspomagające i/lub wdrażające zdolność monitorowania systemu].	

SI-4(22)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *NIEAUTORYZOWANE USŁUGI SIECIOWE***		
	CEL OCENY: *Określić, czy:*		
	SI-4(22)[1]	*organizacja określa procesy autoryzacji lub zatwierdzania usług sieciowych;*	
	SI-4(22)[2]	*organizacja określa personel lub role, które mają być powiadamiane o wykryciu usług sieciowych, które nie zostały autoryzowane lub zatwierdzone w ramach zdefiniowanych przez organizację procesów autoryzacji lub zatwierdzania;*	
	SI-4(22)[3]	*system informacyjny wykrywa usługi sieciowe, które nie zostały autoryzowane lub zatwierdzone w zdefiniowanych przez organizację procesach autoryzacji lub zatwierdzania oraz wykonuje jedną lub więcej z poniższych czynności:*	
		SI-4(22)[3][a]	*przeprowadza audyt; i/lub*
		SI-4(22)[3][b]	*powiadamia personel lub role zdefiniowane przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; udokumentowana autoryzacja/zatwierdzenie usług sieciowych; powiadomienia lub alerty dotyczące wykrycia nieautoryzowanych usług sieciowych; dzienniki lub rejestry monitorowania systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie systemu informacyjnego]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspomagające i/lub wdrażające zdolność monitorowania systemu; zautomatyzowane mechanizmy audytu usług sieciowych; zautomatyzowane mechanizmy powiadamiania o zagrożeniach].		

SI-4(23)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *KOMPUTER GŁÓWNY (HOST)***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-4(23)[1]	*definiuje mechanizmy monitorowania oparte na komputerach głównych (hostach), które należy wdrożyć;*
	SI-4(23)[2]	*definiuje komponenty systemu informacyjnego, w których ma być wdrażany zdefiniowany przez organizację monitoring oparty na hostach; oraz*
	SI-4(23)[3]	*implementuje mechanizmy monitorowania oparte na hostach w zdefiniowanych organizacyjnie komponentach systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące narzędzi i technik monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; mechanizmy monitorowania oparte na komputerach głównych (hostach); dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; wykaz elementów systemu informacyjnego wymagających monitorowania w oparciu o komputer główny (host); dzienniki lub rejestry monitorowania systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie komputerów głównych (hostów) systemu informacyjnego]. **Test**: [*wybierz spośród:* Procesy organizacyjne monitorowania systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające Zdolności monitorowania oparte na hostach].	

SI-4(24)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *WSKAŹNIKI RYZYKA***	
	CEL OCENY: *Ustalić, czy system informacyjny:*	
	SI-4(24)[1]	*odkrywa wskaźniki ryzyka;*

SI-4(24)	**MONITOROWANIE SYSTEMU INFORMACYJNEGO | *WSKAŹNIKI RYZYKA***	
	SI-4(24)[2]	*gromadzi wskaźniki ryzyka;*
	SI-4(24)[3]	*dystrybuuje wskaźniki ryzyka; oraz*
	SI-4(24)[4]	*wykorzystuje wskaźniki ryzyka.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące monitorowania systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; dokumentacja narzędzi i technik monitorowania systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i związana z tym dokumentacja; dzienniki lub rejestry monitorowania systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu; personel organizacji instalujący, konfigurujący i/lub utrzymujący system informacyjny; personel organizacji odpowiedzialny za monitorowanie komputerów głównych (hostów) systemu informacyjnego]. **Test**: [*wybierz spośród:* Procesy organizacyjne monitorowania systemu informacyjnego; procesy organizacyjne związane z odkrywaniem, gromadzeniem, dystrybucją oraz wykorzystaniem wskaźników ryzyka; zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwości monitorowania systemu; zautomatyzowane mechanizmy wspierające i/lub wdrażające odkrywanie, gromadzenie, dystrybucję oraz wykorzystanie wskaźników ryzyka].	

SI-5	**ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY**		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-5(a)	**SI-5(a)[1]**	*definiuje organizacje zewnętrzne, od których mają być otrzymywane alerty bezpieczeństwa systemu informacyjnego, poradniki oraz dyrektywy;*
		SI-5(a)[2]	*otrzymuje na bieżąco alerty bezpieczeństwa systemu informacyjnego, porady i dyrektywy od zdefiniowanych organizacji zewnętrznych;*
	SI-5(b)	*generuje, w razie potrzeby, wewnętrzne alerty bezpieczeństwa, porady i dyrektywy;*	

SI-5	**ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY**			
	SI-5(c)	**SI-5(c)[1]**	*określa personel lub role, którym należy przekazywać alerty bezpieczeństwa, porady i dyrektywy;*	
		SI-5(c)[2]	*definiuje podmioty w ramach organizacji, którym alerty bezpieczeństwa, porady i dyrektywy mają być dostarczane;*	
		SI-5(c)[3]	*definiuje organizacje zewnętrzne, którym alerty bezpieczeństwa, porady i dyrektywy mają być zapewnione;*	
		SI-5(c)[4]	*rozpowszechnia alerty bezpieczeństwa, porady i dyrektywy wśród jednego lub kilku poniższych, organizacyjnie zdefiniowanego/zdefiniowanych:*	
			SI-5(c)[4][a]	*personelu lub ról;*
			SI-5(c)[4][b]	*podmiotów w ramach organizacji; i/lub*
			SI-5(c)[4][c]	*organizacji zewnętrznych; oraz*
	SI-5(d)	**SI-5(d)[1]**	*wdraża dyrektywy dotyczące bezpieczeństwa zgodnie z ustalonymi ramami czasowymi; lub*	
		SI-5(d)[2]	*powiadamia organizację wydającą o stopniu niezgodności.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące alertów bezpieczeństwa, porad i dyrektyw; rejestry alarmów bezpieczeństwa i powiadomień o zagrożeniu; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za alerty bezpieczeństwa i doradztwo; personel organizacji wdrażający, obsługujący, utrzymujący i użytkujący system informacyjny; personel organizacji, elementy organizacyjne i/lub organizacje zewnętrzne, wśród których mają być rozpowszechniane alerty, poradniki oraz dyrektywy; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące definiowania, odbioru, generowania, rozpowszechniania oraz postępowania zgodnego z alertami bezpieczeństwa, poradami i dyrektywami; zautomatyzowane mechanizmy wspierające i/lub wdrażające definiowanie, odbiór, generowanie oraz rozpowszechnianie alertów bezpieczeństwa, porad i dyrektyw; zautomatyzowane mechanizmy wspierające i/lub wdrażające dyrektywy bezpieczeństwa].			

SI-5(1)	**ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY | *AUTOMATYCZNE ALERTY I PORADY***
	CEL OCENY: *Ustalenie, czy organizacja stosuje zautomatyzowane mechanizmy do udostępniania alertów bezpieczeństwa i informacji doradczych w całej organizacji.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące alertów bezpieczeństwa, porad i dyrektyw; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zautomatyzowane mechanizmy wspomagające dystrybucję alertów o zagrożeniu bezpieczeństwa oraz informacji doradczych; rejestry alarmów bezpieczeństwa i powiadomień o zagrożeniu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za alerty bezpieczeństwa i doradztwo; personel organizacji wdrażający, obsługujący, utrzymujący i użytkujący system informacyjny; personel organizacji, elementy organizacyjne i/lub organizacje zewnętrzne, wśród których mają być rozpowszechniane alerty, poradniki oraz dyrektywy; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące definiowaniu, odbieraniu, generowaniu i rozpowszechnianiu ostrzeżeń i porad dotyczących bezpieczeństwa; zautomatyzowane mechanizmy wspierające i/lub wdrażające rozpowszechnianie ostrzeżeń i porad dotyczących bezpieczeństwa].

SI-6	**WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA**		
	CEL OCENY: *Określić, czy:*		
	SI-6(a)	**SI-6(a)[1]**	*organizacja definiuje funkcje bezpieczeństwa, które mają być weryfikowane pod kątem prawidłowego działania;*
		SI-6(a)[2]	*system informacyjny weryfikuje prawidłowe działanie zdefiniowanych przez organizację funkcji bezpieczeństwa;*
	SI-6(b)	**SI-6(b)[1]**	*organizacja definiuje stany przejściowe systemu wymagające weryfikacji funkcji bezpieczeństwa zdefiniowanych przez organizację;*
		SI-6(b)[2]	*organizacja określa częstotliwość weryfikacji poprawnego działania zdefiniowanych przez organizację funkcji bezpieczeństwa;*

SI-6	**WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA**			
		SI-6(b)[3]	*system informacyjny przeprowadza weryfikację:*	
			SI-6(b)[3][a]	*w zdefiniowanych organizacyjnie stanach przejściowych systemu; i/lub*
			SI-6(b)[3][b]	*na polecenie użytkownika o odpowiednich uprawnieniach; i/lub*
			SI-6(b)[3][c]	*z częstotliwością określoną przez organizację;*
	SI-6(c)	**SI-6(c)[1]**	*organizacja określa personel lub role, które należy powiadomić o nieprzeprowadzonych testach weryfikacji bezpieczeństwa;*	
		SI-6(c)[2]	*system informacyjny powiadamia o nieprzeprowadzonych testach sprawdzających bezpieczeństwo zdefiniowany przez organizację personel lub role;*	
	SI-6(d)	**SI-6(d)[1]**	*organizacja określa alternatywne działanie(-a), które należy podjąć w przypadku wykrycia anomalii;*	
		SI-6(d)[2]	*w przypadku wykrycia anomalii system informacyjny wykonuje jedno lub więcej z następujących działań:*	
			SI-6(d)[2][a]	*wyłącza system informacyjny;*
			SI-6(d)[2][b]	*restartuje system informacyjny; i/lub*
			SI-6(d)[2][c]	*wykonuje zdefiniowane organizacyjnie działanie(-a) alternatywne.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące weryfikacji funkcji bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; alerty/powiadomienia o nieudanych testach weryfikacji bezpieczeństwa; wykaz stanów przejściowych systemu wymagających weryfikacji funkcjonalności bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację funkcji bezpieczeństwa; personel organizacji wdrażający, obsługujący i utrzymujący system informacyjny; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu].			

SI-6	**WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA**
	Test: [*wybierz spośród:* Procesy organizacyjne związane z weryfikacją funkcji bezpieczeństwa; zautomatyzowane mechanizmy wspierające i/lub wdrażające możliwości weryfikacji funkcji bezpieczeństwa].

SI-6(1)	**WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA | *POWIADOMIENIE O NIEUDANYCH TESTACH BEZPIECZEŃSTWA***
[Włączone do: SI-6].	

SI-6(2)	**WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA | *WSPARCIE AUTOMATYZACYJNE BADAŃ ROZPROSZONYCH***
	CEL OCENY: *Ustalić, czy system informacyjny wdraża zautomatyzowane mechanizmy wspomagające zarządzanie rozproszonymi testami bezpieczeństwa.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące weryfikacji funkcji bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację funkcji bezpieczeństwa; personel organizacji wdrażający, obsługujący i utrzymujący system informacyjny; administratorzy systemu/sieci; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie weryfikacji funkcji bezpieczeństwa; zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie rozproszonymi testami bezpieczeństwa].

SI-6(3)	**WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA | *RAPORT Z WYNIKÓW WERYFIKACJI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-6(3)[1]	*określa personel lub role wyznaczone do otrzymywania wyników weryfikacji funkcji bezpieczeństwa; oraz*
	SI-6(3)[2]	*przekazuje wyniki weryfikacji funkcji bezpieczeństwa personelowi lub rolom zdefiniowanym przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące weryfikacji funkcji bezpieczeństwa; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; ewidencja wyników weryfikacji funkcji bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację funkcji bezpieczeństwa; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z raportowaniem wyników weryfikacji funkcji bezpieczeństwa; zautomatyzowane mechanizmy wspierające i/lub wdrażające raportowanie wyników weryfikacji funkcji bezpieczeństwa].	

SI-7	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI**		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-7[1]	**SI-7[1][a]**	*definiuje oprogramowanie wymagające użycia narzędzi weryfikacji integralności w celu wykrycia nieautoryzowanych zmian;*
		SI-7[1][b]	*definiuje oprogramowanie układowe wymagające użycia narzędzi weryfikacji integralności w celu wykrycia nieautoryzowanych zmian;*
		SI-7[1][c]	*definiuje informacje wymagające użycia narzędzi do weryfikacji integralności w celu wykrycia nieautoryzowanych zmian;*

SI-7	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI**		
	SI-7[2]	*stosuje narzędzia weryfikacji integralności w celu wykrycia nieautoryzowanych zmian w zdefiniowanych organizacyjnie:*	
		SI-7[2][a]	*aplikacjach;*
		SI-7[2][b]	*oprogramowaniu układowym; oraz*
		SI-7[2][c]	*informacjach.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia weryfikacji integralności i powiązaną z nimi dokumentacja; zapisy generowane/wyświetlane z narzędzi weryfikacji integralności dotyczące oprogramowania nieautoryzowanego, oprogramowania układowego oraz zmian w informacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemów/sieci]. **Test**: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji].		

SI-7(1)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *KONTROLE INTEGRALNOŚCI***		
	CEL OCENY: *Określić, czy:*		
	SI-7(1)[1]	*organizacja określa:*	
		SI-7(1)[1][a]	*aplikacje wymagające dokonywania kontroli integralności;*
		SI-7(1)[1][b]	*oprogramowanie układowe wymagające wykonywania kontroli integralności;*
		SI-7(1)[1][c]	*informacje wymagające wykonania kontroli integralności;*

SI-7(1)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *KONTROLE INTEGRALNOŚCI***		
	SI-7(1)[2]	*organizacja określa stany przejściowe lub zdarzenia istotne dla bezpieczeństwa wymagające kontroli integralności organizacyjnie określonych:*	
		SI-7(1)[2][a]	*aplikacji*
		SI-7(1)[2][b]	*oprogramowania układowego;*
		SI-7(1)[2][c]	*informacji;*
	SI-7(1)[3]	*organizacja określa częstotliwość, z jaką należy przeprowadzać kontrolę integralności zdefiniowanych przez organizację:*	
		SI-7(1)[3][a]	*aplikacji*
		SI-7(1)[3][b]	*oprogramowania układowego;*
		SI-7(1)[3][c]	*informacji;*
	SI-7(1)[4]	*system informacyjny przeprowadza kontrolę integralności aplikacji zdefiniowanych przez organizację, oprogramowania układowego oraz informacji w jednym lub kilku z poniższych stanów:*	
		SI-7(1)[4][a]	*przy uruchamianiu;*
		SI-7(1)[4][b]	*w określonych przez organizację stanach przejściowych lub zdarzeniach mających znaczenie dla bezpieczeństwa; i/lub*
		SI-7(1)[4][c]	*z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia weryfikacji integralności i powiązana dokumentacja; rejestry skanów integralności; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji].		

SI-7(2)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *AUTOMATYCZNE POWIADOMIENIA O NARUSZENIACH INTEGRALNOŚCI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-7(2)[1]	*określa personel lub role, których należy powiadomić w przypadku wykrycia rozbieżności podczas weryfikacji integralności; oraz*
	SI-7(2)[2]	*korzysta ze zautomatyzowanych narzędzi, które zapewniają powiadamianie zdefiniowanego przez organizację personelu lub ról po wykryciu rozbieżności podczas weryfikacji integralności.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia weryfikacji integralności i powiązana dokumentacja; rejestry skanów integralności; zautomatyzowane narzędzia wspierające ostrzeżenia i powiadomienia o rozbieżnościach w zakresie integralności; ostrzeżenia/ powiadomienia dostarczane po wykryciu rozbieżności podczas weryfikacji integralności; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji; zautomatyzowane mechanizmy zapewniające powiadomienia o nieprawidłowościach w zakresie integralności].	

SI-7(3)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *NARZĘDZIA DO CENTRALNEGO ZARZĄDZANIA INTEGRALNOŚCIĄ***
	CEL OCENY: *Ustalić, czy organizacja stosuje centralnie zarządzane narzędzia weryfikacji integralności.*

SI-7(3)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *NARZĘDZIA DO CENTRALNEGO ZARZĄDZANIA INTEGRALNOŚCIĄ***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia weryfikacji integralności i powiązana dokumentacja; rejestry skanów integralności; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za centralne zarządzanie narzędziami weryfikacji integralności; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające centralne zarządzanie narzędziami weryfikacji integralności].

SI-7(4)	**WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA | *OCHRONA PRZED NARUSZENIAMI***
[Włączone do: SA-12].	

SI-7(5)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *AUTOMATYCZNA ODPOWIEDŹ NA NARUSZENIA INTEGRALNOŚCI***		
	CEL OCENY: *Określić, czy:*		
	SI-7(5)[1]	*organizacja określa środki bezpieczeństwa, które należy wdrożyć w przypadku wykrycia naruszeń integralności;*	
	SI-7(5)[2]	*system informacyjny automatycznie wykonuje jedno lub więcej z następujących działań w przypadku wykrycia naruszeń integralności:*	
		SI-7(5)[2][a]	*zamyka system informacyjny;*
		SI-7(5)[2][b]	*restartuje system informacyjny; i/lub*
		SI-7(5)[2][c]	*wprowadza określone organizacyjnie środki bezpieczeństwa.*

SI-7(5)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *AUTOMATYCZNA ODPOWIEDŹ NA NARUSZENIA INTEGRALNOŚCI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia weryfikacji integralności i powiązana dokumentacja; rejestry skanów integralności; dokumentacja kontroli integralności i reakcji na naruszenia integralności; dokumentacja audytu informacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji; zautomatyzowane mechanizmy zapewniające automatyczną odpowiedź na naruszenia integralności; zautomatyzowane mechanizmy wspierające i/lub wdrażające środki bezpieczeństwa, które powinny być wdrożone w przypadku wykrycia naruszeń integralności].

SI-7(6)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *OCHRONA KRYPTOGRAFICZNA***	
	CEL OCENY: *Ustalić, czy system informacyjny wykorzystuje mechanizm kryptograficzny do wykrywania nieautoryzowanych zmian w:*	
	SI-7(6)[1]	*aplikacjach;*
	SI-7(6)[2]	*oprogramowaniu układowym; oraz*
	SI-7(6)[3]	*informacjach.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; mechanizmy kryptograficzne oraz powiązana dokumentacja; rejestry wykrytych nieautoryzowanych zmian w aplikacjach, oprogramowaniu układowym i informacjach; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].	

SI-7(6)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *OCHRONA KRYPTOGRAFICZNA***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji; mechanizmy kryptograficzne wspomagające integralność aplikacji, oprogramowania układowego i informacji].

SI-7(7)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *INTEGRACJA WYKRYWANIA I ODPOWIEDZI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-7(7)[1]	*definiuje nieautoryzowane zmiany istotne z punktu widzenia bezpieczeństwa w systemie informacyjnym; oraz*
	SI-7(7)[2]	*włącza wykrywanie nieautoryzowanych, zdefiniowanych przez organizację zmian istotnych z punktu widzenia bezpieczeństwa w systemie informacyjnym, jako zdolność reagowania na incydenty organizacyjne.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; procedury dotyczące reagowania na incydenty; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; zapisy reakcji na incydenty; zapisy z audytu informacji; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; personel organizacji odpowiedzialny za reagowanie na incydenty]. **Test**: [*wybierz spośród:* Procesy organizacyjne mające na celu włączenie wykrywania nieautoryzowanych zmian istotnych dla bezpieczeństwa do Zdolności reagowania na incydenty; aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji; zautomatyzowane mechanizmy wspierające i/lub implementujące włączenie wykrywania nieautoryzowanych zmian istotnych dla bezpieczeństwa do Zdolności reagowania na incydenty].	

<table>
<tr><th colspan="5">SI-7(8) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | ZDOLNOŚĆ AUDYTU ISTOTNYCH ZDARZEŃ</th></tr>
<tr><td></td><td colspan="4">CEL OCENY:
Określić, czy:</td></tr>
<tr><td></td><td>SI-7(8)[1]</td><td colspan="3">organizacja wyznacza personel lub role, które mają być powiadamiane o wykryciu potencjalnego naruszenia integralności;</td></tr>
<tr><td></td><td>SI-7(8)[2]</td><td colspan="3">organizacja określa inne działania, które należy podjąć w przypadku wykrycia potencjalnego naruszenia integralności;</td></tr>
<tr><td></td><td rowspan="5">SI-7(8)[3]</td><td>SI-7(8)[3][a]</td><td colspan="2">system informacyjny, po wykryciu potencjalnego naruszenia integralności, zapewnia możliwość przeprowadzenia audytu tego zdarzenia;</td></tr>
<tr><td rowspan="4">SI-7(8)[3][b]</td><td colspan="2">system informacyjny, po wykryciu potencjalnego naruszenia integralności, inicjuje jedno lub więcej z następujących działań:</td></tr>
<tr><td>SI-7(8)[3][b][1]</td><td>generuje zapis z audytu;</td></tr>
<tr><td>SI-7(8)[3][b][2]</td><td>alarmuje aktualnego użytkownika;</td></tr>
<tr><td>SI-7(8)[3][b][3]</td><td>alarmuje personel lub role określone przez organizację; i/lub</td></tr>
<tr><td>SI-7(8)[3][b][4]</td><td>podejmuje inne organizacyjnie zdefiniowane działania.</td></tr>
<tr><td></td><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia weryfikacji integralności i powiązana dokumentacja; rejestry skanów integralności; zapisy reakcji na incydenty, wykaz zmian istotnych z punktu widzenia bezpieczeństwa w systemie informacyjnym; zautomatyzowane narzędzia obsługujące alerty oraz powiadomienia w przypadku wykrycia nieautoryzowanych zmian w zakresie bezpieczeństwa; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu].</td></tr>
</table>

SI-7(8)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *ZDOLNOŚĆ AUDYTU ISTOTNYCH ZDARZEŃ***
	Test: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji; wykaz zmian istotnych z punktu widzenia bezpieczeństwa w systemie informacyjnym; zautomatyzowane narzędzia obsługujące alerty oraz powiadomienia w przypadku wykrycia nieautoryzowanych zmian w zakresie bezpieczeństwa].

SI-7(9)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *WERYFIKACJA PROCESU URUCHAMIANIA***	
	CEL OCENY: *Określić, czy:*	
	SI-7(9)[1]	*organizacja ustala urządzenia wymagające weryfikacji integralności procesu uruchamiania systemu; oraz*
	SI-7(9)[2]	*system informacyjny weryfikuje integralność procesu uruchamiania urządzeń zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia do weryfikacji integralności i powiązana dokumentacja; dokumentacja; rejestry skanów weryfikacji integralności; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; deweloper systemu]. **Test**: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające integralność weryfikacji procesu uruchamiania systemu].	

SI-7(10)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *OCHRONA URUCHAMIANIA OPROGRAMOWANIA UKŁADOWEGO***	
	CEL OCENY: *Ustalić, czy:*	
	SI-7(10)[1]	*organizacja określa zabezpieczenia, które należy wdrożyć w celu ochrony integralności oprogramowania układowego w urządzeniach;*
	SI-7(10)[2]	*organizacja określa urządzenia wymagające zdefiniowanych przez organizację zabezpieczeń, które należy wdrożyć w celu ochrony integralności oprogramowania układowego; oraz*
	SI-7(10)[3]	*system informacyjny wdraża środki bezpieczeństwa zdefiniowane przez organizację w celu ochrony integralności oprogramowania układowego w urządzeniach zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; narzędzia do weryfikacji integralności i powiązana dokumentacja; rejestry skanów weryfikacji integralności; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji; automatyczne mechanizmy wspierające lub wdrażające ochronę integralności oprogramowania układowego; zabezpieczenia wdrażające ochronę integralności oprogramowania układowego].	

SI-7(11)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *ZAMKNIĘTE ŚRODOWISKO Z OGRANICZONYMI UPRAWNIENIAMI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-7(11)[1]	*definiuje oprogramowanie instalowane przez użytkownika, które ma być wykonywane w ograniczonym fizycznym lub wirtualnym środowisku maszyny z ograniczonymi uprawnieniami; oraz*
	SI-7(11)[2]	*wymaga, aby zdefiniowane organizacyjnie oprogramowanie instalowane przez użytkownika było uruchamiane w ograniczonym fizycznym lub wirtualnym środowisku maszyny z ograniczonymi uprawnieniami.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji; zautomatyzowane mechanizmy wspierające lub wdrażające wykonywanie oprogramowania w ograniczonym środowisku (fizycznym lub wirtualnym); zautomatyzowane mechanizmy wspierające lub wdrażające ograniczone uprawnienia w ograniczonym środowisku].	

SI-7(12)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *WERYFIKACJA INTEGRALNOŚCI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-7(12)[1]	*definiuje oprogramowanie instalowane przez użytkownika, wymagające weryfikacji integralności przed wykonaniem; oraz*
	SI-7(12)[2]	*wymaga, aby integralność zdefiniowanego organizacyjnie oprogramowania instalowanego przez użytkownika była weryfikowana przed wykonaniem.*

SI-7(12)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *WERYFIKACJA INTEGRALNOŚCI***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja weryfikacji integralności; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji; automatyczne mechanizmy wspomagające i/lub wdrażające weryfikację integralności oprogramowania zainstalowanego przez użytkownika przed jego wykonaniem].

SI-7(13)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *WYKONANIE KODU W ŚRODOWISKACH CHRONIONYCH***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-7(13)[1]	*umożliwia wykonanie kodu binarnego lub maszynowego uzyskanego ze źródeł z ograniczoną gwarancją lub bez gwarancji;*
	SI-7(13)[2]	*pozwala na wykonanie kodu binarnego lub maszynowego bez udostępniania kodu źródłowego tylko w ograniczonych maszynach fizycznych lub wirtualnych;*
	SI-7(13)[3]	*określa personel lub role wymagane do udzielania jednoznacznej zgody na wykonanie kodu binarnego lub maszynowego; oraz*
	SI-7(13)[4]	*umożliwia wykonanie kodu binarnego lub maszynowego za uprzednią pisemną zgodą zdefiniowanego przez organizację personelu lub ról.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry zatwierdzające	

SI-7(13)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *WYKONANIE KODU W ŚRODOWISKACH CHRONIONYCH***
	wykonanie kodu binarnego i kodu wykonywanego maszynowo; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające zatwierdzanie wykonania kodu binarnego lub kodu wykonywanego maszynowo].

SI-7(14)	**, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *KOD WYKONYWALNY BINARNY LUB MASZYNOWY***		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-7(14)(a)	**SI-7(14)(a)[1]**	*zakazuje używania kodu binarnego lub maszynowego ze źródeł z ograniczoną gwarancją lub bez gwarancji;*
		SI-7(14)(a)[2]	*zakazuje stosowania kodu binarnego lub maszynowego bez podania kodu źródłowego;*
	SI-7(14)(b)	**SI-7(14)(b)[1]**	*przewiduje wyjątki od wymogu kod źródłowy tylko w przypadku istotnych wymagań misyjnych/operacyjnych; oraz*
		SI-7(14)(b)[2]	*przewiduje wyjątki od wymogu podawania kodu źródłowego tylko za zgodą upoważnionej osoby.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry zatwierdzające wykonanie kodu binarnego i kodu wykonywanego maszynowo; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].		

SI-7(14)	**, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *KOD WYKONYWALNY BINARNY LUB MASZYNOWY***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; osoba autoryzująca; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające lub wprowadzające zakaz wykonywania kodu binarnego lub kodu wykonywanego maszynowo].

SI-7(15)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *AUTORYZACJA KODU***		
	CEL OCENY: *Określić, czy:*		
	SI-7(15)[1]	**SI-7(15)[1][a]**	*organizacja określa składniki oprogramowania, które przed instalacją muszą być uwierzytelnione przez mechanizmy kryptograficzne;*
		SI-7(15)[1][b]	*organizacja określa składniki oprogramowania układowego, które przed instalacją muszą zostać uwierzytelnione przez mechanizm kryptograficzny;*
	SI-7(15)[2]	**SI-7(15)[2][a]**	*system informacyjny wdraża mechanizm kryptograficzny w celu uwierzytelniania przed instalacją składników oprogramowania określonych przez organizację; oraz*
		SI-7(15)[2][b]	*system informacyjny implementuje mechanizmy kryptograficzne do uwierzytelniania przed instalacją komponentów oprogramowania układowego zdefiniowanych organizacyjnie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące aplikacji, oprogramowania układowego i integralność informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; mechanizmy kryptograficzne I powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].		

SI-7(15)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *AUTORYZACJA KODU***
	Wywiad: [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Mechanizmy kryptograficznego uwierzytelniające aplikacje/oprogramowanie układowe przed instalacją].

SI-7(16)	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | *LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-7(16)[1]	*definiuje okres czasu, jako maksymalny okres dopuszczalny dla procesów wykonywanych bez nadzoru; oraz*
	SI-7(16)[2]	*nie pozwala na realizację procesów bez nadzoru przez okres dłuższy niż określony przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące integralności aplikacji i informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za aplikacje, oprogramowanie układowe i/lub integralność informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Aplikacje, oprogramowanie układowe i narzędzia weryfikacji integralności informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające limity czasowe realizacji procesu bez nadzoru].	

SI-8	**OCHRONA PRZED SPAMEM**		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-8(a)	*wykorzystuje mechanizmy ochrony przed spamem:*	
		SI-8(a)[1]	*w punktach wejścia do systemu informacyjnego w celu wykrycia niechcianych wiadomości;*
		SI-8(a)[2]	*w punktach wejścia do systemu informacyjnego w celu podjęcia działań w związku z niezamówionymi wiadomościami;*
		SI-8(a)[3]	*w punktach wyjścia systemu informacyjnego w celu wykrycia niechcianych wiadomości;*
		SI-8(a)[4]	*w punktach wyjścia z systemu informacyjnego w celu podjęcia działań w związku z niezamówionymi wiadomościami; oraz*
	SI-8(b)	*aktualizuje mechanizmy ochrony przed spamem, gdy nowe wersje aktualizacyjne są dostępne zgodnie z polityką organizacyjną i procedurą zarządzania konfiguracją.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; polityka i procedury zarządzanie konfiguracją (CM-1); procedury dotyczące ochrony przed spamem; mechanizmy ochrony przed spamem; zapisy aktualizacji mechanizmów ochrony przed spamem; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę przed spamem; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące wdrożenia ochrony przed spamem; zautomatyzowane mechanizmy wspierające i/lub wdrażające ochronę przed spamem].		

SI-8(1)	**OCHRONA PRZED SPAMEM | *CENTRALNE ZARZĄDZANIE***
	CEL OCENY: *Ustalić, czy organizacja centralnie zarządza mechanizmami ochrony przed spamem.*

SI-8(1)	**OCHRONA PRZED SPAMEM | *CENTRALNE ZARZĄDZANIE***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące ochrony przed spamem; mechanizmy ochrony przed spamem; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę przed spamem; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie centralnego zarządzania ochroną przed spamem; zautomatyzowane mechanizmy wspierające i/lub wdrażające centralne zarządzanie ochroną przed spamem].

SI-8(2)	**OCHRONA PRZED SPAMEM | *AUTOMATYCZNE AKTUALIZACJE***
	CEL OCENY: *Ustalić, czy system informacyjny automatycznie aktualizuje mechanizmy ochrony przed spamem.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące ochrony przed spamem; mechanizmy ochrony przed spamem; zapisy aktualizacji mechanizmów ochrony przed spamem; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę przed spamem; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie ochrony przed spamem; zautomatyzowane mechanizmy wspierające i/lub wdrażające automatyczne aktualizacje do mechanizmów ochrony przed spamem].

SI-8(3)	**OCHRONA PRZED SPAMEM | *CIĄGŁA ZDOLNOŚĆ DO NAUKI***
	CEL OCENY: *Ustalić, czy system informacyjny wdraża mechanizmy ochrony przed spamem z możliwością uczenia się, w celu skuteczniejszej identyfikacji legalnego ruchu telekomunikacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące ochrony przed spamem; mechanizmy ochrony przed spamem; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za ochronę przed spamem; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie ochrony przed spamem; zautomatyzowane mechanizmy wspierające i/lub wdrażające mechanizmy ochrony przed spamem z możliwością nauki].

SI-9	**OGRANICZENIA WPROWADZANIA INFORMACJI**
[Włączone do: AC-2, AC-3, AC-5, AC-6].	

SI-10	**WERYFIKACJA WPROWADZANYCH INFORMACJI**	
	CEL OCENY: *Określić, czy:*	
	SI-10[1]	*organizacja określa informacje wejściowe wymagające kontroli wiarygodności; oraz*
	SI-10[2]	*system informacyjny sprawdza wiarygodność wprowadzanych informacji zdefiniowanych przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; zasady i procedury kontroli dostępu; polityka i procedury w zakresie rozdziału obowiązków; procedury dotyczące weryfikacji wprowadzanych informacji; dokumentacja narzędzi automatycznych oraz wniosków o weryfikację wiarygodności informacji; wykaz wprowadzanych informacji wymagających weryfikacji wiarygodności; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację wprowadzanych informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające kontrole wiarygodności wprowadzanych informacji].	

SI-10(1)	**WERYFIKACJA WPROWADZANYCH INFORMACJI | *RĘCZNE ZASTĘPOWANIE***		
	CEL OCENY: *Określić, czy:*		
	SI-10(1)(a)	**SI-10(1)(a)[1]**	*organizacja definiuje informacje wejściowe, dla których system informacyjny zapewnia możliwość ręcznego zastąpienia weryfikacji danych wejściowych;*
		SI-10(1)(a)[2]	*system informacyjny zapewnia możliwość ręcznego zastąpienia w celu weryfikacji poprawności danych wejściowych zdefiniowanych przez organizację;*
	SI-10(1)(b)	**SI-10(1)(b)[1]**	*organizacja definiuje upoważnione osoby, które mogą korzystać z funkcji zastępowania ręcznego;*

SI-10(1)	**WERYFIKACJA WPROWADZANYCH INFORMACJI | *RĘCZNE ZASTĘPOWANIE***		
		SI-10(1)(b)[2]	*system informacyjny ogranicza korzystanie z możliwości zastąpienia ręcznego wprowadzania danych do osób upoważnionych zdefiniowanych przez organizację; oraz*
	SI-10(1)(c)	*system informacyjny kontroluje korzystanie z zastępowania ręcznego.*	
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; zasady i procedury kontroli dostępu; polityka i procedury rozdziału obowiązków; procedury dotyczące weryfikacji wprowadzanych informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację wprowadzanych informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z wykorzystaniem funkcji zastępowania ręcznego; zautomatyzowane mechanizmy wspomagające i/lub wdrażające funkcję zastępowania ręcznego w celu weryfikacji danych wejściowych; zautomatyzowane mechanizmy wspomagające i/lub wdrażające audyt wykorzystania funkcji zastępowania ręcznego].		

SI-10(2)	**WERYFIKACJA WPROWADZANYCH INFORMACJI | *PRZEGLĄD / USUWANIE BŁĘDÓW***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-10(2)[1]	*określa okres czasu, w którym należy dokonać przeglądu i usunięcia błędów weryfikacji danych wejściowych; oraz*
	SI-10(2)[2]	*zapewnia, że błędy weryfikacji danych wejściowych są sprawdzane i rozwiązywane w określonym przez organizację okresie czasu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; zasady i procedury kontroli dostępu; polityka i procedury rozdziału obowiązków; procedury dotyczące weryfikacji wprowadzanych informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; przeglądanie zapisów dotyczących błędów weryfikacji poprawności wprowadzanych informacji i wynikających z nich	

SI-10(2)	WERYFIKACJA WPROWADZANYCH INFORMACJI | *PRZEGLĄD / USUWANIE BŁĘDÓW*
	działań; zapisy lub dzienniki błędów weryfikacji wprowadzanych informacji; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację wprowadzanych informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące przeglądu i rozwiązywania błędów weryfikacji danych wejściowych; zautomatyzowane mechanizmy wspierające i/lub wdrażające przegląd i rozwiązywanie błędów weryfikacji danych wejściowych].

SI-10(3)	WERYFIKACJA WPROWADZANYCH INFORMACJI | *PRZEWIDYWALNE ZACHOWANIE*
	CEL OCENY: *Ustalić, czy system informacyjny zachowuje się w sposób przewidywalny i udokumentowany, odzwierciedlający cele organizacyjne i systemowe w przypadku otrzymania nieprawidłowych danych wejściowych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące weryfikacji wprowadzanych informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację wprowadzanych informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub implementujące przewidywalne zachowanie w przypadku otrzymania niepoprawnych danych wejściowych].

SI-10(4)	**WERYFIKACJA WPROWADZANYCH INFORMACJI | *INTERAKCJE CZASOWE***
	CEL OCENY: *Ustalenie, czy organizacja uwzględnia interakcje czasowe pomiędzy komponentami systemu informacyjnego przy określaniu właściwych odpowiedzi na nieprawidłowe dane wejściowe.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące weryfikacji wprowadzanych informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację wprowadzanych informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Procesy organizacyjne służące do określania odpowiednich reakcji na nieprawidłowe dane wejściowe; zautomatyzowane mechanizmy wspierające i/lub wdrażające reakcje na nieprawidłowe dane wejściowe].

SI-10(5)	**WERYFIKACJA WPROWADZANYCH INFORMACJI | *OGRANICZANIE DANYCH WEJŚCIOWYCH DO ZAUFANYCH ŹRÓDEŁ I ZATWIERDZONYCH FORMATÓW***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-10(5)[1]	*definiuje zaufane źródła, do których należy ograniczyć korzystanie z informacji wejściowych;*
	SI-10(5)[2]	*definiuje formaty, do których wykorzystanie danych wejściowych informacji ma być ograniczone;*
	SI-10(5)[3]	*ogranicza korzystanie z informacji wejściowych do:*
	SI-10(5)[3][a]	*źródeł zaufania zdefiniowanych przez organizację; i/lub*
	SI-10(5)[3][b]	*formatów zdefiniowanych organizacyjnie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące weryfikacji wprowadzanych informacji; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego	

SI-10(5)	**WERYFIKACJA WPROWADZANYCH INFORMACJI | *OGRANICZANIE DANYCH WEJŚCIOWYCH DO ZAUFANYCH ŹRÓDEŁ I ZATWIERDZONYCH FORMATÓW***	
	i powiązana dokumentacja; lista zaufanych źródeł informacji wejściowej; lista dopuszczalnych formatów ograniczeń dotyczących wprowadzania danych; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację wprowadzanych informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Procesy organizacyjne mające na celu ograniczenie ilości wprowadzanych informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające ograniczenie ilości wprowadzanych informacji].	

SI-11	**OBSŁUGA BŁĘDÓW**	
	CEL OCENY: *Określić, czy:*	
	SI-11(a)	*system informacyjny generuje komunikaty o błędach, które dostarczają informacji niezbędnych do działań naprawczych, nie ujawniając informacji, które mogłyby zostać wykorzystane przez przeciwników;*
	SI-11(b)	**SI-11(b)[1]** *organizacja określa personel lub role, którym mają być przekazywane komunikaty o błędach; oraz*
		SI-11(b)[2] *system informacyjny udostępnia komunikaty o błędach tylko personelowi lub rolom zdefiniowanym przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące obsługi błędów systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja zawierająca strukturę/treść komunikatów o błędach; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację wprowadzanych informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu].	

SI-11	**OBSŁUGA BŁĘDÓW**
	Test: [*wybierz spośród:* Procesy organizacyjne dotyczące obsługi błędów; zautomatyzowane mechanizmy wspierające i/lub wdrażające obsługę błędów; zautomatyzowane mechanizmy wspierające i/lub wdrażające zarządzanie komunikatami o błędach].

SI-12	**PRZECHOWYWANIE I RETENCJA INFORMACJI**	
	CEL OCENY: *Ustalić, czy organizacja, zgodnie z obowiązującym przepisami, rozporządzeniami wykonawczymi, dyrektywami, zasadami, regulacjami, standardami i wymaganiami operacyjnymi:*	
	SI-12[1]	*przetwarza informacje w ramach systemu informacyjnego;*
	SI-12[2]	*przetwarza dane wyjściowe z systemu informacyjnego;*
	SI-12[3]	*przechowuje informacje w systemie informacyjnym; oraz*
	SI-12[4]	*przechowuje dane wyjściowe z systemu informacyjnego.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; przepisy, rozporządzenia wykonawcze, dyrektywy, polityki, regulacje, standardy oraz wymagania operacyjne mające zastosowanie do przechowywania i retencji informacji; polityka i procedury ochrony nośników danych; procedury dotyczące obsługi i przechowywania danych przetwarzanych w systemie informacyjnym; zapisy dotyczące retencji informacji, inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za przechowywanie i retencję informacji; personel organizacji odpowiedzialny za bezpieczeństwo informacji/administratorzy sieci]. **Test**: [*wybierz spośród:* Procesy organizacyjne w zakresie przechowywania i retencji informacji; zautomatyzowane mechanizmy wspierające i/lub wdrażające przechowywanie i retencję informacji].	

SI-13	**PRZEWIDYWANIE AWARII**		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-13(a)	**SI-13(a)[1]**	*definiuje elementy systemu informacyjnego, dla których należy określić średni czas między awariami (MTTF);*
		SI-13(a)[2]	*określa MTTF dla zdefiniowanych przez organizację komponentów systemu informacyjnego w określonych środowiskach działania;*
	SI-13(b)	**SI-13(b)[1]**	*definiuje kryteria zastępcze dotyczące MTTF, które mają być stosowane, jako środek wymiany komponentów aktywnych i rezerwowych;*
		SI-13(b)[2]	*zapewnia zastępcze składniki systemu informacyjnego w zdefiniowanych przez organizację kryteriach zastępczych dotyczących MTTF; oraz*
		SI-13(b)[3]	*zapewnia środki do wymiany aktywnych i rezerwowych komponentów przy zdefiniowanych przez organizację kryteriach zastępowania MTTF.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące przewidywania awarii; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz kryteriów zastępczych dotyczących MTTF; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określanie MTTF i działania związane z MTTF; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacji odpowiedzialny za plan ciągłości działania]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z zarządzaniem MTTF].		

SI-13(1)	**PRZEWIDYWANIE AWARII | *PRZENIESIENIE ODPOWIEDZIALNOŚCI KOMPONENTÓW***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-13(1)[1]	*określa maksymalny ułamek lub procent średniego czasu, w którym nie można przenieść odpowiedzialności za komponent systemu informacyjnego, który jest wyłączony z eksploatacji, na komponent zastępczy; oraz*
	SI-13(1)[2]	*wyłącza komponent systemu informacyjnego z eksploatacji, przenosząc odpowiedzialność za komponent na komponenty zastępcze nie później niż w określonym przez organizację ułamku lub procencie średniego czasu do wystąpienia awarii.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące przewidywania awarii; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określanie MTTF; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacji odpowiedzialny za plan ciągłości działania]. **Test**: [*wybierz spośród:* Procesy organizacyjne zarządzania MTTF; zautomatyzowane mechanizmy wspierające i/lub wdrażające przeniesienie odpowiedzialności za komponent na komponenty zastępcze].	

SI-13(2)	**PRZEWIDYWANIE AWARII | *LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU***
[Włączone do: SI-7(16)].	

SI-13(3)	**PRZEWIDYWANIE AWARII | *RĘCZNY TRANSFER MIĘDZY SKŁADNIKAMI***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-13(3)[1]	*określa minimalną częstotliwość, z jaką organizacja ręcznie inicjuje transfer pomiędzy aktywnym i rezerwowymi komponentami systemu informacyjnego, jeśli średni czas do wystąpienia awarii przekracza określony przez organizację okres czasu;*
	SI-13(3)[2]	*definiuje okres czasu, który musi upłynąć od średniego czasu między awariami, przed rozpoczęciem przez organizację ręcznego inicjowania transferu między aktywnym i rezerwowymi komponentami systemu informacyjnego; oraz*
	SI-13(3)[3]	*ręcznie inicjuje transfery pomiędzy komponentami systemu informacyjnego aktywnego i rezerwowego z częstotliwością określoną przez organizację, jeżeli średni czas do wystąpienia awarii przekracza okres czasu określony przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące przewidywania awarii; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za określanie MTTF; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacji odpowiedzialny za plan ciągłości działania]. **Test**: [*wybierz spośród:* Procesy organizacyjne związane z zarządzaniem MTTF oraz przeprowadzaniem ręcznego transferu pomiędzy komponentami aktywnym i rezerwowymi].	

<table>
<tr><td colspan="5">SI-13(4) PRZEWIDYWANIE AWARII | INSTALACJA KOMPONENTÓW Z LISTY REZERWOWEJ / POWIADOMIENIE</td></tr>
<tr><td></td><td colspan="4">CEL OCENY:
Określić, czy organizacja:</td></tr>
<tr><td></td><td>SI-13(4)(a)</td><td>SI-13(4)(a)[1]</td><td colspan="2">definiuje okres czasu, w którym rezerwowe komponenty systemu informacyjnego mają zostać skutecznie i transparentnie zainstalowane w przypadku wykrycia awarii komponentów systemu informacyjnego;</td></tr>
<tr><td></td><td></td><td>SI-13(4)(a)[2]</td><td colspan="2">zapewnia skuteczną i transparentną instalację rezerwowych komponentów systemu informacyjnego w określonym przez organizację okresie czasu;</td></tr>
<tr><td></td><td>SI-13(4)(b)</td><td>SI-13(4)(b)[1]</td><td colspan="2">definiuje alarm, który ma być aktywowany w przypadku wykrycia awarii komponentów systemu informacyjnego;</td></tr>
<tr><td></td><td></td><td rowspan="3">SI-13(4)(b)[2]</td><td colspan="2">w przypadku wykrycia awarii komponentów systemu informacyjnego wykonuje jedną lub więcej z poniższych czynności:</td></tr>
<tr><td></td><td></td><td>SI-13(4)(b)[2][a]</td><td>aktywuje alarm zdefiniowany przez organizację; i/lub</td></tr>
<tr><td></td><td></td><td>SI-13(4)(b)[2][b]</td><td>automatycznie wyłącza system informacyjny.</td></tr>
<tr><td></td><td colspan="4">POTENCJALNE METODY I OBIEKTY OCENY:
Sprawdź: [wybierz spośród: Polityka integralności systemu i informacji; procedury dotyczące przewidywania awarii; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; wykaz działań, które należy podjąć po wykryciu awarii komponentu systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry].
Wywiad: [wybierz spośród: Personel organizacji odpowiedzialny za określanie MTTF; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacji odpowiedzialny za plan ciągłości działania].
Test: [wybierz spośród: Procesy organizacyjne zarządzania MTTF; zautomatyzowane mechanizmy wspierające i/lub wdrażające transparentną instalację komponentów rezerwowych; zautomatyzowane mechanizmy wspierające i/lub wdrażające alarmy lub wyłączanie systemu w przypadku wykrycia awarii komponentów].</td></tr>
</table>

SI-13(5)	**PRZEWIDYWANIE AWARII | *PRZEŁĄCZANIE AWARYJNE***		
	CEL OCENY: *Określić, czy organizacja:*		
	SI-13(5)[1]	*definiuje zdolność przełączania awaryjnego, którą należy zapewnić na potrzeby systemu informacyjnego;*	
	SI-13(5)[2]	*zapewnia jedną z następujących, zdefiniowanych przez organizację, Zdolności przejmowania funkcji w przypadku awarii systemu informacyjnego:*	
		SI-13(5)[2][a]	*prace przełączeniowe w czasie rzeczywistym; i/lub*
		SI-13(5)[2][b]	*prace przełączeniowe w akceptowanym czasie odpowiedzi na awarie.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące przewidywania awarii; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; dokumentacja dotycząca przełączania awaryjnego dostarczona dla systemu informacyjnego; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za przełączanie awaryjne; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; personel organizacji odpowiedzialny za plan ciągłości działania]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące zarządzania programem przełączania awaryjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające program przełączania awaryjnego].		

SI-14	**ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM (ATAKI TYPU APT)**	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-14[1]	*definiuje nietrwałe komponenty systemu informacyjnego oraz usługi, które mają zostać wdrożone;*

SI-14	**ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM (ATAKI TYPU APT)**			
	SI-14[2]	**SI-14[2][a]**	*definiuje częstotliwość kończenia nietrwałych komponentów i usług, zdefiniowanych przez organizację, które są inicjowane w znanym stanie;*	
		SI-14[2][b]	*implementuje nietrwałe, zdefiniowane przez organizację składniki systemu informacyjnego oraz usługi, które są inicjowane w znanym stanie i które zakończyły jeden lub więcej z poniższych elementów:*	
			SI-14[2][b][1]	*po zakończeniu sesji użytkowania; i/lub*
			SI-14[2][b][2]	*okresowo z częstotliwością określoną przez organizację.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące nietrwałości składników elementów systemu informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za nietrwałość komponentów; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające inicjację i wycofanie komponentów nietrwałych].			

SI-14(1)	**ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM (ATAKI TYPU APT) | *ODŚWIEŻANIE Z ZAUFANYCH ŹRÓDEŁ***	
	CEL OCENY: *Określić, czy organizacja:*	
	SI-14(1)[1]	*definiuje zaufane źródła, z których należy pozyskiwać oprogramowanie i dane wykorzystywane podczas aktualizacji komponentów systemu informacyjnego i usług serwisowych; oraz*
	SI-14(1)[2]	*zapewnia, że oprogramowanie i dane wykorzystywane podczas aktualizacji komponentów systemu informacyjnego i usług serwisowych są pozyskiwane ze zdefiniowanych przez organizację zaufanych źródeł.*

SI-14(1)	**ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM (ATAKI TYPU APT) | *ODŚWIEŻANIE Z ZAUFANYCH ŹRÓDEŁ***
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące zapobieganiu zaawansowanym długotrwałym atakom (ataki typu APT) na komponenty system informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za pozyskiwanie podzespołów i usług serwisowych z zaufanych źródeł; personel organizacji odpowiedzialny za bezpieczeństwo informacji]. **Test**: [*wybierz spośród:* Procesy organizacyjne dotyczące definiowania i uzyskiwania uaktualnień komponentów i usług z zaufanych źródeł; zautomatyzowane mechanizmy wspierające i/lub wdrażające uaktualnienia komponentów i usług].

SI-15	**FILTROWANIE INFORMACJI WYJŚCIOWYCH**	
	CEL OCENY: *Określić, czy:*	
	SI-15[1]	*organizacja określa programy i/lub aplikacje, których dane wyjściowe wymagają weryfikacji w celu zapewnienia, że informacje są zgodne z oczekiwaną zawartością; oraz*
	SI-15[2]	*system informacyjny weryfikuje informacje wyjściowe z programów i/lub aplikacji zdefiniowanych przez organizację w celu zapewnienia zgodności informacji z oczekiwaną zawartością.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące filtrowania informacji wyjściowych; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za weryfikację informacji wyjściowych; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu].	

SI-15	**FILTROWANIE INFORMACJI WYJŚCIOWYCH**
	Test: [*wybierz spośród:* Procesy organizacyjne weryfikacji informacji wyjściowych; zautomatyzowane mechanizmy wspierające i/lub wdrażające weryfikację informacji wyjściowych].

SI-16	**OCHRONA PAMIĘCI**	
	CEL OCENY: *Określić, czy:*	
	SI-16[1]	*organizacja określa zabezpieczenia, które należy wdrożyć w celu ochrony pamięci systemu informacyjnego przed nieautoryzowanym wykonaniem kodu; oraz*
	SI-16[2]	*system informacyjny wdraża określone organizacyjnie zabezpieczenia w celu ochrony własnej pamięci przed nieautoryzowanym wykonaniem kodu.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące ochrony pamięci system informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista zabezpieczeń chroniących pamięć systemu informacyjnego przed nieautoryzowanym wykonaniem kodu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za zabezpieczenie pamięci; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Zautomatyzowane mechanizmy wspierające i/lub wdrażające zabezpieczenia chroniące pamięć systemu informacyjnego przed nieautoryzowanym wykonaniem kodu].	

SI-17	**BEZPIECZNE PROCEDURY**	
	CEL OCENY: *Określić, czy:*	
	SI-17[1]	*organizacja określa bezpieczne procedury, która ma być wdrożona w przypadku wystąpienia określonych przez organizację stanów awaryjnych;*

SI-17	**BEZPIECZNE PROCEDURY**	
	SI-17[2]	*organizacja określa stany awaryjne, w wyniku których zdefiniowana przez organizację bezpieczne procedury zostanie wdrożona w momencie wystąpienia takich stanów; oraz*
	SI-17[3]	*system informacyjny wdraża zdefiniowaną przez organizację bezpieczne procedury w przypadku wystąpienia zdefiniowanych przez organizację stanów awaryjnych.*
	POTENCJALNE METODY I OBIEKTY OCENY: **Sprawdź:** [*wybierz spośród:* Polityka integralności systemu i informacji; procedury dotyczące ochrony pamięci system informacyjnego; dokumentacja projektowa systemu informacyjnego; ustawienia konfiguracji systemu informacyjnego i powiązana dokumentacja; lista zabezpieczeń chroniących pamięć systemu informacyjnego przed nieautoryzowanym wykonaniem kodu; rejestry audytów systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [*wybierz spośród:* Personel organizacji odpowiedzialny za bezpieczne procedury; personel organizacji odpowiedzialny za bezpieczeństwo informacji; administratorzy systemu/sieci; deweloper systemu]. **Test**: [*wybierz spośród:* Organizacyjne bezpieczne procedury; zautomatyzowane mechanizmy wspierające i/lub wdrażające bezpieczne procedury].	