NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	Narodowy Standard Cyberbezpieczeństwa		
Nazwa standardu	Symbol	Wersja	Data wydania
Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu.	**NSC 800-37**	1.0	01/09/2021

Ramy Zarządzania Ryzykiem w Organizacjach i Systemach Informatycznych

Bezpieczeństwo i ochrona prywatności w cyklu życia systemu

PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA
Warszawa 2021

Szanowni Państwo,

Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów udostępnia do wykorzystania w Państwa działalności zestaw publikacji specjalnych. Stanowią one rekomendację w postaci Narodowych Standardów Cyberbezpieczeństwa, o których mowa w kierunku interwencji 6.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, *Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń*. Mimo, że prezentowane standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST), to posiadają one mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, stosowane w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych.

Zaprezentowane publikacje stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę, jaka w tym zakresie stosowana jest w administracji federalnej USA.

Na prezentowany zestaw publikacji składają się następujące pozycje:[1]

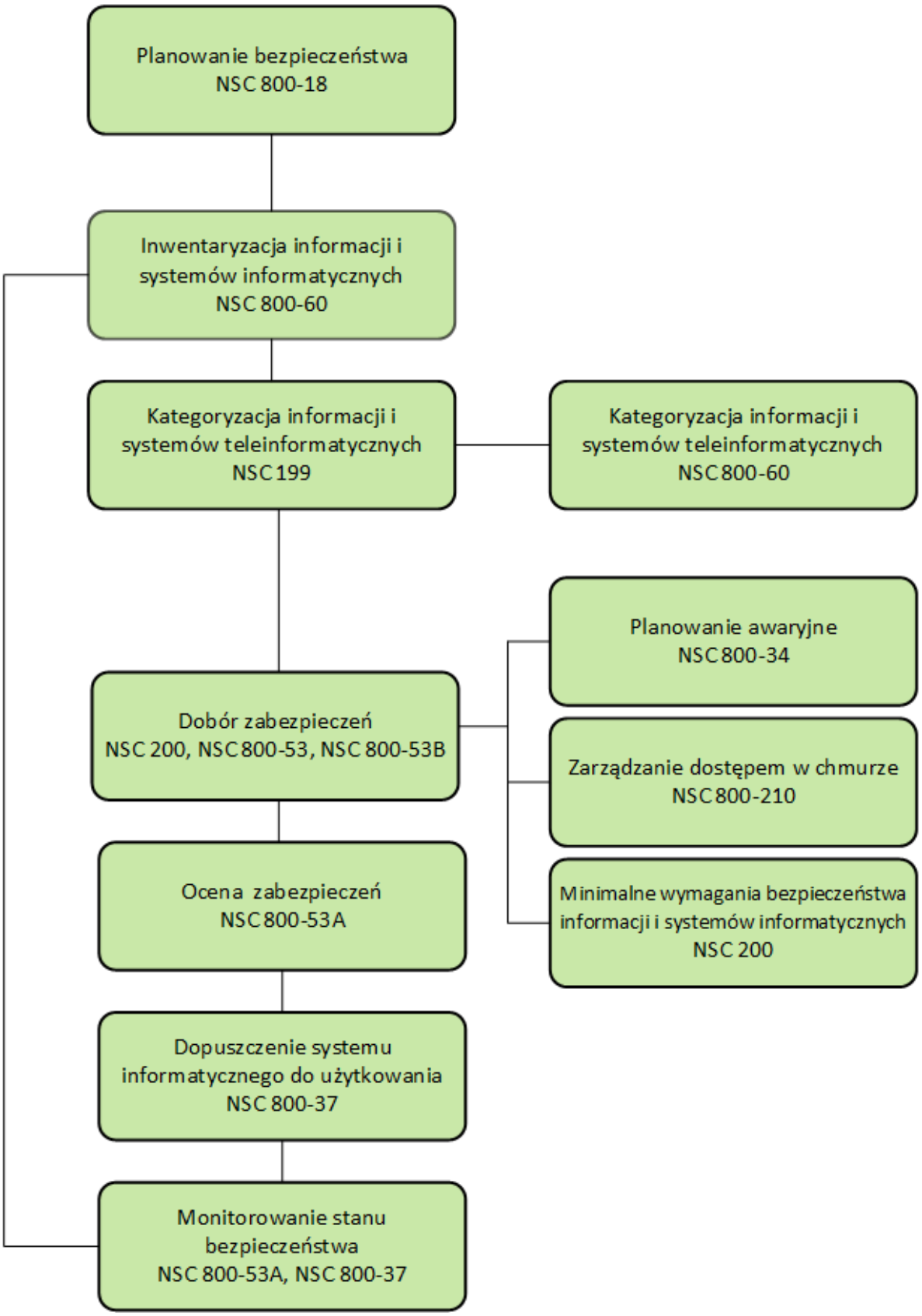
- NSC[2] 199, *Standardy kategoryzacji bezpieczeństwa* – na podstawie FIPS 199;
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych* – na podstawie FIPS 200;
- NSC 500-92, *Architektura referencyjna chmury obliczeniowej – rekomendacje* – na podstawie NIST SP 500-292;

[1] Wymienione są podstawowe dokumenty. Każdy z nich może się odwoływać w rozdziale *Referencje* do szeregu powiązanych publikacji, które składają się na całościowy proces osiągania cyberbezpieczeństwa.

[2] NSC – Narodowy Standard Cyberbezpieczeństwa.

- NSC 800-18, *Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych 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 informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* – na podstawie NIST SP 800-37;
- NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53;
- NSC 800-53A, *Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny* – na podstawie NIST SP 800-53A;
- NSC 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53B;
- NSC 800-60, *Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego* – 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.

Korzystając z tych publikacji można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę. Cykl zarządzania bezpieczeństwem bazujący na publikacjach NIST wykorzystuje następujące dokumenty:


Planowanie bezpieczeństwa
NSC 800-18
Inwentaryzacja informacji i systemów informatycznych
NSC 800-60
Kategoryzacja informacji i systemów teleinformatycznych
NSC 199
Kategoryzacja informacji i systemów teleinformatycznych
NSC 800-60
Dobór zabezpieczeń
NSC 200, NSC 800-53, NSC 800-53B
Planowanie awaryjne
NSC 800-34
Zarządzanie dostępem w chmurze
NSC 800-210
Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych
NSC 200
Ocena zabezpieczeń
NSC 800-53A
Dopuszczenie systemu informatycznego do użytkowania
NSC 800-37
Monitorowanie stanu bezpieczeństwa
NSC 800-53A, NSC 800-37

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował wiele standardów i wytycznych w celu zapewnienia wspólnego podejścia do problematyki bezpieczeństwa informacji i systemów teleinformatycznych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji, bezpieczeństwa systemów teleinformatycznych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością operacji organizacyjnych i majątku, osób fizycznych, innych organizacji 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, a także dzięki jednolitemu podejściu, ułatwia wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznymi i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi które zostały opracowane przez inne organizacje (np. ISO), 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 dozwolone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejście do zagadnień związanych z bezpieczeństwem informacji, systemów teleinformatycznych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST jako godne zaufania i rekomendują stosowanie ich przez polskie podmioty w 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. Identyfikacja taka nie ma na celu nakłaniania do nich lub ich poparcia, nie ma też na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w tym obszarze.

W niniejszym Narodowym Standardzie Cyberbezpieczeństwa (NSC) mogą znajdować się odniesienia do innych publikacji opracowywanych obecnie przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa zgodnie z przypisanymi mu obowiązkami ustawowymi. Informacje zawarte w tej publikacji, 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, obowiązują aktualne wymagania, wytyczne i procedury, jeśli takie istnieją. W celach planistycznych i wprowadzania zmian, organizacje będą mogły uważnie śledzić rozwój tych nowych publikacji opracowywanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Niniejsza publikacja, ***Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji SP 800-37, Rev. 2.

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.***

Występujące w publikacji odwołania do materiałów wyszczególnianych w nawiasach kwadratowych [ ] odnoszą się do polskojęzycznych standardów NSC (np. [NSC 800-30]) oraz ogólnodostępnych dokumentów anglojęzycznych (np. [SP 800-160], [*Ramy Cyberbezpieczeństwa:* ID.AM-6; ID.GV-2], [ISO 15288], [NIST CSF]). Dokumenty te stanowią uzupełnienie i rozszerzenie wiedzy na temat szerokorozumianego cyberbezpieczeństwa.

SPIS TREŚCI

ROZDZIAŁ 1 WPROWADZENIE

POTRZEBA ZARZĄDZANIA RYZYKIEM

Powodzenie misji i funkcji biznesowych organizacji, która zależy od systemów informatycznych[3] wspomagających realizację ich misji i działalności zależy od ochrony poufności, integralności, dostępność informacji przetwarzanych przez te systemy oraz ochrony danych osobowych. Zagrożenia dla systemów informatycznych obejmują awarie sprzętu, zakłócenia środowiskowe, błędy ludzkie lub maszynowe oraz celowe ataki, które są często wyrafinowane, zdeterminowane, dobrze zorganizowane i dobrze finansowane. W przypadku powodzenia, ataki na systemy informatyczne mogą spowodować poważne lub katastrofalne szkody w działalności organizacji[4] i majątku osób fizycznych, jednostek organizacyjnych i Państwa.[5] Dlatego konieczne jest, aby organizacje zachowały czujność i aby kadra kierownicza wyższego szczebla, liderzy i menedżerowie w całej organizacji rozumieli swoje obowiązki i byli odpowiedzialni za ochronę aktywów organizacji i zarządzanie ryzykiem.[6]

Oprócz odpowiedzialności za ochronę aktywów organizacji przed zagrożeniami występującymi we współczesnym środowisku, organizacje mają obowiązek rozważenia

[3] System informatyczny / teleinformatyczny to dyskretny zestaw zasobów informatycznych zorganizowanych w celu gromadzenia, przetwarzania, konserwacji, użytkowania, udostępniania, rozpowszechniania lub dysponowania informacjami. Termin system informatyczny obejmuje na przykład systemy komputerowe ogólnego przeznaczenia, przemysłowe/ procesowe systemy sterowania, systemy cyberfizyczne, systemy broni, superkomputery, systemy dowodzenia, kontroli i łączności, urządzenia takie jak smartfony i tablety, systemy kontroli środowiska, urządzenia/czujniki wbudowane oraz systemy kopiowania (utrwalania na papierze).

[4] Działania organizacyjne obejmują misję, funkcje, wizerunek i reputację.

[5] Niekorzystne skutki obejmują, na przykład, naruszenie zasad ochrony (kompromitacje) w zakresie systemów obsługujących aplikacje i infrastruktury krytycznej lub mających nadrzędne znaczenie dla ciągłości działania Państwa.

[6] Ryzyko jest miarą stopnia, w jakim jednostka jest zagrożona przez potencjalne okoliczności lub zdarzenia. Ryzyko jest również funkcją negatywnych skutków, które powstają w przypadku wystąpienia danej okoliczności lub zdarzenia, oraz prawdopodobieństwa ich wystąpienia. Rodzaje ryzyka obejmują: ryzyko programowe; ryzyko zgodności/ryzyko regulacyjne; ryzyko finansowe; ryzyko prawne; ryzyko misji/przedsiębiorstwa; ryzyko polityczne; ryzyko związane z bezpieczeństwem i ochroną prywatności (w tym ryzyko związane z łańcuchem dostaw); ryzyko projektu; ryzyko utraty reputacji; ryzyko związane ze zdrowiem; ryzyko planowania strategicznego.

i zarządzania ryzykiem odnoszącym się do osób fizycznych w przypadku, gdy systemy informatyczne przetwarzają dane osobowe (*ang. personal identification information - PII*).[7] Programy bezpieczeństwa informacji i ochrony danych osobowych (prywatności) wdrażane przez organizacje mają uzupełniające się cele w odniesieniu do zarządzania poufnością, integralnością i dostępnością PII. Podczas, gdy wiele zagrożeń dla bezpieczeństwa danych osobowych wynika z nieautoryzowanych działań, które prowadzą do utraty poufności, integralności lub dostępności PII, inne zagrożenia dla prywatności wynikają z autoryzowanych działań obejmujących tworzenie, gromadzenie, wykorzystywanie, przetwarzanie, przechowywanie, obsługę, rozpowszechnianie, ujawnianie lub usuwanie PII, które umożliwiają organizacji realizację jej misji lub celów biznesowych. Na przykład, organizacje mogą nie dostarczyć odpowiedniego powiadomienia o przetwarzaniu informacji z zakresu PII, pozbawiając daną osobę wiedzy o takim przetwarzaniu, lub też może ona zostać wprowadzona w zakłopotanie lub napiętnowana przez autoryzowane ujawnienie informacji z zakresu PII. Podczas gdy zarządzanie ryzykiem utraty prywatności wymaga ścisłej koordynacji między bezpieczeństwem informacji, a programami ochrony prywatności ze względu na komplementarny charakter celów tych programów w zakresie poufności, integralności i dostępności PII, ryzyko utraty prywatności budzi również wyraźne obawy, które wymagają specjalistycznej wiedzy i podejścia. Dlatego też niezwykle istotne jest, aby organizacje również tworzyły i utrzymywały stosowne programy ochrony prywatności w celu zapewnienia zgodności z obowiązującymi wymogami w zakresie ochrony prywatności i zarządzania ryzykiem dla osób fizycznych związanym z przetwarzaniem PII.

Coraz bardziej niepokojące dla organizacji jest również ryzyko związane z łańcuchem dostaw, stanowiące część zagrożeń dla bezpieczeństwa i prywatności. Ze względu na rosnącą

[7] PII to "informację, która może być wykorzystana do rozróżniania lub identyfikowania tożsamości osoby fizycznej, samodzielnie lub w połączeniu z innymi informacjami, które są powiązane lub możliwe do powiązania z konkretną osobą fizyczną". Organizacje mogą również zdecydować się na rozważenie ryzyka dla osób fizycznych, które może wynikać z interakcji z systemami informatycznymi, w przypadku, gdy przetwarzanie PII może mieć mniejszy wpływ niż wpływ, jaki system wywiera na zachowanie lub działalność osób fizycznych. Takie skutki stanowiłyby ryzyko dla indywidualnej autonomii, a organizacje mogą być zmuszone do podjęcia kroków w celu zarządzania tymi zagrożeniami, oprócz zagrożenia bezpieczeństwa informacji i prywatności.

zależność od zewnętrznych dostawców oraz na zastosowanie gotowych komercyjnych produktów, systemów i usług, rosną ataki lub zakłócenia w łańcuchu dostaw, które mają wpływ na systemy organizacji. Takie ataki mogą być trudne do wykrycia lub zarządzania i mogą mieć poważne lub katastrofalne skutki dla systemów organizacji. Zarządzanie ryzykiem w łańcuchu dostaw (*ang. supply chain risk management – SCRM*) pokrywa się i współgra z zarządzaniem ryzykiem w zakresie bezpieczeństwa i ochrony prywatności. Niniejsza publikacja integruje praktyki zarządzania ryzykiem w zakresie bezpieczeństwa i ochrony prywatności związane z ryzykiem w łańcuchu dostaw (SCRM) do ram zarządzania ryzykiem (*ang. Risk Management Framework – RMF*), aby pomóc w promowaniu kompleksowego podejścia do zarządzania ryzykiem w zakresie bezpieczeństwa i prywatności. Podczas gdy publikacja koncentruje się głównie na zarządzaniu ryzykiem związanym z bezpieczeństwem informacji i ochroną prywatności, koncepcje SCRM, które wspierają zarządzanie ryzykiem związanym z bezpieczeństwem i prywatnością, są wyszczególnione w kilku obszarach, aby podkreślić i wyjaśnić, w jaki sposób można się nimi posługiwać przy wykorzystaniu RMF.

1.1. TŁO

Niniejsza publikacja jest wprowadzeniem niniejszego opracowania do stosowania w podmiotach realizujących zadania publiczne. Na zasadach dobrowolności przedstawione w tym opracowaniu wytyczne mogą być stosowane w innych jednostkach organizacyjnych.

RMF kładzie nacisk na zarządzanie ryzykiem poprzez promowanie rozwoju zdolności w zakresie bezpieczeństwa i ochrony prywatności w systemach informatycznych w całym cyklu życia systemu (ang. *system development life cycle – SDLC*)[8] poprzez utrzymywanie na bieżąco świadomości sytuacyjnej w zakresie bezpieczeństwa i ochrony prywatności tych systemów dzięki ciągłym procesom monitorowania oraz poprzez dostarczanie informacji liderom wyższego szczebla i kadrze kierowniczej w celu ułatwienia podejmowania decyzji

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

dotyczących akceptacji ryzyka dla operacji organizacyjnych i aktywów, osób fizycznych, innych organizacji i państwa, wynikającego z użytkowania i funkcjonowania ich systemów.

RMF:

- Zapewnia powtarzalny proces mający na celu promowanie ochrony informacji i systemów informatycznych współmiernej do ryzyka;
- Kładzie nacisk na niezbędne przygotowanie całej organizacji do zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością;
- Ułatwia kategoryzację informacji i systemów, wybór, wdrażanie, ocenę i monitorowanie zabezpieczeń oraz autoryzację systemów informatycznych oraz zabezpieczeń wspólnych;[9]
- Promuje wykorzystanie automatyzacji do zarządzania ryzykiem w czasie zbliżonym do rzeczywistego oraz bieżącej autoryzacji systemu i zabezpieczeń poprzez wdrożenie procesów ciągłego monitorowania;
- Zachęca do stosowania prawidłowych i wymiernych mierników, aby dostarczyć liderom i menedżerom wyższego szczebla informacji niezbędnych do podejmowania opłacalnych, opartych na ryzyku decyzji dotyczących systemów informatycznych wspierających ich misje i funkcje biznesowe;
- Ułatwia integrację wymagań[10] i zabezpieczeń w zakresie bezpieczeństwa i ochrony prywatności z architekturą korporacyjną, SDLC, procesami akwizycji i procesami inżynierii systemów;
- Łączy procesy zarządzania ryzykiem na poziomie organizacji i misji/procesów biznesowych z procesami zarządzania ryzykiem na poziomie systemu informatycznego za pośrednictwem SAORM lub RM; oraz

[9] W rozdziale 3 opisano siedem kroków i związane z nimi zadania w ramach RMF.
[10] W sekcji 2.6 opisano związek między wymogami i zabezpieczeniami w odniesieniu do realizacji RMF.

- Ustanawia odpowiedzialność i rozliczalność za wdrożenie zabezpieczeń w ramach systemów informatycznych, w tym za zabezpieczenia dziedziczone przez te systemy.

RMF zapewnia dynamiczne i elastyczne podejście do efektywnego zarządzania ryzykiem w zakresie bezpieczeństwa i ochrony prywatności w różnych środowiskach, w których występują złożone i wyrafinowane zagrożenia, zmieniające się misje i funkcje biznesowe oraz zmieniające się słabości systemowe i organizacyjne. Ramy te są neutralne pod względem politycznym i technologicznym, co ułatwia bieżące aktualizacje zasobów informatycznych oraz działania w zakresie modernizacji systemów informatycznych, wspierając i pomagając w zapewnieniu świadczenia podstawowych misji i usług w takich okresach przejściowych.

1.2. CEL I ZASTOSOWANIE

Niniejsza publikacja opisuje RMF i zawiera wytyczne dotyczące zarządzania ryzykiem w zakresie bezpieczeństwa i prywatności oraz stosowania RMF w systemach informatycznych i organizacjach. Wytyczne te zostały opracowane w celu:

- Zapewnienia, że zarządzanie ryzykiem związanym z bezpieczeństwem i prywatnością systemu jest zgodne z misją i celami biznesowymi organizacji oraz strategią zarządzania ryzykiem ustaloną przez kierownictwo wyższego szczebla za pośrednictwem SAORM lub RM;
- Osiągnięcia ochrony prywatności osób fizycznych oraz ochrony bezpieczeństwa informacji i systemów informatycznych poprzez wdrożenie odpowiednich strategii reagowania na ryzyko;
- Wspierania spójnych, świadomych i bieżących decyzji dotyczących zezwoleń,[11] relacji z partnerami oraz przejrzystości i identyfikowalności informacji dotyczących bezpieczeństwa i prywatności;

[11] [SP 800-137] zawiera wytyczne dotyczące stałego monitorowania bezpieczeństwa informacji, wspomagające bieżące autoryzację. Przyszłe publikacje będą dotyczyły stałego monitorowania prywatności.

- Ułatwienia integracji wymagań i zabezpieczeń w zakresie bezpieczeństwa i prywatności z architekturą korporacyjną, procesami SDLC, procesami akwizycji i procesami inżynierii systemów;[12] oraz
- Ułatwienia wdrożenia ochrony infrastruktury krytycznej.

Niniejsza publikacja ma na celu pomóc organizacjom[13] w zarządzaniu ryzykiem związanym z bezpieczeństwem i ochroną prywatności oraz w spełnieniu wymogów przepisów ustawowych, wykonawczych i polityki.

Zakres niniejszej publikacji odnosi się do systemów informatycznych podmiotów realizujących zadania publiczne, które gromadzą, przetwarzają, przechowują, wykorzystują, dzielą się, rozpowszechniają lub dysponują informacjami, niezależnie od tego, czy są to informacje w formie cyfrowej, czy innej niż cyfrowa. Zasoby informacyjne obejmują informacje i związane z nimi zasoby, takie jak personel, sprzęt, fundusze i technologie informatyczne.

1.3. ODBIORCY DOCELOWI

Niniejsza publikacja służy osobom związanym z projektowaniem, opracowywaniem, wdrażaniem, oceną, eksploatacją, utrzymaniem i dysponowaniem systemami informatycznymi, w tym osobom:

- Realizującym misję lub obowiązki w zakresie własności organizacji lub obowiązki powiernicze (np. kierownicy jednostek organizacyjnych);
- Odpowiedzialnym za system informatyczny, bezpieczeństwo informacji lub zarządzanie prywatnością, nadzór lub obowiązki w zakresie zarządzania (np. senior

[12] [SP 800-160] zawiera wytyczne dotyczące inżynierii bezpieczeństwa systemów oraz budowania wiarygodnych, bezpiecznych systemów.

[13] Terminu "organizacja" używa się w niniejszej publikacji do określenia podmiotu o dowolnej wielkości, złożoności lub umiejscowieniu w strukturze organizacyjnej (np. Urząd, agencja, lub, w stosownych przypadkach, któregokolwiek z jego elementów operacyjnych).

leaders[14], *risk executives (RE)*[15], *authorizing official (AO)*[16], *chief information officer* (CIO)[17], *senior agency information security officer (SAISO)*[18], *senior agency official for privacy (SAOP)*[19];

- Odpowiedzialnym za przeprowadzanie ocen bezpieczeństwa lub prywatności oraz za monitorowanie systemów informatycznych, np. inspektorzy kontroli, audytorzy i właściciele systemów;
- Mającym obowiązki związane z wdrażaniem zasad bezpieczeństwa lub ochrony prywatności oraz obowiązki operacyjne, na przykład właściciele systemów, dostawcy zabezpieczeń wspólnych, właściciele/zainteresowani informacjami, właściciele misji lub firm, architekci ds. bezpieczeństwa lub ochrony prywatności oraz Inżynierowie bezpieczeństwa systemów lub ochrony prywatności;
- Odpowiedzialnym za rozwój systemów informatycznych i zaopatrzenie (np. kierownicy programów, personel ds. zamówień, twórcy produktów i systemów, integratorzy systemów i architekci korporacyjni); oraz
- Odpowiedzialnym za logistykę lub dyspozycję (np. kierownicy programów, personel ds. zamówień, integratorzy systemów i zarządcy nieruchomości).

Wyczerpujący wykaz i opis ról i obowiązków związanych z RMF znajduje się w Załączniku D.

[14] Kierownicy wyższego szczebla
[15] Osoba (lub grupa osób, kierowana przez wyższego rangą pracownika w jednostce organizacyjnej) odpowiedzialna za zarządzanie ryzykiem.
[16] Osoba lub komórka organizacyjna dokonująca autoryzacji polegającej na dopuszczeniu systemu informatycznego do eksploatacji w jednostce organizacyjnej, w tym za dopuszczenie do stosowania zabezpieczeń wspólnych dla wielu systemów.
[17] Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za technologie informacyjne, zwykle członek kierownictwa jednostki organizacyjnej.
[18] Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za bezpieczeństwo informacji. Inaczej: chief information security officer (CISO); lub senior information security officer (SISO) – w zależności od kultury organizacyjnej danej jednostki organizacyjnej.
[19] Osoba w jednostce organizacyjnej odpowiedzialna za prywatność i ochronę danych osobowych.

1.4. ORGANIZACJA NINIEJSZEJ PUBLIKACJI

Pozostała część tej publikacji jest zorganizowana w następujący sposób:

- W rozdziale drugim opisano koncepcje związane z zarządzaniem ryzykiem związanym z bezpieczeństwem i prywatnością systemu informatycznego. Obejmują one: organizacyjny obraz zarządzania ryzykiem; etapy RMF i strukturę zadań; związek między bezpieczeństwem informacji i programami ochrony prywatności oraz sposób, w jaki programy te są traktowane w RMF; zasoby informacyjne, jako elementy systemu; granice autoryzacji; bezpieczeństwo i podejście wobec prywatności; oraz kwestie bezpieczeństwa i ochrony prywatności związane z zarządzaniem ryzykiem w łańcuchu dostaw.
- W rozdziale trzecim opisano zadania wymagane do wdrożenia etapów w RMF, w tym: przygotowanie na poziomie organizacji i systemu informatycznego; kategoryzację informacji i systemów informatycznych; wybór zabezpieczeń, dopasowanie i wdrożenie; ocenę skuteczności zabezpieczeń; system informatyczny i zabezpieczenia wspólne; bieżące monitorowanie zabezpieczeń; oraz utrzymywanie świadomości w zakresie bezpieczeństwa i ochrony prywatności systemów informatycznych w organizacji.
- Załączniki pomocnicze zawierają dodatkowe informacje i wskazówki dotyczące stosowania RMF, w tym:
  - Referencje;
  - Słownik terminów;
  - Akronimy;
  - Role i obowiązki;
  - Podsumowanie zadań RMF;
  - Autoryzacja systemu i zabezpieczeń wspólnych;
  - Rozważania dotyczące zakresu autoryzacji;
  - Rozważania dotyczące autoryzacji cyklu życia systemu.

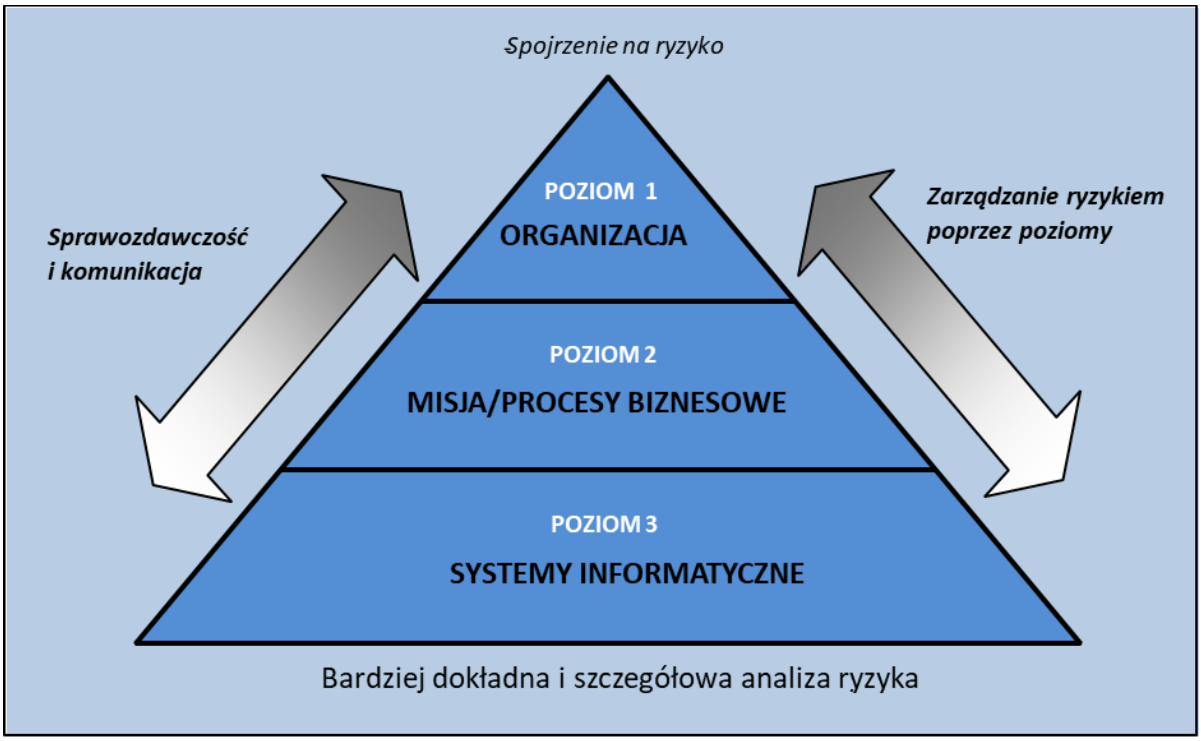
ROZDZIAŁ 2 PODSTAWY

JAK ZARZĄDZAĆ RYZYKIEM ZWIĄZANYM Z BEZPIECZEŃSTWEM I PRYWATNOŚCIĄ W ORGANIZACJACH?

W niniejszym rozdziale opisano podstawowe pojęcia związane z zarządzaniem bezpieczeństwem systemów informatycznych i ryzykiem związanym z ochroną prywatności w organizacjach. Pojęcia te obejmują etapy RMF i strukturę zadań, bezpieczeństwo informacji i programy ochrony prywatności w RMF, system informatyczny, komponenty systemu i sposób ustalania granic autoryzacji; bezpieczeństwo i status prywatności, oraz praktyki zarządzania ryzykiem w zakresie bezpieczeństwa i ochrony prywatności związane z łańcuchem dostaw.

2.1. ZARZĄDZANIE RYZYKIEM W SKALI ORGANIZACJI

Zarządzanie ryzykiem związanym z bezpieczeństwem i prywatnością systemów informatycznych jest złożonym przedsięwzięciem, które wymaga zaangażowania całej organizacji - od liderów wyższego szczebla, dostarczających strategiczną wizję oraz cele i zadania najwyższego szczebla dla organizacji, poprzez liderów średniego szczebla planujących, realizujących i zarządzających projektami, po osoby opracowujące, wdrażające, obsługujące i utrzymujące systemy wspierające misję i funkcje biznesowe organizacji. Zarządzanie ryzykiem to holistyczne działanie, które ma wpływ na każdy aspekt organizacji, w tym na misję i planowanie biznesowe, architekturę korporacyjną, procesy SDLC oraz działania z zakresu inżynierii systemów, które są integralną częścią procesów cyklu życia systemu. Rysunek 1 ilustruje wielopoziomowe podejście do zarządzania ryzykiem opisane w [SP 800-39], które odnosi się do ryzyka bezpieczeństwa i prywatności na poziomie *organizacji*, *misji/procesów biznesowych* oraz *systemu informatycznego*. Komunikacja i raportowanie to dwukierunkowy przepływ informacji pomiędzy trzema poziomami w celu zapewnienia, że ryzyko jest uwzględniane w całej organizacji.



Rysunek 1. Podejście do zarządzania ryzykiem w organizacji

Działania prowadzone na poziomach 1 i 2 mają kluczowe znaczenie dla przygotowania organizacji do realizacji RMF. Przygotowanie takie obejmuje szeroki zakres działań, które wykraczają poza zwykłe zarządzanie ryzykiem w zakresie bezpieczeństwa i ochrony prywatności związanych z obsługą lub korzystaniem z określonych systemów i obejmuje działania niezbędne do właściwego zarządzania ryzykiem w zakresie bezpieczeństwa i ochrony prywatności w całej organizacji. Decyzje o sposobie zarządzania ryzykiem na poziomie systemu nie mogą być podejmowane w oderwaniu od poziomu 1 i 2. Takie decyzje są ściśle związane z:

- Misją lub celami biznesowymi organizacji;
- Inicjatywami modernizacyjnymi w zakresie systemów, komponentów i usług;

- Architekturą korporacyjną i potrzebami zarządzania mającymi na celu zmniejszanie złożoności systemów[20] poprzez ich konsolidację, optymalizację i standaryzację;[21]
- Alokacją zasobów w celu zapewnienia, że organizacja może prowadzić swoją misję i działalność biznesową efektywnie, sprawnie i w sposób efektywny kosztowo.

Przygotowanie organizacji do realizacji RMF powinno obejmować:

- Przydzielenie ról i obowiązków w procesach zarządzania ryzykiem organizacyjnym;
- Ustalenie strategii zarządzania ryzykiem i organizacyjnej tolerancji na ryzyko;
- Identyfikację misji, funkcji biznesowych i procesów biznesowych systemów informatycznych mających za zadanie je wspierać;
- Identyfikację kluczowych interesariuszy (wewnętrznych i zewnętrznych w stosunku do organizacji), wykazują zainteresowanie systemem informatycznym;
- Identyfikację i priorytetyzację aktywów (w tym aktywów informacyjnych);
- Zrozumienie zagrożeń dla systemów informatycznych i organizacji;
- Zrozumienie potencjalnego niekorzystnego wpływu na osoby;
- Przeprowadzanie szacowania ryzyka na poziomie organizacji i systemu;
- Określanie i ustalanie priorytetów w zakresie wymogów bezpieczeństwa i ochrony prywatności;[22]

[20] Zarządzanie złożonością systemów poprzez konsolidację, optymalizację i standaryzację zmniejsza powierzchnię ataku i wpływ technologii możliwy do wykorzystania przez przeciwników.
[21] Architektura korporacyjna definiuje misję, informacje i technologie niezbędne do jej realizacji oraz procesy przejściowe do wdrażania nowych technologii w odpowiedzi na zmieniające się potrzeby misji. Obejmuje ona również architekturę bazową, architekturę docelową oraz plan sekwencyjny.
[22] Wymagania dotyczące bezpieczeństwa i ochrony prywatności można uzyskać z wielu źródeł (np. Z ustaw, rozporządzeń, dyrektyw, regulacji, polityki, standardów i misji/biznesu/wymagań operacyjnych).

- Ustalenie granic autoryzacji dla systemów informatycznych i zabezpieczeń wspólnych;[23]
- Zdefiniowanie systemów informatycznych pod kątem architektury korporacyjnej;
- Opracowanie architektury bezpieczeństwa i ochrony prywatności, które obejmują zabezpieczenia odpowiednie dla dziedziczenia przez systemy informatyczne;
- Określanie, uzgodnienie i wyeliminowanie sprzecznych wymogów w zakresie bezpieczeństwa i ochrony prywatności;
- Przypisywanie wymagań dotyczących bezpieczeństwa i ochrony prywatności do systemów informatycznych, komponentów systemu i organizacji.

W przeciwieństwie do działań na poziomie 1 i 2, które przygotowują organizację do realizacji RMF, poziom 3 odnosi się do ryzyka z perspektywy *systemu informatycznego* i jest oparty na decyzjach dotyczących ryzyka na poziomie organizacji oraz na poziomie procesu misyjnego / biznesowego. Decyzje dotyczące ryzyka na Poziomie 1 i 2 mogą mieć wpływ na wybór i wdrażanie zabezpieczeń na danym poziomie systemu. Zabezpieczenia są wyznaczane przez organizację, jako zabezpieczenia specyficzne dla systemu, hybrydowe lub wspólne (dziedziczone), zgodnie z architekturą korporacyjną, architekturą bezpieczeństwa lub ochrony prywatności oraz wszelkimi dostosowanymi poziomami zabezpieczeń podstawowych lub nakładkami, które zostały opracowane przez organizację.[24]

Organizacje ustalają *identyfikowalność* zabezpieczeń zgodnie z wymogami bezpieczeństwa i ochrony prywatności, które zabezpieczenia te mają spełniać. Ustanowienie takiej identyfikowalności zapewnia spełnienie wszystkich wymogów podczas projektowania, opracowywania, wdrażania, eksploatacji, konserwacji i dysponowania systemem. Każdy

[23] Granice uprawnień określają zakres uprawnień dla systemów informatycznych i zabezpieczeń wspólnych (tj. Elementy systemu określające system lub zestaw wspólnych zabezpieczeń dostępnych w procesie dziedziczenia).

[24] Zabezpieczenia mogą być przydzielane na wszystkich trzech poziomach w hierarchii zarządzania ryzykiem. Na przykład, zabezpieczenia wspólne mogą być przydzielane na poziomie organizacji, misji/procesu biznesowego lub systemu informatycznego.

poziom hierarchii zarządzania ryzykiem jest beneficjentem udanej realizacji RMF, co wzmacnia iteracyjny charakter procesu zarządzania ryzykiem, w ramach którego zagrożenia dla bezpieczeństwa i ochrony prywatności są określane, oceniane, uwzględniane i monitorowane na różnych szczeblach organizacyjnych.

Bez odpowiedniego przygotowania do zarządzania ryzykiem na poziomie organizacyjnym, działania z zakresu bezpieczeństwa i ochrony prywatności mogą stać się zbyt kosztowne, wymagać zbyt wielu wykwalifikowanych specjalistów ds. bezpieczeństwa i ochrony prywatności oraz tworzyć nieskuteczne rozwiązania. Na przykład, organizacje, które nie wdrożą efektywnej architektury korporacyjnej, będą miały trudności z konsolidacją, optymalizacją i standaryzacją swojej infrastruktury informatycznej. Dodatkowo, nietrafne decyzje architektoniczne i projektowe mogą niekorzystnie wpłynąć na zdolność organizacji do wdrażania efektywnych rozwiązań z zakresu bezpieczeństwa i ochrony prywatności. Brak odpowiedniego przygotowania ze strony organizacji może skutkować niepotrzebną redundancją, a także nieefektywnymi, kosztownymi i wrażliwymi systemami, usługami i aplikacjami.

2.2. ETAPY I STRUKTURA RAM ZARZĄDZANIA RYZYKIEM

RMF składa się z siedmiu etapów; etapu przygotowawczego, który ma zapewnić gotowość organizacji do realizacji procesu, oraz sześciu etapów głównych. Wszystkie siedem kroków ma zasadnicze znaczenie dla pomyślnej realizacji RMF. Rysunek 2 ilustruje etapy realizacji Ram Zarządzania Ryzykiem (RMF).

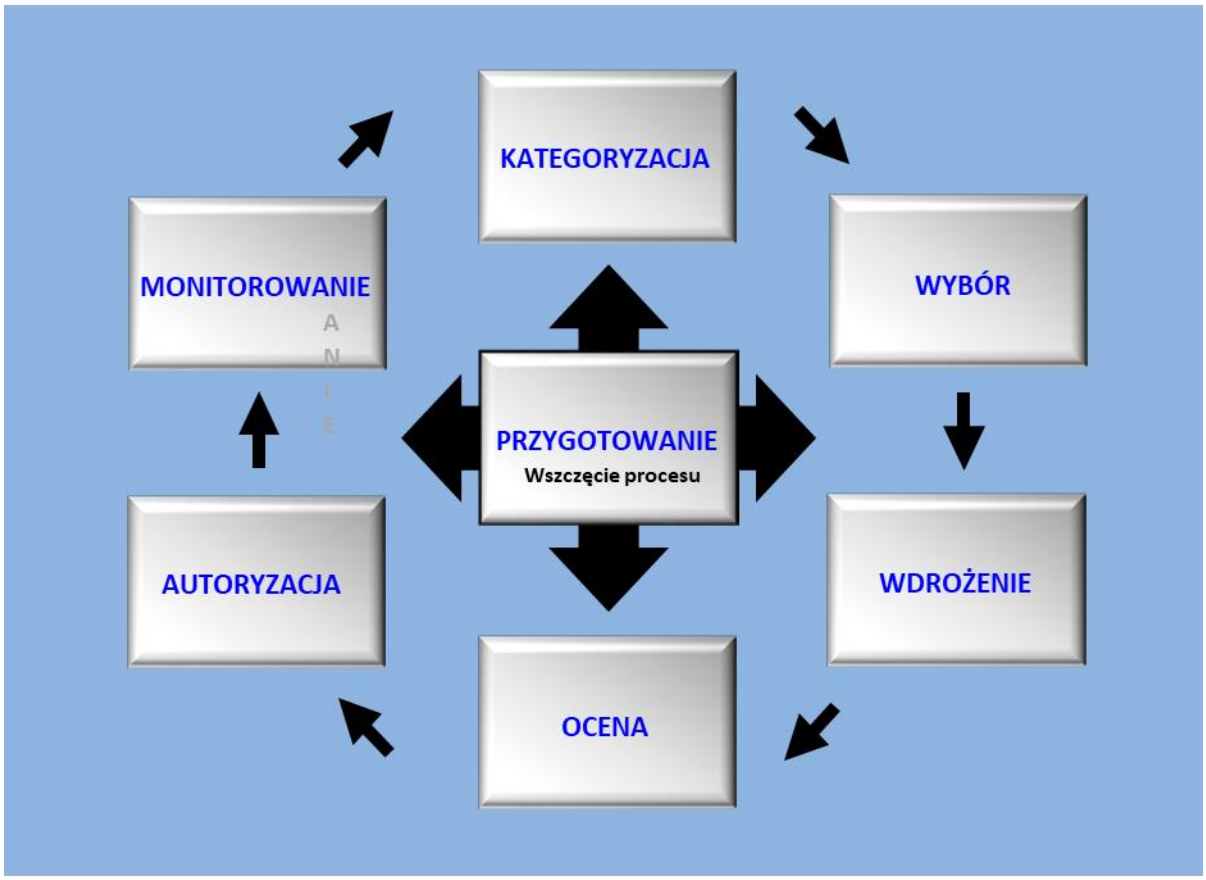
Są to następujące etapy:

- **Przygotowanie** do realizacji RMF z perspektywy organizacyjnej i systemowej poprzez ustalenie kontekstu i priorytetów zarządzania ryzykiem w zakresie bezpieczeństwa i ochrony prywatności.

- **Kategoryzacja** systemu i informacji przetwarzanych, przechowywanych i przekazywanych przez system w oparciu o analizę wpływu strat.[25]
- **Wybór** wstępny zestawu środków bezpieczeństwa systemu i dostosowanie zabezpieczeń do potrzeb, celem zmniejszenia ryzyka, na podstawie oceny, do dopuszczalnego poziomu ryzyka.
- **Wdrożenie** zabezpieczeń i opisanie, w jaki sposób są one stosowane w systemie i środowisku jego działania.
- **Ocena** zabezpieczeń w celu ustalenia, czy są one wprowadzane prawidłowo, działają zgodnie z założeniami i przynoszą pożądane rezultaty w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatności.
- **Autoryzacja** użytkowania systemu lub zabezpieczeń wspólnych (autoryzacja) w oparciu o stwierdzenie, że ryzyko dla operacji organizacyjnych i aktywów, osób, innych organizacji i państwa jest dopuszczalne.
- **Monitorowanie** na bieżąco systemu i związanych z nim zabezpieczeń, w tym ocena skuteczności zabezpieczeń, dokumentowanie zmian w systemie i środowisku działania, przeprowadzanie ocen ryzyka i analiz wpływu oraz zgłaszanie statusu bezpieczeństwa i ochrony prywatności systemu.

[25] Wpływ strat jest jednym z czterech czynników ryzyka branych pod uwagę podczas szacowania ryzyka - pozostałe trzy czynniki to zagrożenia, podatności i prawdopodobieństwo ich wystąpienia [NSC 800-30]. Organizacje wykorzystują wyniki szacowania ryzyka przy kategoryzacji informacji i systemów. W przypadku krajowych systemów bezpieczeństwa ważne może być uwzględnienie w ramach kategoryzacji konkretnych kwestii mających wpływ na czynniki ryzyka, takich jak: czy system przetwarza, przechowuje lub przekazuje informacje klasyfikowane lub wywiadowcze; czy system będzie miał bezpośredni lub pośredni dostęp do niego personelu spoza kraju; oraz czy informacje przetwarzane, przechowywane lub przekazywane przez system będą się pokrywać z dziedzinami bezpieczeństwa. [CNSSI 1253] dostarcza dodatkowych informacji na temat kategoryzacji krajowych systemów bezpieczeństwa. W przypadku polskich przepisów w pewnym zakresie zastosowanie ma Załącznik nr 2 do uchwały nr 97 Rady Ministrów z dnia 11 września 2019 r. W sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa".

RMF działają na wszystkich szczeblach hierarchii zarządzania ryzykiem przedstawionej na rysunku 1. Rozdział trzeci zawiera szczegółowy opis każdego z zadań niezbędnych do realizacji poszczególnych etapów w ramach RMF.



Rysunek 2. Ramy Zarządzania Ryzykiem - RMF

Pomimo, ze etapy RMF opisane powyżej i w rozdziale trzecim są wymienione w porządku sekwencyjnym, etapy następujące po etapie *Przygotowanie* mogą być realizowane w porządku niesekwencyjnym. Po wykonaniu zadań w ramach etapu *Przygotowania*, organizacje realizujące RMF po raz pierwszy dla systemu lub zestawu zabezpieczeń wspólnych, zazwyczaj wykonują pozostałe kroki w porządku sekwencyjnym. Jednakże w procesie zarządzania ryzykiem może istnieć wiele punktów, w których istnieje potrzeba odejścia od porządku sekwencyjnego ze względu na rodzaj systemu, decyzje dotyczące ryzyka podejmowane przez kierownictwo wyższego szczebla lub też dopuszczenie

powtarzających się cykli w ramach zadania lub powrót do zrealizowanego zadania (np. podczas rozwoju stosującego metodyką projektowania zwinnego - *ang. agile development*). W momencie, gdy organizacja znajduje się na etapie *Monitorowania*, zdarzenia mogą dyktować niesekwencyjne wykonanie kroków. Na przykład, zmiany w zakresie ryzyka lub funkcjonalności systemu mogą wymagać ponownego wykonania jednego lub więcej kroków w RMF w celu uwzględnienia zmiany.

ELASTYCZNOŚĆ WE WDRAŻANIU RAM ZARZĄDZANIA RYZYKIEM

Od organizacji oczekuje się realizacji wszystkich kroków i zadań w RMF (oprócz zadań oznaczonych jako opcjonalne). Organizacje mają jednak znaczną elastyczność w sposobie realizacji każdego z etapów i zadań w ramach RMF, o ile spełniają wszystkie obowiązujące wymogi i skutecznie zarządzają ryzykiem związanym z bezpieczeństwem i prywatnością. Celem jest umożliwienie organizacjom wdrażania RMF w najbardziej efektywny, skuteczny i opłacalny sposób, aby wspierać misję i potrzeby biznesowe zgodnie z taktyką, która promuje skuteczne bezpieczeństwo i prywatność. Elastyczna realizacja może obejmować realizację zadań w innej (potencjalnie niesekwencyjnej) kolejności, kładąc nacisk na określone zadania w stosunku do innych lub łącząc niektóre zadania w stosownych przypadkach. Może ona również obejmować wykorzystanie ram cyberbezpieczeństwa w celu usprawnienia realizacji zadań związanych z RMF.

Elastyczność wdrożenia może być również zastosowana do *wyboru* zabezpieczeń i ich *dopasowania* (*ang. tailoring*) do potrzeb bezpieczeństwa i ochrony prywatności organizacji lub przeprowadzania ocen zabezpieczeń w trakcie całego procesu.

Na przykład, wybór, dopasowanie, implementacja i ocena zabezpieczeń mogą być dokonywane przyrostowo w trakcie cyklu życia systemu (SDLC). Wdrożenie "*dopasowania zabezpieczeń*" pomaga zapewnić, że rozwiązania w zakresie bezpieczeństwa i ochrony prywatności są dostosowane do konkretnych misji, funkcji biznesowych, ryzyka i środowisk operacyjnych organizacji. Ostatecznie, elastyczność nieodłącznie związana z realizacją RMF promuje skuteczne bezpieczeństwo i prywatność, które pomagają chronić systemy, od których zależą organizacje w zakresie misji i sukcesu biznesowego oraz osoby, których informacje są przetwarzane przez te systemy.

Uwaga: Ponieważ RMF jest procesem SDLC, który kładzie nacisk na bieżącą autoryzację, organizacje mają możliwość elastycznego określania, który krok RMF należy wprowadzić (lub ponownie wprowadzić) w oparciu o ocenę ryzyka i zadania opisane w kroku *Poziom*

Przygotowania Systemu. Wyznaczenie odpowiedniego etapu RMF wymaga oceny aktualnego stanu systemu, przeglądu działań, które zostały już zakończone w odniesieniu do systemu, identyfikacji proponowanego etapu i zadania wejścia do RMF, analizy luk w celu zapewnienia, że ryzyko jest akceptowalne oraz dokumentowania decyzji, powiadamiania zainteresowanych stron oraz udzielania zezwolenia przez właściwego decydenta.

Chociaż podejście do zarządzania ryzykiem przedstawione na Rysunku 1 jest przedstawione jako hierarchiczne, dynamika projektu i organizacji jest zazwyczaj bardziej złożona. Podejście do zarządzania ryzykiem wybrane przez organizację może się różnić w zależności od sytuacji, od postępowania hierarchicznego z góry do dołu do zdecentralizowanego konsensusu między partnerami. Jednakże, we wszystkich przypadkach, organizacje stosują spójne podejście, które jest stosowane w procesach zarządzania ryzykiem w całej organizacji, od poziomu *organizacji* do poziomu *systemu informatycznego.* Personel organizacji identyfikuje i zabezpiecza zasoby niezbędne do realizacji zadań z zakresu zarządzania ryzykiem, opisanych w niniejszej publikacji oraz zapewniają, że zasoby te są dostępne dla odpowiedniego personelu. Alokacja zasobów obejmuje środki na realizację zadań związanych z zarządzaniem ryzykiem oraz przydzielenie wykwalifikowanego personelu, który jest potrzebny do realizacji tych zadań.

Każdy etap RMF posiada deklarację celu, określony zestaw wyników oraz zestaw zadań, które są realizowane w celu osiągnięcia tych wyników. Wyniki mogą być osiągane na różnych poziomach zarządzania ryzykiem - niektóre z nich są uniwersalne dla całej organizacji, podczas gdy inne są zorientowane na system lub misję/jednostkę biznesową. Rysunek 3 przedstawia przykład oświadczenia o celu i rezultatach dla etapu Przygotowanie - Poziom Organizacji.

3.1 Przygotowanie

Cel

Celem etapu ***Przygotowania*** jest przeprowadzenie niezbędnych działań na poziomie organizacji, misji i procesu biznesowego oraz systemu informatycznego organizacji, aby pomóc w przygotowaniu organizacji do zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością z wykorzystaniem *Ram Zarządzania Ryzykiem*.

PRZYGOTOWYWANIE ZADAŃ - POZIOM ORGANIZACYJNY

Tabela 1 zawiera podsumowanie zadań i oczekiwanych wyników dla RMF na poziomie *organizacji* w kroku *Przygotowanie*. Ponadto przedstawiono również obowiązujące konstrukcje ram cyberbezpieczeństwa.

TABELA 1: PRZYGOTOWANIE ZADAŃ I REZULTATÓW - POZIOM ORGANIZACYJNY

Zadania	REZULTATY
ZADANIE P-1 FUNKCJE ZARZĄDZANIA RYZYKIEM	Identyfikowanie osób fizycznych i przypisywanie im kluczowych ról w realizacji Ram Zarządzania Ryzykiem. [*Ramy Cyberbezpieczeństwa:* ID.AM-6; ID.GV-2][26]
ZADANIE P-2 STRATEGIA ZARZĄDZANIA RYZYKIEM	Ustanawianie strategii zarządzania ryzykiem organizacji, która obejmuje określenie i wyrażenie tolerancji dla ryzyka organizacyjnego. [*Ramy Cyberbezpieczeństwa:* ID.RM; ID.SC]
ZADANIE P-3	Ocena zakończonego lub aktualizacja istniejącego szacowania ryzyka w skali całej organizacji.

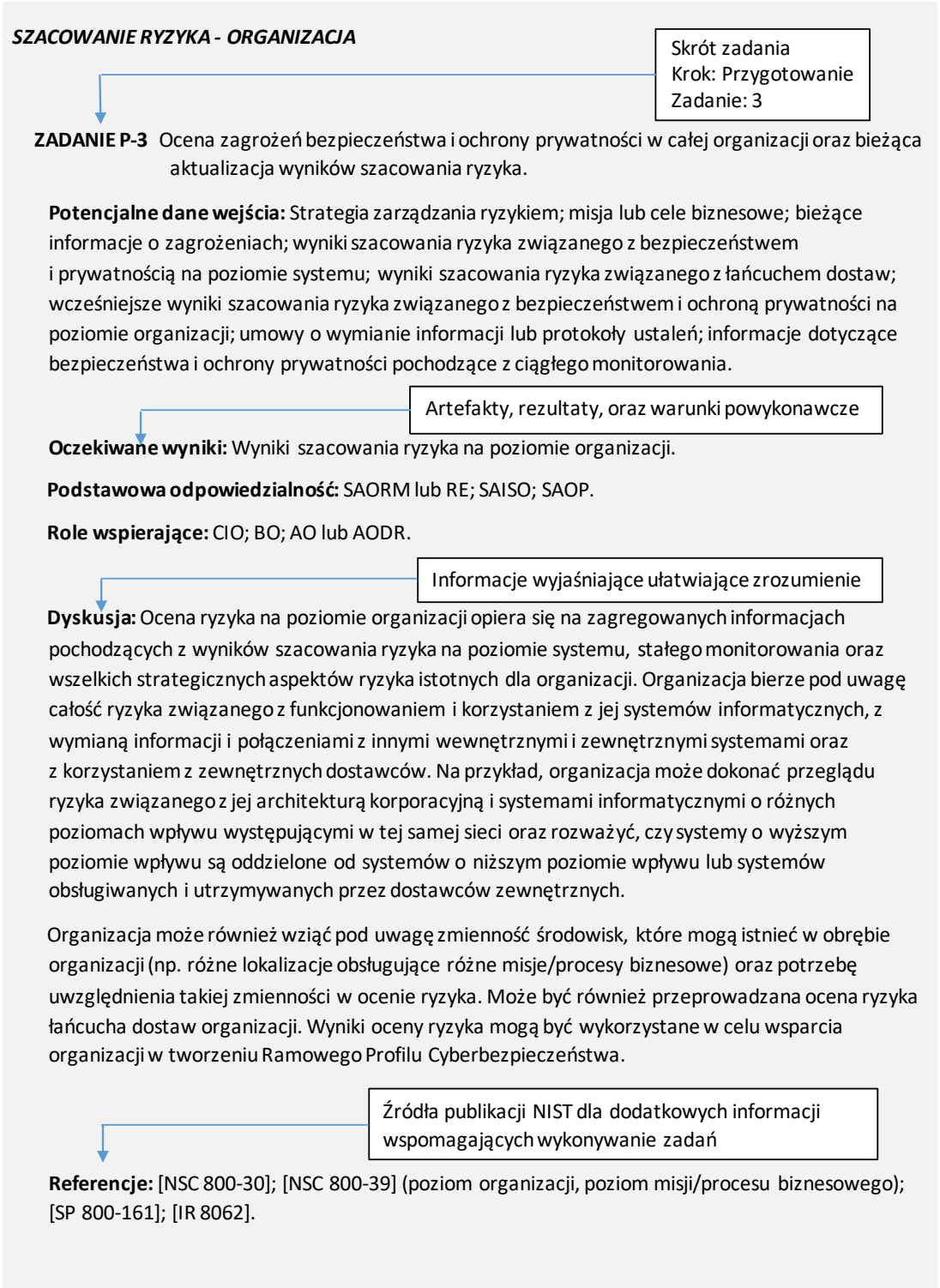
SZACOWANIE RYZYKA – ORGANIZACJA	[*Ramy Cyberbezpieczeństwa:* ID.RA; ID.SC-2]
ZADANIE P-4 **DOSTOSOWYWANIE PRZEZ ORGANIZACJĘ PODSTAWOWYCH MECHANIZMÓW ZABEZPIECZEŃ I PROFILI RAM CYBERBEZPIECZEŃSTWA (OPCJONALNIE)**	Ustanawia się i udostępnia dostosowane do potrzeb organizacji podstawowe mechanizmy zabezpieczeń i/lub profile ram cyberbezpieczeństwa. [*Ramy Cyberbezpieczeństwa:* profil]
ZADANIE P-5 IDENTYFIKACJA ZABEZPIECZEŃ WSPÓLNYCH	Zabezpieczenia wspólne, które są dostępne do dziedziczenia przez systemy organizacji, są identyfikowane, dokumentowane i publikowane.
ZADANIE P-6 PRIORYTETYZACJA NA POZIOMIE WPŁYWU (NIEOBOWIĄZKOWO)	Przeprowadza się priorytetyzację systemów organizacji o tym samym poziomie wpływu. [*Ramy Cyberbezpieczeństwa:* ID.AM-5]
ZADANIE P-7 STRATEGIA CIĄGŁEGO MONITOROWANIA – ORGANIZACJA	Opracowywana i wdrażana jest organizacyjna strategia monitorowania skuteczności zabezpieczeń. [*Ramy Cyberbezpieczeństwa:* DE.CM; ID.SC-4]

Rysunek 3. Struktura zadaniowa Ram Zarządzania Ryzykiem

[26] Niektóre z wskazanych dokumentów nie mają odzwierciedlenia w polskim systemie prawa, niemniej przytoczone zostały w celu naświetlenia kontekstu, w jakim podejmowane są powyższe działania. Dotyczy to całego dokumentu.

Każde zadanie zawiera P*otencjalne dane wejściowe* niezbędne do jego wykonania oraz oczekiwany zestaw *Dane wyjściowe* generowanych w wyniku realizacji zadania.[27] Dodatkowo, w każdym zadaniu opisywana jest *Podstawowa odpowiedzialność* oraz *Role i obowiązki* zarządzania ryzykiem związane z danym zadaniem oraz fazę SDLC, w której następuje wykonanie zadania.[28] Sekcja *Dyskusja* dostarcza informacji związanych z zadaniem, aby ułatwić zrozumienie i promować skuteczne wykonanie zadania. Na końcu, uzupełniając opis zadania RMF, znajduje się lista *Referencje*, które mają dostarczyć organizacjom dodatkowych informacji dla każdego zadania. W stosownych przypadkach referencje określają również zadania związane z inżynierią bezpieczeństwa systemów, które są powiązane z zadaniem w ramach RMF.[29] Rysunek 4 ilustruje strukturę zadaniową typowego zadania związanego z RMF.

[27] Potencjalne dane wejściowe dla danego zadania nie zawsze mogą wywodzić się z oczekiwanych wyników poprzedniego zadania. Może to wynikać z faktu, że kroki RMF nie zawsze są wykonywane w kolejności sekwencyjnej, co powoduje przerwanie sekwencyjnych zależności.
[28] Załącznik D zawiera opis każdej z ról i obowiązków określonych w zadaniach.
[29] [NSC 800-160] opisuje procesy inżynierii bezpieczeństwa systemów oparte na cyklu życia systemu.



Rysunek 4. Ramowa struktura zadań zarządzania ryzykiem

2.3. BEZPIECZEŃSTWO INFORMACJI I OCHRONA PRYWATNOŚCI W RAMACH ZARZĄDZANIA RYZYKIEM

Realizacja Ram Zarządzania Ryzykiem wymaga ścisłej współpracy pomiędzy programami bezpieczeństwa informacji, a programami ochrony prywatności. Pomimo, że programy bezpieczeństwa informacji i programy ochrony prywatności mają różne cele, to jednak cele te nakładają się na siebie i uzupełniają. Programy bezpieczeństwa informacji są odpowiedzialne za ochronę informacji i systemów informatycznych przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem (tj. nieautoryzowaną działalnością lub zachowaniem systemu) w celu zapewnienia poufności, integralności i dostępności. Programy ochrony prywatności są odpowiedzialne za zapewnienie zgodności z obowiązującymi wymogami w zakresie ochrony danych osobowych i prywatności oraz za zarządzanie ryzykiem odnoszącym się do osób związanych z tworzeniem, gromadzeniem, wykorzystywaniem, przetwarzaniem, rozpowszechnianiem, przechowywaniem, obsługą, ujawnianiem lub usuwaniem (zwanymi łącznie *przetwarzaniem*) danych osobowych (PII).[29] Przygotowując się do realizacji etapów RMF, organizacje rozważają, w jaki sposób najlepiej promować i instytucjonalizować współpracę między obydwoma programami, aby zapewnić osiągnięcie celów obu obszarów na każdym etapie procesu.

Jeżeli system informatyczny przetwarza informacje o charakterze danych osobowych, program bezpieczeństwa informacji i program ochrony prywatności organizacji ponoszą wspólną odpowiedzialność za zarządzanie ryzykiem dla osób, które może wynikać z nieautoryzowanej działalności lub zachowania systemu. Wymaga to współpracy tych

[29] Programy ochrony prywatności mogą również uwzględniać ryzyko odnoszące się do osób fizycznych, które może wynikać z ich interakcji z systemami informatycznymi, w przypadku, gdy przetwarzanie danych dotyczących PII może mieć mniejszy wpływ niż oddziaływanie, jakie system ma na zachowanie lub działalność osób fizycznych. Takie skutki stanowiłyby ryzyko dla indywidualnej autonomii, a organizacje mogą być zmuszone do podjęcia kroków mających na celu zarządzania tymi zagrożeniami, dodatkowo w stosunku do zagrożeń dla bezpieczeństwa informacji i prywatności.

dwóch programów przy wyborze, wdrażaniu, ocenie i monitorowaniu zabezpieczeń. [30] O ile jednak programy bezpieczeństwa informacji i programy ochrony prywatności mają uzupełniające się cele w odniesieniu do zarządzania poufnością, integralnością i dostępnością PII, o tyle ochrona prywatności osób fizycznych nie może być osiągana wyłącznie poprzez zabezpieczenie PII.

Nie wszystkie zagrożenia dla prywatności wynikają z nieautoryzowanego działania lub zachowania systemu, takiego jak nieautoryzowany dostęp lub ujawnienie danych osobowych. Niektóre zagrożenia dla prywatności mogą wynikać z autoryzowanej działalności, która wykracza poza zakres bezpieczeństwa informacji. Na przykład programy ochrony prywatności są odpowiedzialne za zarządzanie ryzykiem dla osób fizycznych, które może wynikać z tworzenia, gromadzenia, wykorzystywania i utrzymywania PII, nieodpowiedniej jakości lub integralności PII oraz braku odpowiedniego powiadomienia, przejrzystości lub współdziałania. W związku z tym, aby pomóc w zapewnieniu zgodności z obowiązującymi wymaganiami w zakresie ochrony prywatności i zarządzaniu ryzykiem dla prywatności wynikającym z autoryzowanego i nieautoryzowanego przetwarzania informacji z zakresu PII, programy ochrony prywatności organizacji również wybierają, wdrażają, oceniają i monitorują zabezpieczenia w tym obszarze.[31]

[30] Na przykład w Zadaniu C-2 etapu Kategoryzacja, programy ochrony prywatności i bezpieczeństwa współpracują ze sobą, biorąc pod uwagę potencjalnie negatywny wpływ na działalność organizacji, aktywa organizacyjne, osoby fizyczne, inne organizacje i Państwo wynikający z utraty poufności, integralności lub dostępności danych osobowych, w celu określenia poziomu wpływu na system informatyczny. Wynikający z tego poziom wpływu decyduje o wyborze minimalnego zestawu zabezpieczeń w Zadaniu S-1 kroku - Wybór.

[31] Może zaistnieć potrzeba wybrania różnych zabezpieczeń w celu ograniczenia ryzyka dla prywatności związanego z autoryzowanym przetwarzaniem danych osobowych wpływających na identyfikację. Na przykład, może istnieć ryzyko, że osoby fizyczne będą ośmieszone lub napiętnowane w przypadku ujawnienia pewnych informacji na ich temat. Chociaż szyfrowanie mogłoby zapobiec nieautoryzowanemu ujawnieniu danych osobowych, nie uwzględnia ono jednak żadnego ryzyka dla prywatności związanego z ujawnieniem informacji stronom upoważnionym do ich odszyfrowania i dostępu do nich. Aby ograniczyć to ryzyko, organizacje musiałyby ocenić ryzyko zezwolenia upoważnionym stronom na odszyfrowanie informacji i potencjalnie wybrać zabezpieczenia, które ograniczyłyby to ryzyko. W takim przypadku organizacja może wybrać mechanizmy zabezpieczeń, które umożliwią osobom fizycznym zrozumienie praktyk ujawniania informacji przez organizację i dokonanie wyboru w zakresie tego dostępu lub zastosowanie zróżnicowanych technik kryptograficznych zwiększających prywatność lub służących oddzieleniu informacji od osoby fizycznej.

Zabezpieczenie prywatności definiuje się jako zabezpieczenia administracyjne, techniczne lub fizyczne, stosowane w organizacji w celu zapewnienia zgodności z obowiązującymi wymogami w zakresie ochrony prywatności i zarządzania ryzykiem w zakresie ochrony prywatności. Zabezpieczenie prywatności różni się od *środków bezpieczeństwa*, które definiuje się jako zabezpieczenie lub środek zaradczy przewidziany dla systemu informatycznego lub organizacji w celu ochrony poufności, integralności i dostępności systemu i jego informacji. Ze względu na wspólną odpowiedzialność, jaką ponoszą programy bezpieczeństwa informacji i programy ochrony prywatności organizacji za zarządzanie ryzykiem dla osób fizycznych, wynikającym z nieautoryzowanej działalności lub zachowania systemu, zabezpieczenia, które osiągają zarówno cele bezpieczeństwa, jak i ochrony prywatności, są zarówno zabezpieczeniami prywatności, jak i bezpieczeństwa. Niniejsze wytyczne odnoszą się do takich zabezpieczeń, które umożliwiają osiągnięcie obu zestawów celów jako "zabezpieczenie". Gdy w niniejszych wytycznych używa się deskryptorów "prywatność" i "bezpieczeństwo" z terminem *zabezpieczenie*, odnosi się on do tych zabezpieczeń w okolicznościach, gdy są one wybierane, wdrażane i oceniane pod kątem poszczególnych celów.

Procesy zarządzania ryzykiem opisane w niniejszej publikacji mają zastosowanie również do programów bezpieczeństwa i ochrony prywatności. Jednak w niektórych obszarach ryzyka, którymi muszą zarządzać programy bezpieczeństwa i ochrony prywatności, nakładają się na siebie, a w innych nie. W związku z tym ważne jest, aby organizacje rozumiały wzajemne oddziaływanie między ochroną prywatności i bezpieczeństwem w celu promowania skutecznej współpracy między personelem (rolami) ds. ochrony prywatności i bezpieczeństwa na każdym szczeblu organizacji.

2.4. SYSTEM I ELEMENTY SYSTEMU

Ważne jest, aby opisać systemy informatyczne w kontekście procesu SDLC oraz sposób, w jaki zdolności w zakresie bezpieczeństwa i ochrony prywatności są wdrażane w ramach komponentów tych systemów. Dlatego też organizacje realizujące projekty związane z RMF

przyjmują szerokie spojrzenie na cykl życia opracowywanych systemów informatycznych, aby zapewnić związek kontekstowy i powiązanie z koncepcjami architektonicznymi i inżynieryjnymi, które umożliwiają zajęcie się zagrożeniami dla bezpieczeństwa i prywatności (w tym zagrożeniami dla łańcucha dostaw) w całym cyklu życia i na odpowiednim poziomie szczegółowości, co pomoże zapewnić osiągnięcie takich możliwości. [ISO 15288] zapewnia inżynierskie spojrzenie na system informatyczne i podmioty, z którymi system wchodzi w interakcję w swoim środowisku pracy.

[ISO 15288] definiuje *system informatyczny, jako* zbiór współdziałających elementów, które są zorganizowane w celu osiągnięcia jednego lub więcej określonych celów. Tak jak zasoby informacyjne składające się na system informatyczny obejmują informacje i inne zasoby (np. personel, sprzęt, fundusze i technologie informatyczne), tak komponenty systemu obejmują elementy technologii lub maszyn, elementy ludzkie oraz elementy fizyczne lub środowiskowe. Każdy z *elementów systemu*[32] w ramach systemu spełnia określone wymagania i może być wdrożony za pomocą sprzętu, oprogramowania lub oprogramowania sprzętowego (*ang. firmware*);[33] fizycznych struktur lub urządzeń lub ludzi, procesów, zasad i procedur. Poszczególne elementy systemu lub kombinacja elementów systemu mogą spełniać określone wymagania. Wzajemne połączenia pomiędzy komponentami systemu pozwalają tym elementom na interakcję niezbędną do wytworzenia zdolności określonej w wymaganiach systemowych. Wreszcie, każdy system działa w środowisku, które ma wpływ na system i jego działanie.

[32] Terminy element systemu i zasób informacyjny są stosowane zamiennie w niniejszej publikacji. Zasób informacyjny obejmuje informacje i związane z nimi zasoby, takie jak personel, sprzęt, fundusze i technologie informatyczne. Zgodnie z prawem, system składa się z dyskretnego zestawu zasobów informacyjnych.

[33] Termin komponent systemu odnosi się do elementu systemu, który jest wdrażany za pomocą sprzętu, oprogramowania lub oprogramowania sprzętowego.

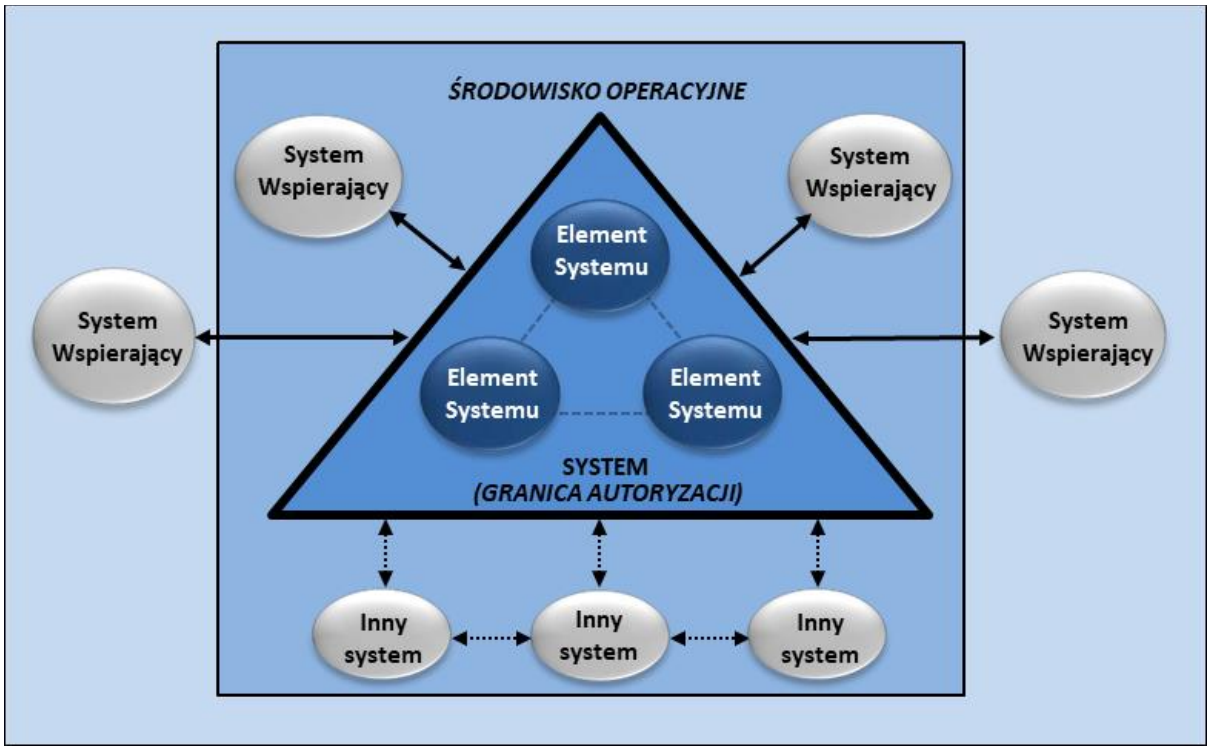
Granica autoryzacji określa system[34] na potrzeby realizacji RMF, w celu ułatwienia zarządzania ryzykiem i rozliczalności. System może być wspierany przez jeden lub więcej *systemów wspomagających*, które zapewniają wsparcie podczas cyklu życia systemu. Systemy wspomagające nie są zawarte w granicach autoryzacji systemu i niekoniecznie istnieją w środowisku, w którym ten system działa. System wspomagający może zapewniać zabezpieczenia wspólne (tj. dziedziczone) lub może obejmować dowolny rodzaj usługi lub funkcji wykorzystywanej przez system, takiej jak usługi identyfikacji i uwierzytelniania, usługi sieciowe lub funkcje monitorowania. Wreszcie, istnieją *inne systemy,* z którymi system wchodzi w interakcję w środowisku operacyjnym. Inne systemy również znajdują się poza granicami autoryzacji i mogą być beneficjentami usług świadczonych przez system lub mogą po prostu mieć pewną ogólną interakcję.[35]

Rysunek 5 ilustruje koncepcyjny obraz systemu oraz zależności pomiędzy systemem, elementami systemu, systemami wspomagającymi, innymi systemami i środowiskiem pracy.[36]

[34] Historycznie, stosowano zamiennie terminy granica autoryzacji oraz granica systemu. Ze względu na przejrzystość, dokładność i stosowanie znormalizowanej terminologii, termin "granica autoryzacji" jest obecnie używany wyłącznie w odniesieniu do zbioru elementów systemu, które mają być autoryzowane do eksploatacji lub dopuszczone do użytku przez osobę autoryzującą (tj. Zakresu autoryzacji). Granica autoryzacji może również odnosić się do zbioru elementów zabezpieczeń wspólnych, które mają być autoryzowane do celów dziedziczenia.

[35] Zarządzanie ryzykiem i odpowiedzialność za systemy wspomagające i inne systemy są uwzględnione w ramach ich odpowiednich granic autoryzacji.

[36] Terminy system, element systemu, system wspomagający, inne systemy i środowisko działania nie odnoszą się do konkretnych technologii informatycznych (IT) i technologii operacyjnych (OT).



Rysunek 5. Koncepcyjne spojrzenie na system

Niektóre elementy środowiska pracy mogą być włączone do zakresu autoryzacji (tj. określone, jako "objęte zakresem" autoryzacji), podczas gdy inne części mogą być z autoryzacji wyłączone. Na przykład, jeżeli obiekt (tj. środowisko pracy), które zapewnia ochronę elementów systemu, jest określony jako wchodzący w zakres autoryzacji systemu, zabezpieczenia ochrony fizycznej i środowiskowej (np. fizyczne kontrole dostępu w punktach wejścia, urządzenia obwodu zabezpieczeń) są zawarte w granicach autoryzacji i dlatego są uwzględnione w planie bezpieczeństwa systemu. Jeżeli obiekt zapewnia ochronę fizyczną i środowiskową, jako zabezpieczenia wspólne, które mają być dziedziczone przez system, środowisko działania jest poza zasięgiem systemu i nie jest uwzględnione w autoryzacji systemu.[37]

[37] Zabezpieczenia wspólne są określone w planach bezpieczeństwa i ochrony prywatności dla systemu, który je dziedziczy.

System może również komunikować się lub mieć inne interakcje z systemami wspomagającymi i innymi systemami, które są częścią rozszerzonego środowiska pracy, ale znajdują się poza zakresem autoryzacji systemu.[38] Organizacje określają, które części środowiska pracy znajdują się w granicach autoryzacji. Ustalenia te są zazwyczaj specyficzne dla danego systemu i wynikają z uwarunkowań.

2.5. GRANICE AUTORYZACJI

Granica autoryzacji określa zakres ochrony systemu informatycznego (tj. to, co organizacja zgadza się chronić w ramach swojego bezpośredniego zarządzania lub w zakresie swoich obowiązków). Granica autoryzacji[39] obejmuje osoby, procesy i technologie informatyczne (tj. elementy systemu), które są częścią każdego systemu wspierającego misje i funkcje biznesowe organizacji. Zbyt rozbudowane granice autoryzacji (tj. obejmujące zbyt wiele elementów lub komponentów systemu) sprawiają, że proces zarządzania ryzykiem jest niepotrzebnie skomplikowany. Z kolei zbyt ograniczone (tj. obejmujące zbyt małą liczbę elementów lub komponentów systemu) granice autoryzacji zwiększają liczbę systemów, które muszą być zarządzane oddzielnie, a tym samym mogą niepotrzebnie zawyżać koszty bezpieczeństwa i ochrony prywatności informacji ponoszone przez organizację.

Granica autoryzacji systemu jest ustalana na *poziomie zadania przygotowania systemu* RMF (*ang. Prepare Task – System)*, Zadanie P-11. Organizacje mają możliwość elastycznego określania, co stanowi granicę autoryzacji dla systemu. Zestaw elementów systemu zawarty w granicy autoryzacji definiuje system (czyli zakres uprawnień). Kiedy zestaw elementów systemu jest identyfikowany jako granica autoryzacji systemu, elementy te są na ogół objęte

[38] W przypadku połączeń i wymiany informacji pomiędzy systemem, a systemem wspomagającym lub innymi systemami znajdującymi się poza granicą autoryzacji, organizacje biorą pod uwagę ryzyko wynikające z takich połączeń i wymiany informacji.

[39] Systemy informatyczne są dyskretnymi zbiorami zasobów informacyjnych zorganizowanymi w celu przetwarzania, niezależnie od tego, czy informacje te prezentowane są w formie cyfrowej czy analogowej. Zasoby informacyjne obejmują informacje i związane z nimi zbiory, takie jak personel, sprzęt, fundusze i technologie informatyczne. Systemy informacyjne mogą, ale nie muszą zawierać sprzętu, aplikacji i oprogramowania układowego.

tym samym bezpośrednim zarządzaniem.[40] Inne względy dla określenia granicy autoryzacji obejmują identyfikację elementów systemu, które:

- Wspierają tą samą misję lub funkcję biznesowe;
- Charakteryzują się podobnymi właściwościami eksploatacyjnymi oraz wymogami bezpieczeństwa i ochrony prywatności;
- Przetwarzają, przechowują i przekazują podobne rodzaje informacji (np. sklasyfikowanych na tym samym poziomie wpływu);[41] lub
- Osadzone są w tym samym środowisku pracy (lub, w przypadku systemu rozproszonego, rozmieszczone w różnych miejscach o podobnym środowisku pracy).

Zakres granicy autoryzacji jest okresowo weryfikowany w ramach prowadzonego przez organizację procesu ciągłego monitorowania. Podczas, gdy powyższe rozważania mogą być przydatne dla organizacji w określaniu granic autoryzacji do celów zarządzania ryzykiem, rozważania te nie mają na celu ograniczenia elastyczności organizacji w ustanawianiu granic autoryzacji, które promują skuteczne bezpieczeństwo i prywatność z wykorzystaniem dostępnych zasobów organizacji i akceptowalnych dla organizacji kosztów. Załącznik G zawiera dodatkowe informacje i rozważania dotyczące określania granic autoryzacji, w tym granic dla złożonych systemów i aplikacji.

[40] W przypadku systemów informatycznych bezpośrednie zarządzanie zabezpieczeniami obejmuje organy budżetowe, programowe lub operacyjne oraz związaną z nią odpowiedzialność i rozliczalność. Bezpośrednie zarządzanie zabezpieczeniami nie musi oznaczać, że nie istnieje zarządzanie pośrednie.

[41] Jeśli system zawiera informacje o wielu poziomach wpływu, jest on klasyfikowany na najwyższym poziomie wpływu. Patrz [NSC 199] i [NSC 200].

SKUTECZNE GRANICE AUTORYZACJI

Ustalenie właściwych granic autoryzacji dla *systemów* i *zabezpieczeń wspólnych* jest jednym z najważniejszych działań w zakresie zarządzania ryzykiem prowadzonym przez organizację. Granica autoryzacji określa konkretny zakres odpowiedzialności osoby autoryzującej za ochronę zasobów informacyjnych i prywatności osób fizycznych - w tym za korzystanie z systemów, komponentów i usług zewnętrznych dostawców. Ustanowienie właściwych granic autoryzacji jest podstawą do zapewnienia powodzenia misji i sukcesu biznesowego organizacji.

2.6. WYMAGANIA I ZABEZPIECZENIA

Przed przystąpieniem do realizacji RMF ważne jest zrozumienie koncepcji wymagań w zakresie bezpieczeństwa i ochrony prywatności oraz związku między wymaganiami, a zabezpieczeniami. Termin *wymagania* może być stosowany w różnych kontekstach. W kontekście rządowej polityki bezpieczeństwa informacji i ochrony prywatności termin ten jest zwykle używany w odniesieniu do obowiązków w zakresie bezpieczeństwa informacji i ochrony prywatności nałożonych na organizacje przepisami prawa. Oprócz stosowania tego terminu w kontekście polityki rządowej, termin *wymagania* jest używany w niniejszych wytycznych w szerszym znaczeniu, jako wyraz zestawu potrzeb w zakresie ochrony interesariuszy dla danego systemu lub organizacji. Potrzeby w zakresie ochrony interesariuszy i odpowiadające im wymagania dotyczące bezpieczeństwa i ochrony prywatności mogą pochodzić z wielu źródeł (np. z przepisów prawa, rozporządzeń, dyrektyw, regulacji, polityki, standardów, misji i potrzeb biznesowych lub szacowania ryzyka). Termin *wymagania,* używany w niniejszych wytycznych, obejmuje zarówno wymagania prawne, jak i polityczne, a także stanowi wyraz szerszego zestawu potrzeb w zakresie ochrony interesariuszy, które mogą pochodzić z innych źródeł. Wszystkie te wymagania, gdy są stosowane w systemie, pomagają określić wymagane cechy systemu - obejmujące bezpieczeństwo, prywatność i zaufanie.

Organizacje mogą dokonać podziału wymagań dotyczących bezpieczeństwa i ochrony prywatności na bardziej szczegółowe kategorie w zależności od fazy SDLC i celu. Organizacje mogą używać terminu *wymagania dotyczące zdolności* do opisania zdolności, którą system lub organizacja musi zapewnić w celu zaspokojenia potrzeby ochrony interesariuszy. Ponadto, organizacje mogą odnosić się do wymagań systemowych, które dotyczą konkretnego sprzętu, oprogramowania i elementów firmware'u systemu, jako do *specyfikacji wymagań,* czyli do zdolności, które wdrażają całość lub część zabezpieczeń i które mogą być oceniane (tj. jako część procesów weryfikacji, poprawności, testowania i oceny). Wreszcie, organizacje mogą używać terminu *specyfikacja wymagań pracy* w odniesieniu do działań, które muszą być wykonywane operacyjnie lub podczas rozwoju systemu.

Zabezpieczenia mogą być postrzegane, jako środki bezpieczeństwa, właściwe dla osiągnięcia konkretnych celów organizacji w zakresie bezpieczeństwa i ochrony prywatności oraz odzwierciedlające potrzeby ochrony interesariuszy organizacji. Zabezpieczenia są wybierane i wdrażane przez organizację w celu spełnienia wymagań systemowych. Zabezpieczenia mogą obejmować aspekty techniczne, administracyjne i fizyczne. W niektórych przypadkach, wybór i wdrożenie zabezpieczeń może wymagać dodatkowej specyfikacji przez organizację w postaci *wymagań domyślnych* lub wartości parametrów zabezpieczeń. *Wymagania domyślne* i wartości parametrów zabezpieczeń mogą być niezbędne do zapewnienia odpowiedniego poziomu szczegółowości implementacji dla poszczególnych zabezpieczeń w ramach SDLC.

WYMAGANIA ZALEŻNE OD KONTEKSTU

Wymagania dotyczące bezpieczeństwa i ochrony prywatności oraz zagrożenia zidentyfikowane przez organizację prowadzą do konieczności późniejszego wprowadzenia zarówno wymagań dotyczących specyfikacji pracy, jak i deklaracji wymagań dotyczących pracy w zakresie środków bezpieczeństwa i ochrony prywatności w celu reagowania na ryzyko. Zabezpieczenia wybierane są przez organizację w kontekście inżynierii systemów. Jest to ważny aspekt sposobu, w jaki inżynierowie systemów opracowują, wyprowadzają i rozkładają wymagania w ramach procesu SDLC. W ten sposób organizacje zarządzają wymaganiami w zakresie bezpieczeństwa i ochrony prywatności na różnych poziomach szczegółowości i specyfiki w trakcie cyklu życia systemu. Zabezpieczenia odgrywają ważną rolę w cyklu życia poprzez zapewnienie wysokiego poziomu zdolności ochrony, który może być przez organizację udoskonalany i rozszerzany.

2.7. BEZPIECZEŃSTWO I OCHRONA DANYCH OSOBOWYCH I PRYWATNOŚCI

Celem RMF jest pomoc w zapewnieniu odpowiedniej ochrony systemów informatycznych, organizacji i osób fizycznych w całym SDLC oraz zapewnienie personelowi autoryzującemu informacji niezbędnych do podejmowania wiarygodnych, opartych na ryzyku decyzji dotyczących działania lub wykorzystania systemów lub zapewnienia zabezpieczeń wspólnych. Kluczowym aspektem podejmowania decyzji przez personel autoryzujący w oparciu o ryzyko, jest zrozumienie stanu bezpieczeństwa i prywatności systemów informatycznych oraz zabezpieczeń wspólnych, które są dostępne do dziedziczenia przez te systemy. Stan w zakresie bezpieczeństwa i ochrony prywatności reprezentuje status systemów informatycznych i zasobów informacyjnych (np. personelu, sprzętu, funduszy i technologii informatycznych) w ramach organizacji w oparciu o zaufane zasoby (np. ludzi, sprzęt, oprogramowanie, zasady, procedury) oraz możliwości zarządzania obroną organizacji w zakresie działania lub korzystania z systemów, zgodności z obowiązującymi wymogami

w zakresie ochrony prywatności i zarządzania ryzykiem związanym z ochroną prywatności oraz reagowania na zmiany sytuacji.

Bezpieczeństwo i prywatność systemów i organizacji jest określana na bieżąco poprzez ocenę i stałe monitorowanie zabezpieczeń specyficznych dla danego systemu, zabezpieczeń hybrydowych i zabezpieczeń wspólnych.[42] Ocena zabezpieczeń i działania monitorujące dostarczają dowodów na to, że zabezpieczenia wybrane przez organizację są realizowane prawidłowo, działają zgodnie z założeniami i spełniają wymagania bezpieczeństwa i ochrony prywatności w odpowiedzi na przepisy prawa, zasady, standardy lub misję i wymagania biznesowe. Personel autoryzujący korzysta z osiągniętego stanu bezpieczeństwa i prywatności w celu ustalenia, czy ryzyko dla operacji i aktywów organizacji, osób, innych organizacji lub Państwa jest dopuszczalne w oparciu o strategię zarządzania ryzykiem organizacji i jej tolerancję na ryzyko organizacyjne.[43]

2.8. ZARZĄDZANIE RYZYKIEM W ŁAŃCUCHU DOSTAW

Organizacje w celu realizacji misji i funkcji biznesowych w coraz większym stopniu polegają na produktach, systemach i usługach dostarczanych przez zewnętrznych dostawców. Organizacje są odpowiedzialne za ryzyko związane z korzystaniem z tych komponentów produktów, systemów i usług.[44] Relacje z zewnętrznymi dostawcami mogą być nawiązywane na różne sposoby, na przykład poprzez wspólne przedsięwzięcia, partnerstwa biznesowe, różnego rodzaju formalne umowy (np. umowy, porozumienia między urzędami, porozumienia branżowe, porozumienia licencyjne) lub umowy outsourcingowe.

Rosnące uzależnienie od produktów, systemów i usług dostawców zewnętrznych, wraz z charakterem relacji z tymi dostawcami, stanowią coraz większe ryzyko dla organizacji. Ryzyko może wzrosnąć na podstawie prawdopodobieństwa wystąpienia i niekorzystnego

[42] Monitorowanie zabezpieczeń jest częścią podejścia do zarządzania ryzykiem w całej organizacji, zdefiniowanego w [SP 800-39].
[43] Patrz: krok RMF Przygotowanie – Poziom organizacji, Zadanie P-2.
[44] Ryzyko związane z łańcuchem dostaw wymaga od organizacji rozważenia kwestii bezpieczeństwa łańcucha dostaw w odniesieniu do wszystkich działań związanych z planowaniem i zarządzaniem zasobami w ramach SDLC, tak, aby ryzyko było odpowiednio zarządzane.

wpływu zdarzeń zagrażających, takich jak wprowadzanie podróbek, nieautoryzowana produkcja, manipulowanie, kradzież, wprowadzanie złośliwego oprogramowania i sprzętu, a także słabe praktyki produkcyjne i rozwojowe w łańcuchu dostaw, w tym brak wbudowanych możliwości w zakresie bezpieczeństwa lub ochrony prywatności, co obliguje organizacje do lepszego zarządzania ryzykiem w jej środowisku.

Ryzyko związane z łańcuchem dostaw może mieć charakter endemiczny lub systemowy w ramach danego elementu systemu, systemu, organizacji, sektora lub kraju. Podczas gdy pojedyncze użycie elementu systemu lub usługi w ramach systemu może stanowić akceptowalne ryzyko dla organizacji, jego powszechne lub rozszerzone użycie w całym systemie, organizacji, sektorze lub kraju może podnieść ryzyko do niedopuszczalnego poziomu. Ryzyko to jest często związane z globalnym i rozproszonym charakterem łańcuchów dostaw produktów i usług oraz z mniejszą świadomością i zrozumieniem przez organizację sposobu, w jaki nabyta przez nie technologia jest rozwijana, integrowana i wdrażana. Obejmuje to procesy, procedury i praktyki stosowane w celu zapewnienia integralności, bezpieczeństwa, odporności, możliwości ochrony prywatności i jakości nabytych produktów, systemów i usług.

W celu przeciwdziałania ryzyku związanemu z łańcuchem dostaw, organizacje opracowują zasady *zarządzanie ryzykiem w łańcuchu dostaw* (*ang. supply chain risk management - SCRM),* która jest ważnym narzędziem służącym do kierowania działaniami związanymi z łańcuchem dostaw. Wytyczne i informacje zawarte w obowiązujących przepisach prawa, zasadach i regulacjach, wspierają zasady SCRM obowiązujące w organizacji (np. nabywanie i zaopatrzenie, bezpieczeństwo i prywatność informacji, logistykę, jakość i łańcuch dostaw). Polityka ta odnosi się do celów i założeń zawartych w planie strategicznym organizacji, jej misji i funkcji biznesowych, a także wymagań klientów wewnętrznych i zewnętrznych. Określa ona również w organizacji punkty integracji SCRM z zarządzaniem ryzykiem i procesami SDLC. Wreszcie, polityka SCRM definiuje role i obowiązki SCRM w organizacji, wszelkie zależności między tymi rolami oraz interakcję między nimi. Role SCRM określają obowiązki w zakresie zakupów, przeprowadzania szacowania ryzyka, gromadzenia informacji

o zagrożeniach w łańcuchu dostaw, identyfikacji i wdrażania środków zaradczych opartych na ryzyku oraz pełnienia funkcji monitorujących.

Przykładowo, możliwe jest wymaganie od zewnętrznych dostawców przetwarzających informacje organizacji lub działających w imieniu rządu, spełnienia tych samych wymogów bezpieczeństwa i prywatności, które obowiązują podmioty publiczne. Wymogi w zakresie bezpieczeństwa i ochrony prywatności dotyczące dostawców zewnętrznych, w tym zabezpieczeń systemów przetwarzania, przechowywania lub przekazywania informacji organizacji, są wyrażone w umowach lub innych formalnych porozumieniach. RMF może być skutecznie wykorzystywany do zarządzania ryzykiem związanym z łańcuchem dostaw.[45] Koncepcyjny pogląd na temat systemu przedstawiony na Rysunku 5 może ukierunkowywać i informować o działaniach w zakresie bezpieczeństwa, ochrony prywatności i zarządzania ryzykiem dla wszystkich elementów łańcucha dostaw. Każdy etap RMF może być realizowany przez zewnętrznych dostawców, z wyjątkiem etapu autoryzacji, tj. akceptacji ryzyka, za które odpowiedzialność ponosi kierownictwo wyższego szczebla. Decyzja o autoryzacji systemu jest bezpośrednio związana z zarządzaniem ryzykiem związanym z nabywaniem i wykorzystaniem produktów, systemów i usług dostarczanych przez dostawców zewnętrznych.[46] Wymagane jest również od organizacji opracowanie i wdrożenie planów SCRM.

Zarządzanie ryzykiem związanym z łańcuchem dostaw jest złożonym, wielopłaszczyznowym przedsięwzięciem wymagającym skoordynowanych wysiłków w całej organizacji - budowania relacji zaufania i komunikacji zarówno z interesariuszami wewnętrznymi, jak i zewnętrznymi. Działania SCRM obejmują identyfikację i ocenę zidentyfikowanego ryzyka, określenie

[45] Ryzyko związane z łańcuchem dostaw oznacza ryzyko, które wynika z utraty poufności, integralności lub dostępności informacji lub systemów informatycznych i odzwierciedla potencjalny niekorzystny wpływ na działalność organizacji (w tym misję, funkcje, wizerunek lub reputację), aktywa organizacyjne, osoby, inne organizacje i Państwo. W przypadku, gdy elementy systemu przetwarzają dane osobowe, praktyki SCRM odnoszą się zarówno do bezpieczeństwa informacji, jak i ryzyka związanego z prywatnością.

[46] Autoryzacja (tzn. Akceptacja ryzyka) organizacyjnych systemów informatycznych jest nieodłączną odpowiedzialnością organizacji. Jest to podstawowa koncepcja, która może być wykorzystywana przez kadrę kierowniczą wyższego szczebla w organizacjach na wszystkich poziomach łańcucha dostaw do zarządzania ryzykiem w zakresie bezpieczeństwa i prywatności.

odpowiednich działań łagodzących, opracowanie odpowiednich planów SCRM w celu udokumentowania wybranych działań łagodzących oraz monitorowanie wyników w odniesieniu do planów SCRM. Ponieważ łańcuchy dostaw różnią się w poszczególnych organizacjach i wewnątrz nich, plany SCRM są dostosowane do indywidualnych programów, uwarunkowań organizacyjnych i operacyjnych. Dostosowane do potrzeb plany stanowią podstawę do określenia, czy system jest "odpowiedni do celu", a zabezpieczenia są odpowiednio dostosowane. Dostosowane do potrzeb plany SCRM pomagają organizacjom skoncentrować swoje zasoby na najbardziej krytycznych misjach i funkcjach biznesowych w zidentyfikowane ryzyka.

Stwierdzenie, że ryzyko związane z nabyciem produktów, systemów lub usług od zewnętrznych dostawców jest dopuszczalne, zależy od poziomu zaufania[47], jaki organizacja może uzyskać od tych dostawców. Poziom zaufania opiera się na stopniu kontroli, jaki organizacja może wywierać na zewnętrznym dostawcy w odniesieniu do zabezpieczeń niezbędnych do ochrony produktu, systemu lub usługi oraz na dowodach przedstawionych przez dostawcę w odniesieniu do skuteczności tych zabezpieczeń.

Stopień kontroli ustalany jest na podstawie szczegółowych warunków umowy lub porozumienia o poziomie usług. Niektóre organizacje mają szeroką kontrolę za pośrednictwem narzędzi kontraktowych lub innych umów, które określają wymogi bezpieczeństwa i ochrony prywatności dla zewnętrznego dostawcy. Natomiast inne organizacje mają ograniczoną kontrolę, ponieważ kupują usługi lub produkty komercyjne dostępne na rynku „z półki". Poziom zaufania może być również oparty na wielu innych czynnikach, które przekonują organizację, że wymagane zabezpieczenia zostały wdrożone i że istnieje wiarygodne określenie skuteczności tych zabezpieczeń. Na przykład, autoryzowana zewnętrzna usługa w chmurze świadczona na rzecz organizacji poprzez

[47] Poziom poświadczenia zapewniany przez zewnętrznego dostawcę może być różny od tych, którzy zapewniają poświadczenia na wysokim poziomie (np. Partnerzy biznesowi we wspólnym przedsięwzięciu, który mają wspólny model biznesowy i cele) tj. Takich, którzy zapewniają mniejszą liczbę poświadczeń i reprezentują większe źródła ryzyka (np. Partnerzy biznesowi w jednym przedsięwzięciu, którzy są również konkurentami w innym sektorze rynku).

ugruntowaną relację w branży (*ang. line-of-business*) może zapewnić poziom zaufania do usługi, który mieści się w zakresie tolerancji ryzyka organizacji. Ostatecznie odpowiedzialność za reagowanie na ryzyka związane z wykorzystaniem produktów, systemów i usług dostarczanych przez dostawców zewnętrznych spoczywa na organizacji i personelu autoryzującym. Organizacje wymagają, aby przy rozwiązywaniu problemów związanych z bezpieczeństwem systemów lub zagrożeniami dla prywatności ustanowić odpowiedni *łańcuch zaufania* z zewnętrznymi dostawcami.

STRATEGIE I PLANY ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

Organizacje dysponują elastycznością w zakresie sposobu dokumentowania szczegółów strategii i planów SCRM. Szczegóły strategii SCRM dla Poziomów 1 i 2 (poziomy organizacji i misji/procesów biznesowych), mogą być udokumentowane w planie programu bezpieczeństwa informacji dla organizacji lub w oddzielnej strategii SCRM na poziomie organizacji i/lub misji/procesów biznesowych. Szczegóły planu SCRM dla Poziomu 3 (poziom systemu informatycznego) mogą być udokumentowane w planie bezpieczeństwa systemu informatycznego lub w oddzielnym planie SCRM na poziomie systemu.

ROZDZIAŁ 3 PROCES

REALIZACJA ZADAŃ RAMOWYCH W ZAKRESIE ZARZĄDZANIA RYZYKIEM

W niniejszym rozdziale opisano kroki i związane z nimi zadania, które składają się na ramy zarządzania ryzykiem RMF oraz wybrane osoby lub grupy (określone role organizacyjne), które realizują takie zadania.[48] Organizacje, gdy tylko jest to możliwe, dostosowują swoje role w zakresie zarządzania ryzykiem do uzupełniających się lub podobnych ról zdefiniowanych dla SDLC oraz zgodnych z misjami i funkcjami biznesowymi. Zadania związane z funduszami RMF są realizowane jednocześnie z procesami SDLC w organizacji lub jako ich część. W organizacji zadania związane z zarządzaniem ryzykiem w RMF są realizowane jednocześnie z procesami SDLC lub jako ich część. Ponadto, oczekiwane rezultaty wymagane przez RMF (np. plany bezpieczeństwa i plany ochrony prywatności, raporty z oceny, plany i etapy działań), mogą być rutynowo uzyskiwane z procesów SDLC istniejących w organizacji i nie muszą być opracowywane wyłącznie do celów wdrażania RMF.

DOPASOWANIE RMF DO SDLC

Najlepsze wdrożenie RMF to takie, które jest nie do odróżnienia od rutynowych procesów SDLC prowadzonych przez organizacje. Oznacza to, że zadania RMF są ściśle powiązane z bieżącymi działaniami w ramach procesów SDLC, zapewniając bezproblemową integrację bezpieczeństwa i ochrony prywatności w systemach organizacyjnych - oraz wykorzystując w maksymalnym stopniu artefakty generowane przez procesy SDLC do tworzenia niezbędnych dowodów w pakietach autoryzacyjnych, aby ułatwić podejmowanie przez liderów w organizacjach wiarygodnych, opartych na ryzyku decyzji.

[48] Załącznik D opisuje role i obowiązki kluczowych uczestników zaangażowanych w zarządzanie ryzykiem organizacyjnym i realizację RMF. Wiele ról związanych z zarządzaniem ryzykiem zdefiniowanych w niniejszej publikacji ma swoje odpowiedniki zdefiniowane w procesie SDLC.

Proces realizacji zadań RMF może się różnić w zależności od organizacji. Podczas, gdy zadania pojawiają się w kolejności sekwencyjnej, w procesie zarządzania ryzykiem może istnieć wiele punktów, które wymagają odstępstwa od kolejności sekwencyjnej, w tym konieczność powtarzania cykli pomiędzy początkową realizacją zadania, a ponownym jego wykonaniem. Na przykład, wyniki oceny zabezpieczeń mogą wyzwolić zestaw działań naprawczych podejmowanych przez właścicieli systemów i dostawców zabezpieczeń wspólnych, co z kolei może wymagać ponownej oceny wybranych zabezpieczeń. Monitorowanie zabezpieczeń może wygenerować cykl śledzenia zmian w systemie i środowisku jego działania, ocenę wpływu na bezpieczeństwo i prywatność informacji, ponowną ocenę zabezpieczeń, podejmowanie działań naprawczych oraz raportowanie stanu bezpieczeństwa i prywatności systemu i organizacji.

Może istnieć możliwość odejścia od sekwencyjnego charakteru zadań, gdy jest to bardziej efektywne, skuteczne lub opłacalne. Na przykład, podczas gdy zadania oceny zabezpieczeń są wymienione po zadaniach wdrażania zabezpieczeń, organizacje mogą rozpocząć ocenę zabezpieczeń zaraz po ich wdrożeniu, ale przed pełnym wdrożeniem wszystkich zabezpieczeń opisanych w planach bezpieczeństwa systemu i planach ochrony prywatności. Ocena zabezpieczeń zaraz po ich wdrożeniu może skutkować oceną tych zabezpieczeń w zakresie ochrony fizycznej i środowiskowej w obiekcie przed oceną zabezpieczeń wdrożonych w komponentach sprzętowych, firmware lub programowych systemu (które mogą być wdrożone później). Niezależnie od zlecenia zadania, ostatecznym działaniem przed uruchomieniem systemu jest jednoznaczna akceptacja ryzyka przez osobę autoryzującą.

Etapy RMF i związane z nimi zadania mogą być stosowane do nowych i istniejących systemów w odpowiednich fazach SDLC. W przypadku zarówno nowych jak i istniejących systemów organizacje zapewniają, że wyznaczone zadania zostały wykonane w celu przygotowania do realizacji RMF. W przypadku systemów istniejących, organizacje potwierdzają, że kategoryzacja bezpieczeństwa i (w przypadku systemów informatycznych przetwarzających informacje z zakresu danych osobowych) szacowanie ryzyka w zakresie

ochrony prywatności zostały zakończone i są właściwe oraz że wybrano, dostosowano i wdrożono niezbędne zabezpieczenia.

Zastosowanie etapów RMF i związanych z nimi zadań do istniejących systemów może służyć, jako analiza luk mająca na celu ustalenie, czy ryzyko związane z bezpieczeństwem i prywatnością organizacji było skutecznie zarządzane. Braki w zakresie zabezpieczeń można wyeliminować na etapach wdrażania, oceny, autoryzacji i monitorowania RMF w taki sam sposób, jak w przypadku rozwoju nowych systemów. Jeśli podczas analizy luk nie zostaną wykryte żadne braki i będzie obowiązywała aktualna autoryzacja, organizacja może w RMF przejść bezpośrednio do etapu ciągłego monitorowania. Jeśli aktualna autoryzacja nie obowiązuje, organizacja kontynuuje proces oceny, autoryzacji i monitoringu w typowej kolejności.

DELEGOWANIE ZADAŃ

Role określone w sekcji *Odpowiedzialność podstawowa* dla każdego zadania RMF są odpowiedzialne za zapewnienie realizacji zadania. Role, za które ponosi się główną odpowiedzialność, mogą zakończyć zadanie lub powierzyć wykonanie zadania jednej lub większej liczbie ról *pomocniczych,* z wyjątkiem przypadków, w których przekazanie zadań jest wyraźnie zabronione lub niedozwolone w części "*Dyskusja*" lub w Załączniku D. W przypadku powierzenia wykonania zadania, rola, na której spoczywa Podstawowa odpowiedzialność za to zadanie, pozostaje odpowiedzialna za jego wykonanie.

WSKAZÓWKI DOTYCZĄCE OPTYMALIZACJI WDRAŻANIA RMF

- Wykorzystanie zadań i wyników poziomu organizacji i poziomu systemowego *Etapu Przygotowanie* w celu promowania w organizacjach spójnego punktu wyjścia do realizacji RMF.
- Maksymalne wykorzystanie *zabezpieczeń wspólnych* w celu promowania znormalizowanego, spójnego i efektywnego kosztowo dziedziczenia zdolności w zakresie bezpieczeństwa i ochrony prywatności.
- Maksymalne wykorzystanie *współdzielonych* lub opartych *na chmurze* systemów, usług i aplikacji, w stosownych przypadkach, w celu zmniejszenia liczby uprawnień w organizacji.
- Stosowanie *organizacyjnie dopasowanych poziomów zabezpieczeń w* celu zwiększenia szybkości opracowywania planów bezpieczeństwa i ochrony prywatności, promowania spójności treści planu bezpieczeństwa i ochrony prywatności oraz przeciwdziałania zagrożeniom dla całej organizacji.
- Stosowanie *zdefiniowanych przez organizację zabezpieczeń* opartych na wymaganiach bezpieczeństwa i ochrony prywatności generowanych w procesie inżynierii bezpieczeństwa systemów.
- Maksymalizacja wykorzystania *zautomatyzowanych narzędzi* do zarządzania kategoryzacją bezpieczeństwa; kontrola wyboru, oceny i monitorowania; oraz proces autoryzacji.
- Zmniejszenie poziomu wysiłków i wydatków na zasoby w przypadku systemów o *niewielkim wpływie,* jeżeli systemy te nie mogą negatywnie wpływać na systemy o większym wpływie poprzez połączenia systemowe.
- Maksymalizacja *ponownego wykorzystania* artefaktów RMF (np. wyników oceny bezpieczeństwa i prywatności) dla standardowych wdrożeń sprzętu/oprogramowania, w tym ustawień konfiguracyjnych.

- Zmniejszenie *złożoności* infrastruktury IT/OT poprzez wyeliminowanie zbędnych systemów, elementów systemu i usług - zastosowanie zasady *najmniejszej funkcjonalności.*
- Przejście na *bieżącą autoryzację* i stosowanie metod *ciągłego monitorowania w* celu obniżenia kosztów i zwiększenia efektywności programów bezpie czeństwa i ochrony prywatności.

OPRACOWANIE WYTYCZNYCH DOTYCZĄCYCH BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

RMF jest procesem opartym na SDLC, który może być skutecznie wykorzystywany w celu zapewnienia, że wymogi bezpieczeństwa i ochrony prywatności są spełnione dla systemów informatycznych lub organizacji. Zdefiniowanie jasnych, spójnych i jednoznacznych wymogów w zakresie bezpieczeństwa i ochrony prywatności jest ważnym elementem skutecznej realizacji RMF. Wymagania te są definiowane na wczesnym etapie SDLC we współpracy z kierownikami właściwych komórek organizacyjnych i są włączane do procesów akwizycji i zamówień. Na przykład, organizacje mogą wykorzystać proces inżynierii systemów oparty na cyklu życia do zdefiniowania wstępnego zestawu wymagań dotyczących bezpieczeństwa i ochrony prywatności, który z kolei może być wykorzystany do wyboru zestawu zabezpieczeń[49] w celu spełnienia wymagań. Jeżeli organizacje nabywają systemy, komponenty systemu lub usługi, wymagania lub mechanizmy zabezpieczeń mogą być określone w zapytaniu ofertowym lub innym porozumieniu umownym. Wymagania mogą być również dodawane przez cały cykl życia, np. w przypadku metodologii rozwoju zwinnego, gdzie stale są wdrażane nowe funkcje.

Ramy cyberbezpieczeństwa NIST [NIST CSF][50] (tj. rdzeń, profile) mogą być również wykorzystywane do określania, wyrównywania i unikania potencjalnego konfliktu wymogów bezpieczeństwa, a następnie do informowania o wyborze zabezpieczeń dla organizacji. Profile Ram Cyberbezpieczeństwa mogą stanowić ogniwo łączące działania w zakresie cyberbezpieczeństwa z misją/celami biznesowymi organizacji, co wspiera podejmowanie decyzji w oparciu o ryzyko w całym RMF. Choć Profile mogą być wykorzystywane, jako punkt wyjścia do informowania o wyborze zabezpieczeń i dostosowaniu działań, konieczna jest dalsza ocena w celu zapewnienia wyboru

[49] W sekcji 2.3 znajdują się szczegółowe wskazówki dotyczące wyboru zabezpieczeń ochrony prywatności i zarządzania ryzykiem utraty prywatności.
[50] Brak odpowiednika w Polsce.

odpowiednich zabezpieczeń. Niektóre organizacje mogą zdecydować się na korzystanie z Cybersecurity Framework w zgodzie z publikacjami NIST Systems Security Engineering - identyfikując, dostosowując i eliminując konflikty wymagań w całym sektorze, branży lub organizacji - a następnie stosując podejście inżynierii systemowej w celu dalszego doskonalenia wymagań i uzyskania wiarygodnych bezpiecznych rozwiązań pomagających chronić działalność organizacji, jej aktywa, osoby.[51]

3.1. PRZYGOTOWANIE[52]

CEL

Celem etapu ***Przygotowanie*** jest przeprowadzenie niezbędnych działań na poziomie organizacji, misji i procesu biznesowego oraz systemu informatycznego organizacji, mających na celu pomoc w przygotowaniu organizacji do zarządzania ryzykiem związanym z bezpieczeństwem i ochroną prywatności z wykorzystaniem R*am Zarządzania Ryzykiem*.

PRZYGOTOWYWANIE ZADAŃ - POZIOM ORGANIZACYJNY[53]

Tabela 1 zawiera podsumowanie zadań i oczekiwanych wyników RMF dla etapu *Przygotowanie* na poziomie *organizacji*. Przedstawiono również odnośne konstrukcje ram cyberbezpieczeństwa.

[51] Tamże.
[52] Etap Przygotowanie ma na celu wykorzystanie prowadzonych już działań w ramach programów bezpieczeństwa, ochrony prywatności i łańcucha dostaw, aby podkreślić znaczenie posiadania zarządzania w całej organizacji i odpowiednich zasobów umożliwiających realizację efektywnych kosztowo i spójnych procesów zarządzania ryzykiem w całej organizacji.
[53] Dla ułatwienia, czynności przygotowawcze są podzielone na przygotowanie na poziomie organizacji i przygotowanie na poziomie systemu informatycznego.

Zadania	REZULTATY
ZADANIE P-1 **ROLE ZARZĄDZAJĄCE RYZYKIEM**	• Zidentyfikowanie osób fizycznych i przypisanie im kluczowych ról w realizacji Ram Zarządzania Ryzykiem. [*Ramy Cyberbezpieczeństwa:* **ID.AM-6; ID.GV-2**][54]
ZADANIE P-2 **STRATEGIA ZARZĄDZANIA RYZYKIEM**	• Ustanawianie strategii zarządzania ryzykiem organizacji, która obejmuje określenie i wyrażenie tolerancji dla ryzyka organizacyjnego. [*Ramy Cyberbezpieczeństwa:* **ID.RM; ID.SC**]
ZADANIE P-3 **SZACOWANIE RYZYKA – ORGANIZACJA**	• Ocena zakończonego lub aktualizacja istniejącego szacowania ryzyka w skali całej organizacji. [*Ramy Cyberbezpieczeństwa:* **ID.RA; ID.SC-2**]
ZADANIE P-4 **DOSTOSOWYWANIE PRZEZ ORGANIZACJĘ ZABEZPIECZEŃ BAZOWYCH I PROFILI RAM CYBERBEZPIECZEŃSTWA (OPCJONALNIE)**	• Ustanowienie i udostępnienie dostosowanych do potrzeb organizacji podstawowych mechanizmów zabezpieczeń i/lub Profili Ram Cyberbezpieczeństwa. [*Ramy Cyberbezpieczeństwa:* **Profil**]

[54] W Polsce nie mają zastosowania. Dotyczy to całego dokumentu.

Zadania	REZULTATY
ZADANIE P-5 **IDENTYFIKACJA ZABEZPIECZEŃ WSPÓLNYCH**	• Zabezpieczenia wspólne, które są dostępne do dziedziczenia przez systemy organizacji, są zidentyfikowane, udokumentowane i opublikowane.
ZADANIE P-6 **PRIORYTETYZACJA NA POZIOMIE WPŁYWU (NIEOBOWIĄZKOWO)**	• Przeprowadzona została priorytetyzacja systemów organizacji o tym samym poziomie wpływu. [*Ramy Cyberbezpieczeństwa:* **ID.AM-5**]
ZADANIE P-7 **STRATEGIA CIĄGŁEGO MONITOROWANIA – ORGANIZACJA**	• Opracowywana i wdrażana jest organizacyjna strategia monitorowania skuteczności zabezpieczeń. [*Ramy Cyberbezpieczeństwa:* **DE.CM; ID.SC-4**]

ROLE ZARZĄDZAJĄCE RYZYKIEM

ZADANIE P-1 Identyfikacja i przypisanie poszczególnych osób do określonych ról związanych z zarządzaniem ryzykiem w zakresie bezpieczeństwa i ochrony prywatności.

Potencjalne dane wejściowe: Zasady i procedury bezpieczeństwa organizacji i ochrony prywatności, schematy organizacyjne.

Oczekiwane wyniki: Udokumentowane przypisanie ról w ramach zarządzania ryzykiem.

Podstawowa odpowiedzialność: HA, CIO, SAOP.[55]

Role wspierające: AO lub AODR, SAORM lub RE, SAISO.

Dyskusja: Role i obowiązki kluczowych uczestników procesów zarządzania ryzykiem zostały opisane w załączniku D. Role i obowiązki mogą obejmować, odpowiednio, personel wewnętrzny lub zewnętrzny w stosunku do organizacji. Ponieważ organizacje mają różne misje, funkcje i struktury organizacyjne, mogą występować różnice w nazewnictwie ról związanych z zarządzaniem ryzykiem oraz w sposobie podziału konkretnych obowiązków pomiędzy pracowników organizacji (np. wiele osób wypełniających jedną rolę lub jedna osoba wypełniająca wiele ról). W obu sytuacjach podstawowe funkcje zarządzania ryzykiem pozostają takie same. Organizacje zapewniają, że nie występuje konflikt interesów przy przydzielaniu tej samej osoby do wielu ról w zarządzaniu ryzykiem. Na przykład osoby autoryzujące nie mogą zajmować roli właściciela systemu lub dostawcy zabezpieczeń wspólnych, które autoryzują. Ponadto łączenie wielu ról związanych z bezpieczeństwem i ochroną prywatności wymaga ostrożności, ponieważ te dwie dziedziny mogą wymagać różnej wiedzy specjalistycznej, a w pewnych okolicznościach priorytety mogą być konkurencyjne. Niektóre role mogą być przypisane do grupy lub komórki organizacyjnej, a nie do osoby fizycznej, na przykład podmiotu podmiot oceniający zabezpieczenia, osoby wykonującej zadania z zakresu zarządzania ryzykiem (funkcja) lub administratora systemu.

[55] Akronimy ról - patrz: Załącznik D. Dotyczy to całego dokumentu. Role te są opisane także w publikacji NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*.

Referencje: SP 800-160] (Proces zarządzania zasobami ludzkimi); [SP 800-181]; [NIST CSF] (Rdzeń [Identyfikacja funkcji]).

Uwaga:

Niektóre ze wskazanych dokumentów nie mają odzwierciedlenia w polskim systemie prawa, niemniej przytoczone zostały w celu naświetlenia kontekstu, w jakim podejmowane są powyższe działania. Uwaga ta dotyczy całego dokumentu.

STRATEGIA ZARZĄDZANIA RYZYKIEM

ZADANIE P-2 Ustalenie strategii zarządzania ryzykiem dla organizacji, która obejmuje określenie tolerancji ryzyka.

Potencjalne dane wejściowe: Misja organizacji; polityka organizacji; założenia dotyczące ryzyka w organizacji, ograniczenia, priorytety i kompromisy.

Oczekiwane wyniki: Strategia zarządzania ryzykiem i oświadczenie o tolerancji ryzyka, w tym ryzyko związane z bezpieczeństwem informacji i ochroną prywatności.

Podstawowa odpowiedzialność: HA.

Role wspierające: SAORM lub RE; CIO; SAISO; SAOP.

Dyskusja: Tolerancja ryzyka jest to stopień ryzyka lub niepewności, który jest akceptowalny dla organizacji. Tolerancja ryzyka ma wpływ na wszystkie części procesu zarządzania ryzykiem w organizacji, ma bezpośredni wpływ na decyzje dotyczące zarządzania ryzykiem podejmowane przez kierowników wyższego szczebla lub członków kadry kierowniczej w całej organizacji i stanowi istotne ograniczenie dla tych decyzji. Strategia zarządzania ryzykiem prowadzi i informuje o decyzjach opartych na ryzyku, w tym o tym, w jaki sposób ryzyko związane z bezpieczeństwem i prywatnością jest określane, oceniane, uwzględniane i monitorowane. Strategia zarządzania ryzykiem może składać się z pojedynczego dokumentu lub oddzielnych dokumentów dotyczących zarządzania ryzykiem w zakresie

bezpieczeństwa i ochrony prywatności. Strategia zarządzania[56] ryzykiem wyraźnie określa zagrożenia, założenia, ograniczenia, priorytety, kompromisy i tolerancję ryzyka wykorzystywane przy podejmowaniu decyzji inwestycyjnych i operacyjnych. Strategia ta obejmuje decyzje na poziomie strategicznym oraz rozważania dotyczące sposobu, w jaki liderzy wyższego szczebla i kadra kierownicza mają zarządzać ryzykiem związanym z bezpieczeństwem i prywatnością (w tym ryzykiem związanym z łańcuchem dostaw) dla operacji organizacji, aktywów organizacji, osób, innych organizacji i Państwa. Strategia zarządzania ryzykiem obejmuje wyrażenie tolerancji na ryzyko w organizacji, akceptowalne metody szacowania ryzyka i strategie reagowania na ryzyko, proces spójnego szacowania ryzyka bezpieczeństwa i prywatności w całej organizacji oraz podejście do monitorowania ryzyka w czasie. Ponieważ organizacje definiują i wdrażają strategie, polityki, procedury i procesy zarządzania ryzykiem, ważne jest, aby uwzględniały one aspekty SCRM. Strategia zarządzania ryzykiem w zakresie bezpieczeństwa i prywatności łączy programy bezpieczeństwa i ochrony prywatności z systemami zarządzania zabezpieczeń ustanowionymi w strategii zarządzania ryzykiem korporacyjnym organizacji.

Referencje: [NSC 800-30]; [SP 800-39] (poziom organizacji); [SP 800-160] (zarządzanie ryzykiem, zarządzanie decyzjami, zapewnienie jakości, zarządzanie jakością, ocena i kontrola projektów); [SP 800-161]; [IR 8062]; [IR 8179] (proces analizy krytyczności B); [NIST CSF] (rdzeń [funkcja identyfikacji]).

SZACOWANIE RYZYKA - ORGANIZACJA

ZADANIE P-3 Ocena zagrożeń bezpieczeństwa i prywatności w całej organizacji oraz bieżąca aktualizacja wyników szacowania ryzyka.

Potencjalne dane wejściowe: Strategia zarządzania ryzykiem; misja lub cele biznesowe; bieżące informacje o zagrożeniach; wyniki szacowania ryzyka związanego z bezpieczeństwem

[56] Odrębny dokument dotyczący strategii zarządzania ryzykiem w łańcuchu dostaw nazywany jest planem zarządzania ryzykiem w łańcuchu dostaw.

i prywatnością na poziomie systemu; wyniki szacowania ryzyka związanego z łańcuchem dostaw; wcześniejsze wyniki szacowania ryzyka związanego z bezpieczeństwem i prywatnością na poziomie organizacji; umowy o wymianie informacji lub protokoły ustaleń; informacje dotyczące bezpieczeństwa i ochrony prywatności pochodzące z ciągłego monitorowania.

Oczekiwane wyniki: Wyniki szacowania ryzyka na poziomie organizacji.

Podstawowa odpowiedzialność: SAORM lub RE; SAISO; SAOP.

Role wspierające: CIO; BO; AO lub AODR.

Dyskusja: Szacowanie ryzyka na poziomie organizacji wykorzystuje zagregowane informacje pochodzące z wyników szacowania ryzyka na poziomie systemu, stałego monitorowania oraz wszelkich strategicznych rozważań na temat ryzyka istotnych dla organizacji. Organizacja bierze pod uwagę całość ryzyka związanego z funkcjonowaniem i wykorzystaniem swoich systemów informatycznych, z wymianą informacji i powiązaniami z innymi wewnętrznymi i zewnętrznymi systemami oraz z wykorzystaniem zewnętrznych dostawców. Na przykład, organizacja może dokonać przeglądu ryzyka związanego z jej architekturą korporacyjną i systemami informatycznymi o różnych poziomach wpływu, występującymi w tej samej sieci oraz rozważyć, czy systemy o wyższym poziomie wpływu są oddzielone od systemów o niższym poziomie wpływu lub systemów obsługiwanych i utrzymywanych przez dostawców zewnętrznych. Organizacja może również wziąć pod uwagę zmienność środowisk, które mogą istnieć w obrębie organizacji (np. różne lokalizacje obsługujące różne misje/procesy biznesowe) oraz potrzebę uwzględnienia takiej zmienności w szacowaniu ryzyka.
W organizacji może być również przeprowadzane szacowanie ryzyka łańcucha dostaw.
Wyniki szacowania ryzyka mogą być wykorzystane w celu wsparcia organizacji w tworzeniu Profilu Ram Cyberbezpieczeństwa.

Referencje: [NSC 800-30]; [SP 800-39] (poziom organizacji, poziom misji/procesu biznesowego); [SP 800-161]; [IR 8062].

DOSTOSOWYWANIE PRZEZ ORGANIZACJĘ PODSTAWOWYCH MECHANIZMÓW ZABEZPIECZEŃ I PROFILI RAM CYBERBEZPIECZEŃSTWA (OPCJONALNIE)

ZADANIE P-4 Ustanowienie, udokumentowanie i opublikowanie dostosowanych przez organizację zabezpieczeń bazowych[57] i/lub Profili Ram Cyberbezpieczeństwa.

Potencjalne dane wejściowe: Udokumentowane, dostosowane do organizacji wymagania w zakresie bezpieczeństwa i ochrony prywatności ukierunkowujące wykorzystanie zabezpieczeń bazowych; misja lub cele biznesowe; architektura korporacyjna; architektura bezpieczeństwa; architektura prywatności; wyniki szacowania ryzyka na poziomie organizacji i systemu; lista wspólnych dostawców zabezpieczeń i zabezpieczeń wspólnych dostępnych do dziedziczenia; SP 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji*.[58]

Oczekiwane wyniki: Lista zatwierdzonych lub dostosowanych do organizacji zabezpieczeń bazowych; Profile [NIST CSF].

Podstawowa odpowiedzialność: BO; SAORM lub RE.

Role wspierające: CIO; AO lub AODR; SAISO; SAOP.

Dyskusja: W odpowiedzi na misję organizacyjną lub zapotrzebowanie biznesowe na specjalistyczne zestawy zabezpieczeń zmniejszające ryzyko, można opracować organizacyjnie dopasowane zabezpieczenia bazowe do użytku w całej organizacji. [59] Dostosowane do potrzeb organizacji zabezpieczenia bazowe zapewniają w pełni określony zestaw

[57] W publikacji, zamiennie do pojęcia ***zabezpieczenia bazowe***, używane jest określenie ***zestaw minimalnych zabezpieczeń***.

[58] NSC 800-53 (Wersja 2), oddziela katalog zabezpieczeń od zabezpieczeń bazowych, które historycznie były zawarte w publikacji NSC 800-53 (Wersja 1). Nowa publikacja towarzysząca NSC 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji*, definiuje zalecane zabezpieczenia bazowe. Publikacja NSC 800-53B jest cytowany w poszczególnych zadaniach przedstawianych w RMF.

[59] Dostosowywane zabezpieczenia bazowe mogą być również określane jako nakładki (*ang. Overlays*). Dostosowane zabezpieczenia bazowe mogą być również określane jako nakładki. Dostosowane organizacyjnie zabezpieczenie bazowe jest analogiczne do nakładki obejmującej całą organizację, ponieważ nakładka jest dostosowanym zabezpieczeniem bazowym, które obsługuje wspólnotę interesów, w tym przypadku organizację.

zabezpieczeń podstawowych, zabezpieczeń rozszerzonych oraz dodatkowe wytyczne wynikające z ustalonych podstawowych mechanizmów zabezpieczeń opisanych w [SP 800-53B]. Proces dostosowywania może być również prowadzony i wspierany przez proces inżynierii wymagań opisany w [SP 800-160 V.1]. Organizacje mogą stosować dostosowaną koncepcję zabezpieczeń bazowych w przypadku wystąpienia rozbieżności w stosunku do konkretnych założeń użytych do utworzenia zabezpieczeń bazowych opisanych w [SP 800-53B]. Dotyczy to na przykład sytuacji, w których organizacja jest narażona na określone zagrożenia dla bezpieczeństwa lub prywatności, ma określoną misję lub potrzeby biznesowe albo planuje działać w środowiskach, które nie są uwzględnione w zestawach minimalnych zabezpieczeń.

Dostosowane do potrzeb organizacji zabezpieczenia bazowe i nakładek uzupełniają zabezpieczenia bazowe występujące w NSC, dając możliwość dodania lub wyeliminowania zabezpieczenia w celu dostosowania się do wymagań organizacji przy jednoczesnej ochronie informacji współmiernej do ryzyka. Organizacje mogą korzystać z dostosowanych zabezpieczeń bazowych i nakładek w celu dostosowania zestawu minimalnych zabezpieczeń poprzez opisanie możliwości zastosowania zabezpieczenia oraz poprzez zapewnienie interpretacji dla konkretnych technologii; rodzajów misji lub funkcji biznesowych, operacji, systemów, środowisk i trybów działania oraz wymogów ustawowych lub regulacyjnych. Wiele niestandardowych zabezpieczeń bazowych może być przydatnych dla organizacji o niejednorodnych systemach (np. w organizacjach, które utrzymują systemy o różnych cechach operacyjnych lub przetwarzania albo cechach misji lub działalności).

Dostosowane do organizacji zabezpieczenia bazowe mogą ustanawiać zdefiniowane przez organizację wartości parametrów kontrolnych dla oświadczeń o przypisaniu lub wybraniu zabezpieczeń podstawowych i zabezpieczeń rozszerzonych, które są uzgodnione z konkretnymi grupami interesu, a w razie potrzeby mogą również tworzyć dodatkowe wytyczne. Dostosowane zabezpieczenia bazowe mogą być bardziej lub mniej rygorystyczne niż zabezpieczenia określone w [SP 800-53B] i są stosowane do wielu systemów.

Dostosowane do potrzeb organizacji zabezpieczenia, opracowane poza organizacją, mogą być nakazane do stosowania przez określone przepisy prawa, zasady lub standardy. W niektórych sytuacjach działania dostosowawcze mogą być ograniczone przez twórcę dostosowanych zabezpieczeń lub organ wydający decyzję, co do określonego zabezpieczenia. Dostosowane zabezpieczenia bazowe (lub nakładki) zostały opracowane przez społeczności będące przedmiotem zainteresowania dla chmury i systemów wspólnych, usług i aplikacji; przemysłowych systemów sterowania; ochrony danych osobowych; krajowych systemów bezpieczeństwa; uzbrojenia i systemów kosmicznych; aktywów o wysokiej wartości; zarządzania urządzeniami przenośnymi; rządowej infrastruktury klucza publicznego; oraz zagrożeń dla prywatności.

Organizacje mogą również czerpać korzyści z opracowania jednego lub więcej *Profili* Ram Cyberbezpieczeństwa. Profil Ram Cyberbezpieczeństwa wykorzystuje Podkategorie w Rdzeniu Ram Cyberbezpieczeństwa w celu dostosowania wyników w zakresie cyberbezpieczeństwa do misji lub wymagań biznesowych, tolerancji ryzyka i zasobów organizacji. Uszeregowana pod względem priorytetów lista rezultatów w zakresie cyberbezpieczeństwa opracowana na poziomie organizacji i misji/procesów biznesowych, może być pomocna w podejmowaniu spójnych, opartych na ryzyku decyzji na poziomie systemu. Podkategorie określone w odpowiednich Profilach Ramowych Cyberbezpieczeństwa mogą być również wykorzystywane, jako wytyczne i informacje przy opracowywaniu opisanych powyżej zabezpieczeń bazowych dostosowanych do potrzeb.

Referencje: [NSC 800-53]; [SP 800-53B]; [SP 800-160 V.1] (Analiza działalności lub misji oraz procesy definiowania potrzeb i wymagań interesariuszy); [CSF NIST] (Rdzeń, Profile).

IDENTYFIKACJA ZABEZPIECZEŃ WSPÓLNYCH

ZADANIE P-5 Zidentyfikowanie, udokumentowanie i opublikowanie zabezpieczeń wspólnych, które są dostępne do dziedziczenia przez systemy organizacji.

Potencjalne dane wejściowe: Udokumentowane wymagania dotyczące bezpieczeństwa i ochrony prywatności; istniejące plany zabezpieczeń wspólnych i związane z nimi plany bezpieczeństwa i ochrony prywatności; plany programów bezpieczeństwa informacji i ochrony prywatności; wyniki szacowania ryzyka związanego z bezpieczeństwem i ochroną prywatności na poziomie organizacji i systemów.

Oczekiwane wyniki: Lista dostawców zabezpieczeń wspólnych dostępnych do dziedziczenia; plany bezpieczeństwa i ochrony prywatności (lub równoważne dokumenty) zawierające opis realizacji zabezpieczeń wspólnych (w tym dane wejściowe, oczekiwane zachowanie i oczekiwane wyniki).

Podstawowa odpowiedzialność: SAISO; SAOP.

Role wspierające: BO; SAORM lub RE; CIO; AO lub AODR; CCP; SO.

Dyskusja: Zabezpieczenia wspólne to zabezpieczenia, które mogą być dziedziczone przez jeden lub więcej systemów informatycznych. [60] Zabezpieczenia wspólne mogą obejmować zabezpieczenia z dowolnej kategorii zabezpieczeń [NSC 800-53], na przykład zabezpieczenia z zakresu ochrony fizycznej i środowiskowej, zabezpieczenia granic systemu i monitorowania, zabezpieczenia dotyczące personelu, zasad i procedur, zabezpieczenia w zakresie nabywania, zabezpieczenia w zakresie zarządzania kontem i tożsamością, zabezpieczenia dziennika audytów i rozliczalności lub zabezpieczenia zarządzania skargami i zapytaniami od społeczeństwa dotyczącymi ochrony prywatności. Organizacje określają i wybierają zestaw zabezpieczeń wspólnych i przydzielają te zabezpieczenia komórkom organizacyjnym wyznaczonym, jako zarządzające tymi zabezpieczeniami. Zabezpieczenia wspólne mogą różnić się w zależności od różnych czynników, takich jak lokalizacja hostingu, architektura systemu i struktura organizacji. Ogólna lista zabezpieczeń wspólnych w całej organizacji uwzględnia powyższe czynniki. Zabezpieczenia wspólne mogą być również zidentyfikowane

[60] Zabezpieczenia wspólne są autoryzowane przez wyznaczone osoby autoryzujące przed udostępnieniem zabezpieczeń do dziedziczenia przez systemy organizacyjne. Opis różnych rodzajów autoryzacji znajduje się w Załączniku F.

na różnych poziomach organizacji (np. na poziomie korporacyjnym, departamentu lub urzędu, na poziomie biura lub na poziomie indywidualnego programu). Organizacje mogą ustanowić jedną lub więcej list zabezpieczeń wspólnych, które mogą być dziedziczone przez systemy informatyczne. Wymóg stosowania określonego zabezpieczenia może nie być w pełni spełniony przez zabezpieczenia wspólne. W takich przypadkach zabezpieczenie jest uznawane za zabezpieczenie hybrydowe i jako takie jest przez organizację odnotowywane, łącznie z określeniem, które części wymogu zabezpieczenia są przewidziane do dziedziczenia, jako zabezpieczenie wspólne, a które elementy zabezpieczenia mają być zapewnione na poziomie systemu.

Jeżeli istnieje wiele źródeł zabezpieczeń wspólnych, organizacje określają dostawcę zabezpieczenia wspólnego (tzn. kto zapewnia zabezpieczenie i w jaki sposób, na przykład usługi wspólne, określone systemy lub w ramach określonego typu architektury) oraz jakie systemy lub typy systemów mogą je dziedziczyć. Wykazy zabezpieczeń wspólnych są przekazywane właścicielom systemów, dzięki czemu są oni świadomi możliwości w zakresie bezpieczeństwa i ochrony prywatności, które są dostępne z poziomu organizacji w drodze dziedziczenia. Właściciele systemów nie są zobowiązani do oceny zabezpieczeń wspólnych, które są dziedziczone przez ich systemy, ani do dokumentowania szczegółów wdrożenia zabezpieczenia wspólnego - jest to obowiązkiem dostawców usług zabezpieczeń wspólnych. Podobnie, dostawcy usług zabezpieczeń wspólnych nie są zobowiązani do wglądu w szczegóły dotyczące systemów, które dziedziczą dostarczane przez nich zabezpieczenia.

Wyniki szacowania ryzyka mogą być wykorzystane przy określaniu zabezpieczeń wspólnych w celu ustalenia, czy mechanizmy zabezpieczeń dostępne do celów dziedziczenia spełniają wymogi bezpieczeństwa i ochrony prywatności systemów organizacji oraz środowisk, w których systemy te funkcjonują (w tym do określenia potencjalnych pojedynczych punktów awarii). W przypadku stwierdzenia, że zabezpieczenia wspólne zapewniane przez organizację są niewystarczające dla systemów informatycznych, które je dziedziczą, właściciele systemów mogą uzupełnić zabezpieczenia wspólne o mechanizmy zabezpieczeń specyficzne dla danego systemu lub hybrydowe zabezpieczenia, w celu osiągnięcia

wymaganej ochrony swoich systemów lub zaakceptowania większego ryzyka za zgodą organizacji.

Dostawcy zabezpieczeń wspólnych realizują działania RMF w celu wdrożenia, oceny i monitorowania zabezpieczeń wyznaczonych, jako zabezpieczenia wspólne. Podmiotami zapewniającymi zabezpieczenia wspólne mogą być również właściciele systemu, jeśli zabezpieczenia te funkcjonują w ramach systemu informatycznego. Organizacje wybierają wyższy personel lub członków kadry kierowniczej, którzy autoryzują zabezpieczenia wspólne. Personel wyższego szczebla ds. prywatności jest odpowiedzialny za wyznaczenie zabezpieczeń wspólnych prywatności i udokumentowanie ich w planie programu ochrony prywatności organizacji. Osoba autoryzująca jest odpowiedzialna za zaakceptowanie ryzyka związanego z bezpieczeństwem i prywatnością wynikającego z korzystania z zabezpieczeń wspólnych, odziedziczonych przez systemy organizacji.

Dostawca zabezpieczeń wspólnych jest odpowiedzialny za dokumentowanie tych zabezpieczeń w planach bezpieczeństwa i ochrony prywatności (lub równoważnych dokumentach zalecanych przez organizację), zapewnienie, że zabezpieczenia wspólne są wdrażane i oceniane pod kątem skuteczności przez wykwalifikowanych podmiot oceniających oraz, że ustalenia z oceny są dokumentowane w sprawozdaniach z oceny. Odpowiada także za sporządzanie planu działania, w przypadku stwierdzenia niedopuszczalnych braków, który ma na celu ich naprawienie. Występuje o autoryzację zabezpieczeń do wyznaczonej osoby udzielającej takiej autoryzacji oraz stale monitoruje skuteczność zabezpieczenia. Plany, sprawozdania z oceny oraz plany działania i kluczowe etapy zabezpieczeń wspólnych (lub podsumowanie takich informacji) są udostępniane właścicielom systemów i powinny być wykorzystywane przez personel autoryzujący w celu wydawania decyzji dotyczących zezwoleń na systemy dziedziczące zabezpieczenia wspólne i informowania o nich. Informacje na temat autoryzacji zabezpieczeń wspólnych znajdują się w Zadaniu R-4 i Załączniku F.

Referencje: [NSC 800-53].

Priorytetyzacja na poziomie wpływu

ZADANIE P-6 Priorytetyzacja systemów organizacji o tym samym poziomie wpływu (opcjonalnie).[61]

Potencjalne dane wejściowe: Informacje o kategoryzacji bezpieczeństwa systemów organizacji; opisy systemów; wyniki szacowania ryzyka na poziomie organizacji i systemu; misja lub cele biznesowe; Profile Ram Cyberbezpieczeństwa.

Oczekiwane wyniki: Systemy organizacji zostały podzielone na podkategorie o niskim, średnim i wysokim wpływie (podatności).

Podstawowa odpowiedzialność: SAORM lub RE.

Role wspierające: SAISO; SAOP; BO; SO; CIO; AO lub AODR.

Dyskusja: Zadanie to jest realizowane dopiero po skategoryzowaniu systemów organizacji (zob.: Zadanie - C1). Zadanie to wymaga, aby organizacje najpierw zastosowały oznaczenie najwyższego poziomu wpływu do każdego ze swoich systemów informatycznych skategoryzowanych zgodnie z [NSC 199] i [NSC 200]. Zastosowanie koncepcji oznaczenia najwyższego poziomu wpływu powoduje, że systemy są określane, jako systemy o małym, umiarkowanym lub dużym wpływie zakłócenia lub incydentu.

Organizacje pragnące zwiększyć stopień szczegółowości kategoryzacji systemów, mogą wykorzystać to zadanie do ustalenia priorytetów dla swoich systemów w ramach każdego poziomu wpływu. [62] Na przykład, organizacja może podjąć decyzję o nadaniu priorytetu swoim systemom o umiarkowanych skutkach poprzez przypisanie każdego z nich do jednej z trzech nowych podkategorii: systemy *nisko-umiarkowane*, systemy *umiarkowanie-*

[61] Organizacje mogą skorzystać z tego zadania w połączeniu z opcjonalnym etapem RMF Poziom przygotowania organizacyjnego, Zadanie P-4, aby opracować organizacyjnie dostosowane zestawy minimalnych zabezpieczeń w celu bardziej dokładnych oznaczeń wpływu, na przykład organizacyjnie dostosowane podstawowe mechanizmy zabezpieczeń dla systemów o niskim (*ang. Low-moderate*) i wysokim (*ang. High-moderate*) stopniu umiarkowanego poziomu wpływu. Patrz przepisy o ochronie informacji niejawnych.

[62] Organizacje mogą również zdecydować się na zastosowanie alternatywnego, zdefiniowanego przez organizację podejścia kategoryzacyjnego w celu dodania dodatkowej szczegółowości do poziomów wpływu określonych w [NSC 199].

umiarkowane i systemy *wysoko-umiarkowane.* Systemy wysoko-umiarkowane uzyskują wyższy priorytet niż systemy nisko-umiarkowane i umiarkowanie-umiarkowane, a systemy nisko-umiarkowane niższy priorytet niż systemy umiarkowane i umiarkowanie-umiarkowane. Nadanie priorytetu systemom umiarkowanym daje organizacjom możliwość podejmowania bardziej świadomych decyzji dotyczących wyboru zabezpieczeń oraz dostosowania poziomu zabezpieczeń do potrzeb wynikających z reagowania na zidentyfikowane ryzyka.

Priorytety na poziomie wpływu mogą być również wykorzystywane do określania systemów, które są krytyczne lub istotne dla misji organizacji i operacji biznesowych, a zatem organizacje mogą skupić się na czynnikach złożoności, agregacji i wzajemnych powiązań tych systemów. Ustalanie priorytetów na poziomie wpływu może być prowadzone na każdym poziomie organizacji i opiera się na danych dotyczących kategoryzacji bezpieczeństwa zgłaszanych przez poszczególnych właścicieli systemów. Ustalanie priorytetów na poziomie wpływu może wymagać opracowania dostosowanego do organizacji odpowiedniego zestawu zabezpieczeń dla dodatkowych, bardziej szczegółowych poziomów wpływu.

Profile Ram Cyberbezpieczeństwa mogą być wykorzystywane przez organizacje do wspierania zadania ustalania priorytetów na poziomie wpływu. Misja i cele biznesowe oraz uszeregowane pod względem ważności wyniki zdefiniowane w odpowiednich Profilach Ram Cyberbezpieczeństwa mogą pomóc w rozróżnieniu względnego priorytetu pomiędzy systemami o tym samym poziomie wpływu. Profile Ram Cyberbezpieczeństwa mogą być zorganizowane wokół priorytetu misji/celów biznesowych organizacji, a tym celom przypisuje się względny priorytet. Na przykład, cele związane z bezpieczeństwem człowieka i środowiska mogą być dwoma najważniejszymi celami istotnymi w kontekście profilu. W tym przykładzie, podczas wykonywania zadania P-6, system, który odnosi się do celu związanego z bezpieczeństwem człowieka, może mieć wyższy priorytet niż system, który ma takie same poziomy wpływu, ale nie odnosi się do celu związanego z bezpieczeństwem człowieka.

Referencje: [NSC 199]; [NSC 200]; [NSC 800-30]; [SP 800-39] (Poziomy organizacji i systemu); [SP 80059]; [NSC 800-60 cz. 1]; [SP 800-160] (Proces definiowania wymagań systemowych);

[IR 8179] (Proces analizy krytyczności B); [CNSSI 1253]; [NIST CSF] (Podstawowe [Funkcja identyfikacji]; Profile).

STRATEGIA CIĄGŁEGO MONITOROWANIA – ORGANIZACJA

ZADANIE P-7 Opracowanie i wdrożenie w całej organizacji strategii ciągłego monitorowania skuteczności zabezpieczeń.

Potencjalne dane wejściowe: Strategia zarządzania ryzykiem; wyniki szacowania ryzyka na poziomie organizacji i systemu; polityka bezpieczeństwa i ochrony prywatności w organizacji.

Oczekiwane wyniki: Wdrożona na poziomi organizacji strategia ciągłego monitorowania.

Podstawowa odpowiedzialność: SAORM lub RE.

Role wspierające: CIO; SAISO; SAOP; BO; SO; AO LUB AODR.

Dyskusja: Ważnym aspektem zarządzania ryzykiem jest możliwość monitorowania na bieżąco statusu bezpieczeństwa i ochrony prywatności w całej organizacji oraz skuteczności zabezpieczeń wprowadzanych w ramach systemów organizacji lub dziedziczonych przez nie.[63] Skuteczna strategia ciągłego monitorowania w całej organizacji jest niezbędna do skutecznego i efektywnego kosztowo prowadzenia takiego monitoringu. Strategie ciągłego monitorowania mogą obejmować również kwestie związane z ryzykiem w łańcuchu dostaw, na przykład regularne przeglądy dostawców pochodzących z zagranicy, monitorowanie prognoz zapasów lub wymaganie bieżących audytów dostawców. Wdrożenie solidnego i kompleksowego programu stałego monitorowania pomaga organizacji zrozumieć bezpieczeństwo i prywatność w jej systemach informatycznych. Ułatwia również bieżącą autoryzację po zainicjowaniu pracy systemu lub autoryzację zabezpieczeń wspólnych.

[63] Monitoring skuteczności bezpieczeństwa jest formą oceny zabezpieczeń. [NSC 800-53A], [SP 800-137] oraz [IR 8011 v1] zawierają dodatkowe informacje dotyczące odpowiednio monitorowania, przeprowadzania ocen skuteczności zabezpieczeń oraz automatyzacji ocen skuteczności zabezpieczeń.

Obejmuje to możliwość zmiany misji lub funkcji biznesowych, interesariuszy, technologii, podatności, zagrożeń, ryzyka oraz dostawców systemów, komponentów lub usług.

Strategia ciągłego monitorowania organizacji dotyczy wymagań w zakresie monitorowania na poziomie organizacji, procesu misyjnego/biznesowego oraz systemu informatycznego. Strategia ciągłego monitorowania określa minimalną częstotliwość monitorowania wdrożonych zabezpieczeń w całej organizacji, definiuje podejście do bieżącej oceny zabezpieczeń oraz opisuje sposób prowadzenia bieżącej oceny (np. odnosi się do stosowania i zarządzania zautomatyzowanymi narzędziami oraz instrukcjami dotyczącymi bieżącej oceny zabezpieczeń, w przypadkach, w których monitorowanie nie może być zautomatyzowane). Strategia ciągłego monitorowania może również określać wymogi w zakresie bezpieczeństwa i ochrony prywatności, w tym wobec odbiorców sprawozdań. Kryteria określania minimalnej częstotliwości monitorowania zabezpieczeń ustala się we współpracy z personelem organizacji (np. SAORM lub RE; SAISO; SAOP; CIO; SO; CCP oraz AO lub AODR). Szacowanie ryzyka na poziomie organizacji może być wykorzystywana, jako wskazówka i źródło informacji na temat częstotliwości monitorowania.

Zastosowanie automatyzacji ułatwia zwiększenie częstotliwości i ilości ocen zabezpieczeń w ramach procesu monitorowania. Bieżące monitorowanie zabezpieczeń przy użyciu zautomatyzowanych narzędzi i wspomagających baz danych ułatwia zarządzanie ryzykiem systemów informatycznych w czasie niemal rzeczywistym oraz wspiera bieżące autoryzowanie i efektywne wykorzystanie zasobów. SAORM lub RE zatwierdza strategię ciągłego monitorowania, w tym minimalną częstotliwość, z jaką zabezpieczenia mają być monitorowane.

Referencje: [NSC 800-30]; [SP 800-39] (Organizacja, misja lub proces biznesowy, poziomy systemu); [NSC 800-53]; [NSC 800-53A]; [SP 800-137]; [SP 800-161]; [IR 8011 v1]; [IR 8062]; [NIST CSF] (podstawowe [funkcje identyfikacji, wykrywania]); [CNSSI 1253].

UWAGI DOTYCZĄCE MISJI/PROCESU BIZNESOWEGO (POZIOM 2)

Kwestie związane z misją/procesem biznesowym są poruszane na etapie *Poziomu przygotowania organizacji* RMF oraz na etapie P*rzygotowania systemu* RMF poprzez określenie misji/procesu biznesowego; poprzez identyfikację misji lub właścicieli procesów biznesowych pełniących funkcje podstawowe lub pomocnicze; oraz poprzez określenie misji lub celów biznesowych.

Zadanie P-8 i zadanie P-9 z etapu P*rzygotowanie systemu* RMF, to zadania na poziomie misji/procesów biznesowych prowadzone z ukierunkowaniem specyficznym dla poziomu systemu.

PRZYGOTOWANIE ZADAŃ - POZIOM SYSTEMU

Tabela 2 zawiera podsumowanie zadań i oczekiwanych wyników RMF dla etapu *Przygotowanie* na *poziomie systemu*. Przedstawiono również obowiązujące konstrukcje ram cyberbezpieczeństwa.

TABELA 2: PRZYGOTOWANIE ZADAŃ I WYNIKÓW NA POZIOMIE SYSTEMU

Zadania	Wyniki
ZADANIE P-8 **MISJA LUB PRZEDMIOT DZIAŁANIA**	• Identyfikowane są misje, funkcje biznesowe i procesy biznesowe, które system ma wspierać. [*Ramy Cyberbezpieczeństwa:* **profil**; **poziomy wdrożenia**; **ID.BE**]
ZADANIE P-9 **INTERESARIUSZE SYSTEMU**	• Identyfikuje się podmioty, które są zainteresowane wykorzystywaniem systemu. [*Ramy Cyberbezpieczeństwa:* **ID.AM**; **ID.BE**]
ZADANIE P-10 **IDENTYFIKACJA AKTYWÓW**	• Identyfikowane są aktywa zainteresowanych stron i ustalane są ich priorytety. [*Ramy Cyberbezpieczeństwa:* **ID.AM**]
ZADANIE P-11 **GRANICA AUTORYZACJI**	• Określona jest granica autoryzacji (tzn. co wchodzi w skład systemu).
ZADANIE P-12 **TYP INFORMACJI**	• Określane są typy informacji przetwarzanych przez system. [*Ramy Cyberbezpieczeństwa:* **ID.AM-5**]

Zadania	Wyniki
ZADANIE P-13 **CYKL ŻYCIA INFORMACJI**	• Dla każdego rodzaju informacji przetwarzanej przez system, identyfikowane i interpretowane są wszystkie etapy cyklu życia tych informacji. [*Ramy Cyberbezpieczeństwa:* **ID.AM-3**; **ID.AM-4**]
ZADANIE P-14 **SYSTEM SZACOWANIA RYZYKA**	• Szacowanie ryzyka na poziomie systemu jest zakończone lub istniejące szacowanie ryzyka jest aktualizowane. [*Ramy Cyberbezpieczeństwa:* **ID.RA; ID.SC-2**]
ZADANIE P-15 **DEFINICJA WYMAGAŃ**	• Zdefiniowane są i uszeregowane pod względem ważności wymagania dotyczące bezpieczeństwa i ochrony prywatności. [Ramy Cyberbezpieczeństwa: ID.GV; PR.IP]
ZADANIE P-16 **ARCHITEKTURA KORPORACYJNA**	• Określone jest umiejscowienie systemu w architekturze korporacyjnej.
ZADANIE P-17 **PRZYDZIAŁ WYMAGAŃ**	• Wymagania dotyczące bezpieczeństwa i ochrony prywatności są przypisane do systemu i środowiska, w którym system działa. [*Ramy Cyberbezpieczeństwa:* **ID.GV**]

Zadania	Wyniki
ZADANIE P-18 **REJESTRACJA SYSTEMU**	• System jest zarejestrowany zgodnie z celami zarządzania, odpowiedzialności, koordynacji i nadzoru. [*Ramy Cyberbezpieczeństwa:* **ID.GV**]

MISJA LUB PRZEDMIOT DZIAŁANIA

ZADANIE P-8 Określenie misji, funkcji biznesowych oraz procesów biznesowych, które system ma wspierać.

Potencjalne dane wejściowe: Misja organizacyjna; polityka organizacyjna; informacje o misji/procesie biznesowym; informacje o interesariuszach systemu; Profile Ram Cyberbezpieczeństwa; żądania przedłożenia wniosku lub innych dokumentów dotyczących nabycia; koncepcja działania.

Oczekiwane wyniki: Misje, funkcje biznesowe i procesy biznesowe, które będą wspierane przez system.

Podstawowa odpowiedzialność: BO.

Role wspierające: AO lub AODR; SO; IO/S; CIO; SAISO; SAOP.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Misje organizacji i funkcje biznesowe wpływają na projektowanie i rozwój misji lub procesów biznesowych, które są tworzone w celu realizacji tych misji i funkcji biznesowych. Priorytety misji i funkcji biznesowych wpływają na strategie inwestycyjne, decyzje o finansowaniu, priorytetyzację zasobów i decyzje w zakresie ryzyka, a tym samym na istniejącą architekturę korporacyjną i rozwój związanej z nią architektury bezpieczeństwa

i ochrony prywatności. Informacje są pozyskiwane od interesariuszy w celu uzyskania dokładniejszego zrozumienia misji, funkcji biznesowych i procesów biznesowych organizacji z punktu widzenia bezpieczeństwa systemu i ochrony prywatności.

Referencje: [SP 800-39] (Poziomy organizacji i misji/procesów biznesowych); [SP 800-64]; [SP 800-160] (Analiza działalności lub misji, zarządzanie portfelem i procesy planowania projektów); [CSF NIST] (Podstawowe [Funkcja identyfikacji]); [IR 8179] (Proces analizy krytyczności B).

INTERESARIUSZE SYSTEMU

ZADANIE P-9 Określenie podmiotów, które są zainteresowane zaprojektowaniem, opracowaniem, wdrożeniem, oceną, eksploatacją, utrzymaniem lub wycofaniem systemu.

Potencjalne dane wejściowe: Misja organizacji; cele biznesowe; funkcje biznesowe i procesy biznesowe, które będą wspierane przez system; inne informacje dotyczące misji/procesów biznesowych; bezpieczeństwo organizacji i polityka ochrony prywatności oraz procedury; schematy organizacyjne; informacje o osobach lub grupach (wewnętrznych i zewnętrznych), które są zainteresowane systemem i ponoszą za niego odpowiedzialność decyzyjną.

Oczekiwane wyniki: Lista interesariuszy systemu.

Podstawowa odpowiedzialność: BO, SO.

Role wspierające: CIO; AO lub AODR; IO/S; SAISO; SAOP; CAO.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Interesariuszami są osoby, organizacje lub ich przedstawiciele, którzy są zainteresowani systemem w całym cyklu jego życia obejmującym projektowanie, opracowywanie, wdrażanie, dostarczanie, funkcjonowanie i utrzymanie. Identyfikacja interesariuszy obejmuje również wszystkie aspekty łańcucha dostaw. Interesariusze mogą

znajdować się w tej samej organizacji lub mogą pochodzić z innych organizacji, w sytuacjach, gdy organizacje te mają wspólny interes dotyczący systemu informatycznego. Na przykład, może to mieć miejsce podczas opracowywania, funkcjonowania i utrzymywania systemów opartych na chmurze, systemów usług wspólnych lub każdego systemu, na który organizacje mogą mieć niekorzystny wpływ z powodu naruszenia lub ujawnienia w systemie, lub z różnorodnych przyczyn odnoszących się do łańcucha dostaw. Komunikacja między zainteresowanymi stronami jest ważna na każdym etapie realizacji RMF i w całym SDLC, aby zapewnić spełnienie wymogów bezpieczeństwa i ochrony prywatności, szybkie rozwiązywanie problemów i wątpliwości oraz skuteczną realizację procesów zarządzania ryzykiem.

Referencje: [SP 800-39] (poziom organizacji); [SP 800-64]; [SP 800-160] (definiowanie potrzeb i wymagań zainteresowanych stron oraz procesy zarządzania portfelem); [SP 800-161]; [CSF NIST] (podstawowa [funkcja identyfikacji]).

IDENTYFIKACJA AKTYWÓW

ZADANIE P-10 Identyfikacja aktywów, które wymagają ochrony.

Potencjalne dane wejściowe: Misje, funkcje biznesowe i procesy biznesowe, które będą wspierane przez system informatyczny; analizy wpływu na działalność; interesariusze wewnętrzni; informacje o zewnętrznych interesariuszach systemu; informacje o innych systemach, które współdziałają z danym systemem.

Oczekiwane wyniki: Zestaw aktywów, które mają być chronione.

Podstawowa odpowiedzialność: SO.

Role wspierające: AO lub AODR; BO; IO/S; SAISO; SAOP; SA.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Aktywa są materialnymi i niematerialnymi składnikami majątku, które mają wartość dla realizacji misji lub celów biznesowych. Rzeczowe aktywa trwałe mają charakter fizyczny i obejmują elementy fizyczne/środowiskowe (np. informacje w postaci papierowej; struktury; obiekty), ludzi oraz elementy technologiczne / maszynowe (np. elementy sprzętowe, mechanizmy i sieci). Natomiast wartości niematerialne i prawne nie mają charakteru fizycznego i obejmują misję i procesy biznesowe, funkcje, informacje i dane cyfrowe, oprogramowanie sprzętowe (*ang. firmware*), oprogramowanie i usługi. Aktywa informacyjne mogą mieć charakter materialny lub niematerialny i mogą obejmować informacje niezbędne do realizacji misji lub funkcji biznesowych, świadczenia usług oraz zarządzania/operacji systemu, nadzorowane informacje jawne i informacje wrażliwe oraz wszelkie formy dokumentacji związane z systemem informatycznym. Wartości niematerialne mogą również obejmować wizerunek lub reputację organizacji oraz interesy prywatności osób, których informacje będą przetwarzane przez system. Organizacja określa zakres aktywów zainteresowanych stron, które należy uwzględnić w celu ich ochrony. Aktywa, które wymagają ochrony, są identyfikowane na podstawie obaw interesariuszy i kontekstu, w którym aktywa te są wykorzystywane. Obejmuje to misje lub funkcje biznesowe organizacji, inne systemy, które współdziałają z systemem oraz interesariuszy, których aktywa są wykorzystywane przez misję lub funkcje biznesowe lub przez system. Aktywa mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu.

Referencje: [SP 800-39] (poziom organizacji); [SP 800-64]; [SP 800-160] (proces definiowania potrzeb interesariuszy i wymagań); [IR 8179] (proces analizy krytyczności C); [NIST CSF] (podstawowy [funkcja identyfikacji]); [NARA CUI].

GRANICA AUTORYZACJI

ZADANIE P-11 Ustalenie granicy autoryzacji systemu.

Potencjalne dane wejściowe: Dokumentacja projektowa systemu; schematy sieci; informacje o interesariuszach systemu; informacje o zasobach; schematy architektury sieci i/lub architektury korporacyjnej; struktura organizacyjna (wykresy, informacje).

Oczekiwane wyniki: Udokumentowana granica autoryzacji systemu.

Podstawowa odpowiedzialność: AO.

Role wspierające: CIO; SO; BO; SAISO; SAOP; EA.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Granice autoryzacji określają zakres ochrony systemów informatycznych (tj. to, co organizacja zgadza się chronić pod swoją kontrolą zarządczą lub w ramach swoich obowiązków). Granice autoryzacji są ustalane przez upoważnione osoby z udziałem właściciela systemu w oparciu o misję, zarządzanie lub odpowiedzialność budżetową (zob. Załącznik F). Jasne wyznaczenie granic autoryzacji jest ważne dla rozliczlności i kategoryzacji bezpieczeństwa, szczególnie w sytuacjach, gdy systemy o mniejszym wpływie są połączone z systemami o większym wpływie lub gdy za działanie lub konserwację systemu odpowiedzialni są dostawcy zewnętrzni. Każdy system składa się z zestawu elementów (tj. zasobów informatycznych)[64] zorganizowanych w celu osiągnięcia jednego lub więcej celów oraz wsparcia misji i procesów biznesowych organizacji. Każdy element systemu jest wdrażany w sposób, który pozwala organizacji spełnić określone wymagania w zakresie bezpieczeństwa i ochrony prywatności. Do elementów systemu zalicza się ludzi, elementy technologiczne/maszynowe oraz fizyczne/środowiskowe.

[64] Elementy systemu są wdrażane za pomocą sprzętu, aplikacji lub oprogramowania układowego (*ang. Firmware*); fizycznych struktur lub urządzeń; lub ludzi, procesów i procedur. Termin "komponent systemu" oznacza elementy systemu, które są wdrażane konkretnie za pomocą sprzętu, oprogramowania i oprogramowania sprzętowego.

Termin *system* jest używany do określenia zestawu elementów systemu, wzajemnych połączeń elementów systemu oraz środowiska, na którym koncentruje się realizacja RMF (zob. rys. 5). System jest ujęty w jednej granicy autoryzacji, aby zapewnić rozliczalność. W przypadku systemów przetwarzających dane osobowe, programy ochrony prywatności i bezpieczeństwa współpracują w celu wypracowania wspólnego rozumienia granic autoryzacji. Aby przeprowadzić skuteczne szacowanie ryzyka i wybrać odpowiednie zabezpieczenia, programy ochrony prywatności i bezpieczeństwa zapewniają jasne i spójne zrozumienie, co stanowi granicę autoryzacji. Zrozumienie granic autoryzacji i tego, co będzie się działo poza nimi, może mieć wpływ na wybrane mechanizmy zabezpieczeń i sposób ich wdrażania. Na przykład, jeżeli funkcja systemu obejmuje udostępnianie danych osobowych na zewnątrz, dla tych danych przesyłanych z systemu należy wybrać niezawodne zabezpieczenia w postaci szyfrowania.

Podobnie, w przypadku systemów częściowo lub w całości zarządzanych, utrzymywanych lub obsługiwanych przez dostawców zewnętrznych, umowa wyraźnie opisująca granice autoryzacji zapewnia rozliczalność. Programy ochrony prywatności i bezpieczeństwa są realizowane we współpracy z dostawcami w celu wypracowania wspólnego rozumienia granic autoryzacji. Formalne umowy z zewnętrznymi dostawcami powinny być wykorzystane do określenia, co stanowi granice autoryzacji. Zrozumienie takich granic ułatwia wybór odpowiednich środków bezpieczeństwa do zarządzania ryzykiem w łańcuchu dostaw.

Referencje: [NSC 800-18]; [SP 800-39] (poziom systemu); [SP 800-47]; [SP 800-64]; [SP 800-160 cz. 1] (proces definiowania wymagań systemowych); [NIST CSF] (podstawowy [funkcja identyfikacji]).

TYP INFORMACJI

ZADANIE P-12 Określanie typów informacji, które mają być przetwarzane, przechowywane i przekazywane przez system.

Potencjalne dane wejściowe: Dokumentacja projektowa systemu; aktywa, które mają być chronione; informacje o zadaniach / procesach biznesowych; dokumentacja projektowa systemu.

Oczekiwane wyniki: Lista rodzajów informacji przetwarzanych w systemie.

Podstawowa odpowiedzialność: SO; IO/S.

Rola wspierająca: BO; SSO; SPO[65].

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Identyfikacja typów informacji potrzebnych do wsparcia misji organizacyjnych, funkcji biznesowych oraz procesów misyjnych/biznesowych jest ważnym krokiem w tworzeniu planów bezpieczeństwa i ochrony prywatności dla systemu oraz warunkiem wstępnym do określenia kategoryzacji bezpieczeństwa. [NARA CUI][66] definiuje typy informacji, które wymagają ochrony, jako część swojego programu Nadzorowanych Informacji Jawnych (*ang. Controlled Unclassified Information - CUI*), zgodnie z przepisami ustawowymi, wykonawczymi lub obowiązującymi zasadami. Organizacje mogą definiować dodatkowe typy informacji potrzebne do obsługi misji organizacyjnych, funkcji biznesowych i procesów biznesowych, które nie są zdefiniowane w rejestrze CUI[67] lub w dokumencie [NSC 800-60 cz. 1]. Zidentyfikowane typy informacji są potwierdzane przez właścicieli lub administratorów informacji i dokumentowane w planach bezpieczeństwa i ochrony prywatności systemu.

Referencje: [OMB A-130]; [NARA CUI]; [SP 800-39] (poziom systemu); [NSC 800-60 cz. 1]; [NSC 800-60 cz. 2]; [NIST CSF] (podstawowy [funkcja identyfikacji]).

[65] SPO w systemie jest podstawową rolą, gdy system informatyczny przetwarza informacje z zakresu danych osobowych.
[66] Podano jako przykład, mało adekwatny do polskich realiów.
[67] j.w.

CYKL ŻYCIA INFORMACJI

ZADANIE P-13 Określenie i zrozumienie wszystkich etapów cyklu życia informacji dla każdego typu informacji przetwarzanych, przechowywanych lub przesyłanych przez system.

Potencjalne dane wejściowe: Misje, funkcje biznesowe i procesy biznesowe, które będą wspierane przez system; informacje o interesariuszach systemu; informacje o granicach autoryzacji; informacje o innych systemach, które współdziałają z systemem (np. umowy dotyczące wymiany informacji/połączeń); dokumentacja projektowa systemu; informacje o elementach systemu; lista typów informacji systemowych.

Oczekiwane wyniki: Dokumentacja etapów, przez które informacje przechodzą w systemie, np. mapa danych lub model ilustrujący strukturę lub sposób przetwarzania informacji przez system w całym cyklu życia. Dokumentacja taka obejmuje, na przykład, schematy przepływu danych, schematy powiązań między jednostkami, schematy baz danych oraz słowniki danych.

Podstawowa odpowiedzialność: SAOP; SO; IO/S.

Role wspierające: CIO; BO; SecA; PA; EA; PA, SSE, PE.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Cykl życia informacji opisuje etapy, przez które przechodzą informacje, zwykle określane, jako tworzenie lub zbieranie, przetwarzanie, rozpowszechnianie, wykorzystywanie, przechowywanie i dyspozycje, w tym niszczenie i usuwanie. Identyfikacja i zrozumienie sposobu, w jaki każdy rodzaj informacji jest przetwarzany na wszystkich etapach cyklu życia, pomaga organizacjom określić ustalenia dotyczące ochrony informacji, informuje o ocenie ryzyka dla bezpieczeństwa i prywatności organizacji oraz informuje o wyborze i wdrożeniu środków bezpieczeństwa. Identyfikacja i zrozumienie cyklu życia informacji ułatwia stosowanie praktyk pomagających zapewnić, na przykład, że organizacje

mają uprawnienia do gromadzenia lub tworzenia informacji, opracowywania zasad związanych z przetwarzaniem informacji zgodnie z poziomem ich oddziaływania, tworzenia umów o wymianie informacji oraz przestrzegania harmonogramów przechowywania i dysponowania informacjami.

Korzystanie z narzędzi takich jak mapa danych umożliwia organizacjom zrozumienie, w jaki sposób przetwarzane są informacje, tak, aby mogły one lepiej ocenić, gdzie mogą pojawić się zagrożenia dla bezpieczeństwa i prywatności oraz w jakich przypadkach można najskuteczniej stosować zabezpieczenia. Ważne jest, aby organizacje rozważyły odpowiednie wyznaczenie granicy autoryzacji i interakcji systemu informatycznego z innymi systemami, ponieważ sposób, w jaki informacja wchodzi do systemu i z niego wychodzi, może mieć wpływ na ocenę ryzyka dla bezpieczeństwa i prywatności. Elementy systemu są identyfikowane z dostateczną dokładnością, aby wspierać takie szacowanie ryzyka.

Zidentyfikowanie i zrozumienie cyklu życia informacji jest szczególnie istotne dla oceny zagrożeń dla bezpieczeństwa i prywatności, ponieważ informacje mogą być przetwarzane przez system w każdej z faz SDLC. Na przykład, w fazie testowania i integracji SDLC, przetwarzanie rzeczywistych (tj. „żywych") danych prawdopodobnie zwiększyłoby ryzyko związane z bezpieczeństwem i prywatnością, ale wykorzystanie zastępczych (tj. symulowanych) danych może umożliwić uzyskanie równoważnych korzyści w zakresie testowania systemu przy jednoczesnym ograniczeniu ryzyka.

Referencje: [OMB A-130]; [OMB M-13-13]; [NARA RECM]; [NIST CSF] (podstawowy [funkcja identyfikacji]); [IR 8062].

SYSTEM SZACOWANIA RYZYKA

ZADANIE P-14 Szacowanie ryzyka na poziomie systemu i bieżąca aktualizacja wyników szacowania ryzyka.

Potencjalne dane wejściowe: Aktywa, które mają być chronione; misje, funkcje biznesowe i procesy biznesowe, które będą wspierane przez system; analizy wpływu biznesowego lub

analizy krytyczności; informacje o interesariuszach systemu; informacje o innych systemach, które współdziałają z systemem; informacje o dostawcach; informacje o zagrożeniach; mapa danych; dokumentacja projektowa systemu; Profile Ram Cyberbezpieczeństwa; strategia zarządzania ryzykiem; wyniki szacowania ryzyka na poziomie organizacji.

Oczekiwane wyniki: Raporty z oceny zagrożeń bezpieczeństwa i prywatności.

Podstawowa odpowiedzialność: SO; SSO; SPO.

Role wspierające: SAORM lub RE; AO lub AODR; BO; IO/S; CA.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Zadanie to może wymagać od organizacji przeprowadzenia szacowania ryzyka związanego z bezpieczeństwem i prywatnością w celu zapewnienia, że każdy rodzaj ryzyka jest w pełni oceniany. Szacowanie ryzyka bezpieczeństwa obejmuje identyfikację źródeł zagrożeń[68] i zdarzeń zagrażających aktywom, określenie, czy i w jaki sposób aktywa są podatne na zagrożenia, prawdopodobieństwo, że podatność aktywów na zagrożenia zostanie wykorzystana przez zagrożenie oraz wpływ (lub konsekwencje) utraty aktywów. Jako kluczowy element szacowania ryzyka, aktywa są uszeregowane pod względem ważności na podstawie negatywnego wpływu lub konsekwencji utraty aktywów. Znaczenie straty jest definiowane dla każdego rodzaju aktywów, aby umożliwić określenie konsekwencji straty (tj. negatywnego wpływu straty). Konsekwencje strat mogą być materialne (np. straty pieniężne, przemysłowe) lub niematerialne (np. reputacja) i stanowią ciągłość, która rozciąga się od częściowej straty do całkowitej straty w odniesieniu do danego składnika aktywów. Interpretacja utraty informacji może obejmować, na przykład, utratę posiadania, zniszczenie lub utratę precyzji lub dokładności. Utrata funkcji lub usługi może być interpretowana, jako utrata kontroli, utrata dostępności, utrata zdolności do zapewnienia normalnej funkcji,

[68] Wykorzystanie wiedzy o zagrożeniach, analiza i modelowanie zagrożeń może pomóc organizacjom rozwinąć zdolności w zakresie bezpieczeństwa niezbędne do zmniejszenia podatności organizacji na różne zagrożenia, w tym wrogie cyberataki, awarie sprzętu, klęski żywiołowe oraz błędy przeoczeń i zamówień.

wydajności lub zachowania, lub ograniczona utrata zdolności powodująca poziom degradacji funkcji, wydajności lub zachowania. Fizyczne konsekwencje naruszenia mogą obejmować nieplanowane przestoje w produkcji, uszkodzenia urządzeń przemysłowych, straty w organizacji, katastrofy ekologiczne i zagrożenia dla bezpieczeństwa publicznego. Priorytetowość aktywów opiera się na ich wartości, konsekwencjach fizycznych, kosztach wymiany, krytyczności, wpływie na wizerunek lub reputację, zaufaniu użytkowników, organizacji współpracujących, misji lub partnerów biznesowych. Priorytet aktywów przekłada się na pierwszeństwo w alokacji zasobów, określaniu siły mechanizmów i określaniu poziomów pewności.

Szacowanie ryzyka w zakresie ochrony prywatności przeprowadza się w celu określenia prawdopodobieństwa, że dana operacja, którą system podejmuje podczas przetwarzania danych osobowych, może mieć niekorzystne oddziaływanie i potencjalny wpływ na osoby fizyczne. Te niekorzystne skutki mogą wynikać z nieautoryzowanych działań, które prowadzą do utraty poufności, integralności lub dostępności w systemach informatycznych przetwarzających informacje z zakresu danych osobowych, lub mogą powstać, jako produkt uboczny autoryzowanych działań. Na ocenę ryzyka w zakresie ochrony prywatności mają wpływ czynniki kontekstowe. Czynniki kontekstowe mogą obejmować między innymi poziom wrażliwości danych osobowych, w tym określone elementy lub łącznie; rodzaje organizacji wykorzystujących system lub wchodzących w interakcję z nim oraz postrzeganie organizacji przez osoby fizyczne w odniesieniu do prywatności; zrozumienie przez osoby fizyczne charakteru i celu przetwarzania danych; a także interesy ochrony prywatności osób fizycznych, wiedzę techniczną lub cechy demograficzne, które wpływają na ich zrozumienie lub zachowanie. Zagrożenia dla prywatności osób fizycznych mogą wpływać na ich decyzje dotyczące korzystania z systemu, wpływając tym samym na misję lub cele biznesowe, lub tworzyć odpowiedzialność prawną, ryzyko utraty reputacji lub inne rodzaje ryzyka dla organizacji. Skutki dla organizacji nie stanowią zagrożenia dla prywatności. Niemniej jednak, wpływy te mogą stanowić wskazówkę i źródło informacji przy podejmowaniu decyzji w organizacji oraz wpływać na priorytety i alokację zasobów do reagowania na ryzyko.

Szacowanie ryzyka przeprowadza się również w celu ustalenia, czy wykorzystanie zewnętrznego dostawcy w celu opracowania, wdrożenia, utrzymania, zarządzania, eksploatacji lub dysponowania systemem, elementem systemu lub usługą może spowodować stratę, a także potencjalnego wpływu tej straty. Wpływ ten może być natychmiastowy (np. kradzież fizyczna) lub trwający (np. zdolność przeciwników do replikowania sprzętu krytycznego z powodu kradzieży). Wpływ może mieć charakter endemiczny (np. ograniczony do pojedynczego systemu) lub systemowy (np. obejmujący dowolny system wykorzystujący określony rodzaj elementu systemu). Szacowanie ryzyka łańcucha dostaw uwzględnia podatności, które mogą pojawić się w związku z rozmieszczeniem systemu lub elementu systemu oraz w wyniku korzystania z usług dostawców zewnętrznych. Podatności w łańcuchu dostaw mogą obejmować brak identyfikowalności lub odpowiedzialności, co może prowadzić do potencjalnego wykorzystania podróbek, wprowadzania złośliwego oprogramowania lub systemów złej jakości. Korzystanie z usług dostawców zewnętrznych może prowadzić do utraty identyfikowalności i kontroli nad sposobem opracowywania, wdrażania i utrzymywania systemów, elementów systemu i usług. Jasne zrozumienie zagrożeń, podatności i potencjalnych skutków niepożądanego zdarzenia w łańcuchu dostaw może pomóc organizacjom odpowiednio zrównoważyć ryzyko związane z łańcuchem dostaw z tolerancją ryzyka. Szacowanie ryzyka w łańcuchu dostaw może obejmować informacje pochodzące z audytów, przeglądów i wywiadów z dostawcami. Organizacje opracowują strategię gromadzenia informacji, w tym strategię współpracy z dostawcami w zakresie szacowania ryzyka w łańcuchu dostaw. Taka współpraca pomaga organizacjom wykorzystać informacje od dostawców, ograniczyć zwolnienia, określić potencjalne kierunki działań w zakresie reagowania na ryzyko oraz zmniejszyć obciążenie dostawców.

Szacowanie ryzyka jest przeprowadzane w ramach SDLC i wspieraj różne etapy i zadania RMF. Wyniki szacowania ryzyka są wykorzystywane do definiowania wymogów bezpieczeństwa i ochrony prywatności, podejmowania decyzji kategoryzacyjnych, wyboru, dostosowania, wdrożenia i oceny zabezpieczeń, decyzji autoryzacyjnych, potencjalnych

kierunków działań i ustalania priorytetów reakcji na ryzyko oraz strategii ciągłego monitorowania. Organizacje określają formę prowadzonego szacowania ryzyka (w tym zakres, rygor i formalność takich ocen) oraz sposób raportowania wyników.

Referencje: [NSC 199]; [NSC 200]; [NSC 800-30]; [SP 800-39] (poziom organizacji); [SP 800-59]; [NSC 800-60 cz. 1]; [NSC 800-60 cz. 2]; [SP 800-64]; [SP 800-160 cz. 1] (Potrzeby interesariuszy i definiowanie wymogów oraz procesy zarządzania ryzykiem); [SP 800-161] (Ocena); [IR 8062]; [IR 8179]; [NIST CSF] (Podstawowa [Funkcja identyfikacji]); [CNSSI 1253].

DEFINICJA WYMAGAŃ

ZADANIE P-15 Zdefiniowanie wymagań dotyczących bezpieczeństwa i ochrony prywatności systemu oraz środowiska pracy.

Potencjalne dane wejściowe: Dokumentacja projektowa systemu; wyniki szacowania ryzyka na poziomie organizacji i systemu; znany zestaw aktywów interesariuszy, który ma być chroniony; misje, funkcje biznesowe i procesy biznesowe, które będą wspierane przez system; analizy wpływu biznesowego lub analizy krytyczności; informacje o interesariuszach systemu; mapa cyklu życia informacji dotyczących danych osobowych; Profile Ram Cyberbezpieczeństwa; informacje o innych systemach, które współdziałają z systemem; informacje o zagrożeniach; ustawy, zarządzenia, dyrektywy, rozporządzenia lub zasady mające zastosowanie do systemu; strategia zarządzania ryzykiem.

Oczekiwane wyniki: Udokumentowane wymagania dotyczące bezpieczeństwa i ochrony prywatności.

Podstawowa odpowiedzialność: BO; SO; IO/S; SPO.[69]

Role wspierające: AO lub AODR; SSO; SAISO; SAOP; CAO; SA; PA; EA.

[69] SPO w systemie pełni podstawową rolę tylko wtedy, gdy system informatyczny przetwarza informacje z zakresu danych osobowych.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Potrzeby w zakresie ochrony są wyrazem zdolności ochrony wymaganej przez system w celu zmniejszenia ryzyka w zakresie bezpieczeństwa i prywatności do akceptowalnego poziomu przy jednoczesnym wspieraniu misji lub potrzeb biznesowych. Potrzeby w zakresie ochrony obejmują charakterystykę bezpieczeństwa systemu [70] oraz jego zachowania w zakresie bezpieczeństwa w zakładanym środowisku operacyjnym oraz we wszystkich fazach cyklu życia systemu. Potrzeby w zakresie ochrony odzwierciedlają priorytety zainteresowanych stron, wyniki negocjacji między stronami w odpowiedzi na konflikty, różne priorytety, sprzeczności i określone cele, a zatem są z natury subiektywne. Potrzeby w zakresie ochrony są udokumentowane, aby pomóc w zapewnieniu, że rozumowanie, założenia i ograniczenia związane z tymi potrzebami są dostępne do wykorzystania w przyszłości oraz aby zapewnić identyfikowalność wymogów w zakresie bezpieczeństwa i prywatności. Wymagania dotyczące bezpieczeństwa i ochrony prywatności [71] stanowią formalne, bardziej szczegółowe wyrażenie potrzeb w zakresie ochrony we wszystkich fazach SDLC, związanych z nimi procesach cyklu życia oraz ochronie aktywów związanych z systemem. Wymagania dotyczące bezpieczeństwa i ochrony prywatności są uzyskiwane z wielu źródeł (np. ustaw, rozporządzeń wykonawczych, dyrektyw, regulacji, polityk, standardów, misji i potrzeb biznesowych lub ocen ryzyka). Wymagania dotyczące bezpieczeństwa i ochrony prywatności są ważną częścią formalnego określania wymaganej charakterystyki systemu. [72] Wymagania dotyczące bezpieczeństwa

[70] Na przykład, podstawową cechą bezpieczeństwa jest to, że system wykazuje tylko określone zachowania, interakcje i wyniki.

[71] Termin wymagania może mieć określone znaczenie. Na przykład, wymogi prawne nakładają obowiązki, do których muszą się stosować organizacje. Wymagania dotyczące bezpieczeństwa i ochrony prywatności wynikają jednak z potrzeb ochrony systemu, a te potrzeby ochrony mogą wynikać z wymogów prawnych, misji lub potrzeb biznesowych, szacowania ryzyka lub innych źródeł.

[72] Wymagania dotyczące bezpieczeństwa i ochrony prywatności mogą również obejmować wymagania dotyczące gwarancji. Gwarancja to pewność, co do zdolności systemu do zachowania wiarygodności w zakresie bezpieczeństwa i prywatności w odniesieniu do wszystkich form przeciwności losu wynikających ze złośliwych lub niezłośliwych intencji.

i ochrony prywatności kierują i informują o wyborze zabezpieczeń systemu i działaniach związanych z tymi zabezpieczeniami.

Organizacje mogą wykorzystywać Ramy Cyberbezpieczeństwa do zarządzania wymaganiami bezpieczeństwa i ochrony prywatności oraz wyrażać te wymagania w zdefiniowanych dla organizacji *profilach* Ram Cyberbezpieczeństwa. Na przykład, wielokrotne wymagania mogą być ujednolicone, a nawet pozbawione sprzeczności, przy użyciu struktury funkcji-kategorii-podkategorii rdzenia ramowego. Profile mogą być następnie wykorzystywane do informowania o rozwoju dostosowanych organizacyjnie poziomów odniesienia zabezpieczeń opisanych w kroku *Poziom przygotowania organizacji* RMF, Zadanie P-4.

Referencje: [SP 800-39] (poziom organizacji); [SP 800-64]; [SP 800-160 cz. 1] (proces definiowania potrzeb interesariuszy i wymagań); [SP 800-161] (wielopoziomowe zarządzanie ryzykiem); [IR 8179]; [CSF NIST] (podstawowe [funkcje ochrony, wykrywania, reagowania, odzyskiwania]; profile).

ARCHITEKTURA KORPORACYJNA

ZADANIE P-16 Ustalenie umiejscowienia systemu w architekturze korporacyjnej.

Potencjalne dane wejściowe: Wymagania dotyczące bezpieczeństwa i ochrony prywatności; wyniki szacowania ryzyka na poziomie organizacji i systemu; informacje dotyczące architektury korporacyjnej; informacje dotyczące architektury bezpieczeństwa; informacje dotyczące architektury prywatności; informacje dotyczące aktywów.

Oczekiwane wyniki: Zaktualizowana architektura korporacyjna; zaktualizowana architektura bezpieczeństwa; zaktualizowana architektura prywatności; plany wykorzystania systemów w chmurze i systemów współdzielonych, usług lub aplikacji.

Podstawowa odpowiedzialność: BO; EA; SA; PA.

Role wspierające: CIO; AO lub AODR; SAISO; SAOP; SO; IO/S.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Architektura korporacyjna to praktyka zarządzania stosowana w celu maksymalizacji efektywności procesów biznesowych i zasobów informacyjnych oraz osiągnięcia misji i sukcesu biznesowego. Architektura korporacyjna może zapewnić lepsze zrozumienie technologii informatycznych i operacyjnych zawartych we wstępnym projekcie i rozwoju systemów informatycznych oraz jest warunkiem wstępnym osiągnięcia odporności i zdolności przetrwania tych systemów w środowisku coraz bardziej wyrafinowanych zagrożeń. Architektura korporacyjna daje również organizacjom możliwość konsolidacji, standaryzacji i optymalizacji zasobów informacyjnych i technologicznych. Skutecznie wdrożona architektura tworzy systemy, które są bardziej przejrzyste, a przez to łatwiejsze do zrozumienia i ochrony. Architektura korporacyjna tworzy również jednoznaczny związek między inwestycjami, a wymiernymi usprawnieniami wydajności. Umieszczenie systemu w architekturze korporacyjnej jest ważne, ponieważ zapewnia większą przejrzystość i zrozumienie innych systemów (wewnętrznych i zewnętrznych), które są z nim połączone, a także może być wykorzystane do ustanowienia domen bezpieczeństwa dla zwiększenia poziomu ochrony systemu.

Architektura bezpieczeństwa i architektura prywatności są integralną częścią architektury korporacyjnej. Architektury te reprezentują części architektury korporacyjnej związane z wdrażaniem wymagań dotyczących bezpieczeństwa i ochrony prywatności. Podstawowym celem architektury bezpieczeństwa i prywatności jest zapewnienie, że wymagania dotyczące bezpieczeństwa i ochrony prywatności są konsekwentnie i ekonomicznie spełniane w systemach organizacyjnych i są zgodne ze strategią zarządzania ryzykiem. Architektura bezpieczeństwa i prywatności stanowi mapę drogową, która ułatwia śledzenie drogi od strategicznych celów i zadań organizacji, poprzez potrzeby ochrony i wymagania dotyczące bezpieczeństwa i prywatności, po konkretne rozwiązania w zakresie bezpieczeństwa i ochrony prywatności dostarczane przez ludzi, procesy i technologie.

Referencje: [SP 800-39] (poziom procesu misji/procesu biznesowego); [SP 800-64]; [SP 800-160 cz. 1] (proces definiowania wymagań systemowych); [NIST CSF] (podstawowe [funkcja identyfikacji]; profile); [OMB FEA].

PRZYDZIAŁ WYMAGAŃ

ZADANIE P-17 Przydzielenie wymagań dotyczących bezpieczeństwa i ochrony prywatności do systemu i środowiska pracy.

Potencjalne dane wejściowe: Wyniki szacowania ryzyka na poziomie organizacji i systemu; udokumentowane wymagania dotyczące bezpieczeństwa i ochrony prywatności; wyniki szacowania ryzyka na poziomie organizacji i systemu; lista dostawców wspólnych zabezpieczeń i dostępnych dla dziedziczenia wspólnych zabezpieczeń; opis systemu; informacje o elementach systemu; spis elementów systemu; odpowiednie ustawy, rozporządzenia, dyrektywy, rozporządzenia i polityki.

Oczekiwane wyniki: Lista wymagań bezpieczeństwa i ochrony prywatności przypisanych do systemu, elementów systemu i środowiska pracy.

Podstawowa odpowiedzialność: SA; PA; SSO; SPO.

Role wspierające: CIO; AO lub AODR; BO; SAISO; SAOP; SO.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Wymagania dotyczące bezpieczeństwa i ochrony prywatności są przypisywane w celu kierowania i informowania o wyborze i wdrożeniu zabezpieczeń organizacji, systemu, elementów systemu i/lub środowiska pracy.[73] Przydział wymagań określa, gdzie będą wdrażane zabezpieczenia. Alokacja wymagań chroni zasoby i pomaga usprawnić proces

[73] Środowisko pracy systemu informatycznego odnosi się do fizycznego otoczenia, w którym system przetwarza informacje. Na przykład, wymogi bezpieczeństwa są przypisane do obiektów, w których system jest zlokalizowany i działa. Te wymogi bezpieczeństwa mogą być spełnione przez środki bezpieczeństwa fizycznego [NSC 800-53].

zarządzania ryzykiem poprzez zapewnienie, że wymagania nie są wdrażane na wielu systemach lub elementach systemu, gdy wdrożenie wspólnego zabezpieczenia lub zabezpieczenia systemowego na konkretnym elemencie systemu zapewnia wymaganą zdolność ochrony.

Referencje: [SP 800-39] (Organizacja, zadania/proces biznesowy oraz poziomy systemu); [SP 800-64]; [SP 800-160 cz. 1] (proces definiowania wymagań systemowych); [NIST CSF] (podstawowe [funkcja identyfikacji]; profile); [OMB FEA].

REJESTRACJA SYSTEMU

ZADANIE P-18 Rejestracja systemu w ewidencji systemów.

Potencjalne dane wejściowe: Polityka organizacyjna w zakresie rejestracji systemu; informacje o systemie.

Oczekiwane wyniki: Zarejestrowany system zgodnie z polityką organizacyjną.

Podstawowa odpowiedzialność: SO.

Rola wspierająca: BO; CIO; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Rejestracja systemu, zgodnie z polityką organizacyjną, służy do informowania organizacji zarządzającej o planach rozwoju systemu lub o istnieniu systemu; o kluczowych cechach systemu; oraz o spodziewanych skutkach dla bezpieczeństwa i ochrony prywatności organizacji wynikających z działania i użytkowania systemu. Rejestracja systemu zapewnia organizacjom narzędzie do zarządzania i śledzenia, ułatwiające wprowadzenie systemu do architektury korporacyjnej, wdrożenie zabezpieczeń współmiernych do ryzyka oraz raportowanie pozycji bezpieczeństwa i prywatności zgodnie z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, politykami lub normami. W ramach procesu rejestracji systemu, organizacje dodają system do organizacyjnej inwentaryzacji systemu.

Informacje dotyczące rejestracji systemu są aktualizowane o informacje dotyczące kategoryzacji bezpieczeństwa i charakterystyki systemu po zakończeniu etapu *kategoryzacji.*

Referencje: Brak.

3.2 KATEGORYZACJA[74]

CEL

Celem etapu ***Kategoryzacja*** jest informowanie o procesach i zadaniach zarządzania ryzykiem organizacyjnym poprzez określenie negatywnego wpływu na działania i aktywa organizacji, osób, innych organizacji i Państwa w odniesieniu do utraty poufności, integralności i dostępności systemów organizacyjnych oraz informacji przetwarzanych, przechowywanych i przekazywanych przez te systemy.

KATEGORYZACJA ZADAŃ

Tabela 3 zawiera podsumowanie zadań i oczekiwanych wyników dla etapu *kategoryzacji* RMF.

Przedstawiono również obowiązujące konstrukcje Ram Cyberbezpieczeństwa.

TABELA 3: KATEGORYZACJA ZADAŃ I WYNIKÓW

Zadania	Wyniki
ZADANIE C-1 **OPIS SYSTEMU**	• Opisana i udokumentowana charakterystyka systemu. [*Ramy Cyberbezpieczeństwa:* **Profil**]

[74] Etap kategoryzacji RMF jest warunkiem wstępnym wyboru środków bezpieczeństwa. Jednakże, w odniesieniu do prywatności, istnieją inne czynniki brane pod uwagę przez organizacje, które kierują i informują o wyborze zabezpieczeń prywatności. Czynniki te są opisane w etapie Przygotowania systemu RMF, Zadanie P-15.

Zadania	Wyniki
ZADANIE C-2 **KATEGORYZACJA BEZPIECZEŃSTWA**	• Zakończona kategoryzacja bezpieczeństwa systemu, w tym informacji przetwarzanych przez system reprezentowany przez zidentyfikowane przez organizację typy informacji. [*Ramy Cyberbezpieczeństwa*: **ID.AM-1**; **ID.AM-2**; **ID.AM-3; ID.AM-4**; **ID.AM-5**] • Wyniki kategoryzacji bezpieczeństwa są dokumentowane w planach dotyczących bezpieczeństwa, prywatności i SCRM. [*Ramy Cyberbezpieczeństwa*: **Profil**] • Wyniki kategoryzacji bezpieczeństwa są spójne z architekturą korporacyjną i podejściem do ochrony misji organizacyjnych, funkcji biznesowych i procesów misyjnych/biznesowych. [*Ramy Cyberbezpieczeństwa*: **Profil**] • Wyniki kategoryzacji bezpieczeństwa odzwierciedlają strategię zarządzania ryzykiem w organizacji.
ZADANIE C-3 **PRZEGLĄD I ZATWIERDZANIE KATEGORYZACJI BEZPIECZEŃSTWA**	• Wyniki kategoryzacji bezpieczeństwa są zweryfikowane, a decyzja o kategoryzacji jest zatwierdzona przez kierownika wyższego szczebla w organizacji.

OPIS SYSTEMU

ZADANIE C-1 Udokumentowanie charakterystyki systemu.

Potencjalne dane wejściowe: Dokumentacja projektu systemu i wymagań; informacje o granicach autoryzacji; wykaz wymagań dotyczących bezpieczeństwa i ochrony prywatności przypisanych do systemu, elementów systemu i środowiska pracy; fizyczne lub inne procesy kontrolowane przez elementy systemu; informacje o elemencie systemu; inwentaryzacja elementów systemu; informacje o łańcuchu dostaw elementu systemu, w tym informacje o inwentaryzacji i dostawcach; kategoryzacja bezpieczeństwa; mapa cyklu życia informacji dla typów informacji przetwarzanych, przechowywanych i przesyłanych przez system; informacje o użytkowaniu systemu, użytkownikach i rolach.

Oczekiwane wyniki: Udokumentowany opis systemu.

Podstawowa odpowiedzialność: SO.

Role wspierające: AO lub AODR; IO/S; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Opis charakterystyki systemu jest udokumentowany w planach bezpieczeństwa i ochrony prywatności, zawartych w załącznikach do tych planów lub przywołanych w innych standardowych źródłach dla informacji generowanych w ramach SDLC. W miarę możliwości unika się powielania informacji. Poziom szczegółowości zawarty w planach bezpieczeństwa i ochrony prywatności jest określany przez organizację i jest współmierny do kategoryzacji bezpieczeństwa oraz szacowania ryzyka związanego z bezpieczeństwem i ochroną prywatności systemu. Informacje mogą być dodawane do opisu systemu lub aktualizowane w miarę ich dostępności w trakcie cyklu życia systemu, w trakcie realizacji etapów RMF oraz w miarę zmiany charakterystyki systemu.

Przykłady różnych rodzajów informacji opisowych, które organizacje mogą włączyć do planów bezpieczeństwa i ochrony prywatności: opisowa nazwa systemu i identyfikator

systemu; numer wersji lub wydania systemu; informacje o producencie i dostawcy; osoba odpowiedzialna za system; dane kontaktowe systemu; organizacja, która zarządza systemem, jest jego właścicielem lub kontroluje go; lokalizacja systemu; cel systemu i obsługiwane zadania/procesy biznesowe; sposób, w jaki system jest zintegrowany z architekturą korporacyjną; faza SDLC; wyniki procesu kategoryzacji i szacowania ryzyka związanego z prywatnością; granica autoryzacji; prawa, dyrektywy, polityki, regulacje lub normy wpływające na prywatność osób i bezpieczeństwo systemu; opis architektoniczny systemu, w tym topologia sieci; typy informacji; sprzęt, oprogramowanie układowe i komponenty oprogramowania, które są częścią systemu; sprzęt, oprogramowanie i interfejsy systemu (wewnętrzne i zewnętrzne); przepływ informacji w ramach systemu; zasady połączenia sieciowego w celu komunikacji z systemami zewnętrznymi; połączone systemy i identyfikatory tych systemów; fizyczne lub inne procesy, komponenty i urządzenia kontrolowane przez elementy systemu; użytkownicy systemu (w tym przynależność, prawa dostępu, przywileje, obywatelstwo); pochodzenie systemu w łańcuchu dostaw; konserwacja lub inne stosowne umowy; potencjalni dostawcy komponentów zastępczych dla systemu; alternatywne kompatybilne części składowe systemu; liczba i lokalizacja zapasowych części składowych systemu zastępczego; własność lub eksploatacja systemu (należące do organizacji, obsługiwane przez organizację; należące do organizacji, obsługiwane przez wykonawcę; należące do wykonawcy, obsługiwane przez wykonawcę; punkty kontaktowe ds. reagowania na incydenty; data wydania zezwolenia i data wygaśnięcia zezwolenia; oraz status aktualnego zezwolenia. Informacje dotyczące rejestracji systemu są aktualizowane o informacje charakteryzujące system (zob. Zadanie P-18).

Referencje: [NSC 800-18]; [CSF NIST] (podstawowy [funkcja identyfikacji]).

KATEGORYZACJA BEZPIECZEŃSTWA

ZADANIE C-2 Skategoryzowanie systemu i udokumentowanie wyników kategoryzacji bezpieczeństwa.

Potencjalne dane wejściowe: Strategia zarządzania ryzykiem; tolerancja ryzyka organizacyjnego; informacje dotyczące granic autoryzacji systemu; wyniki szacowania ryzyka na poziomie organizacji i systemu; typy informacji przetwarzanych, przechowywanych lub przekazywanych przez system; lista wymagań w zakresie bezpieczeństwa i ochrony prywatności przypisanych do systemu, elementów systemu i środowiska działania; uprawnienia lub cel organizacji w zakresie obsługi systemu; analizy wpływu biznesowego lub analizy krytyczności; informacje o misjach, funkcjach biznesowych i procesach biznesowych wspieranych przez system.

Oczekiwane wyniki: Poziomy wpływu określone dla każdego typu informacji i dla każdego atrybutu bezpieczeństwa (poufność, integralność, dostępność); kategoryzacja bezpieczeństwa oparta na oznaczeniu najwyższego poziomu wpływu na informację.

Podstawowa odpowiedzialność: SO; IO/S.

Role wspierające: SAORM lub RE; CIO; SAISO; SAOP; AO lub AODR; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Ustalenia dotyczące kategoryzacji bezpieczeństwa uwzględniają potencjalny negatywny wpływ na działalność organizacji, aktywa organizacyjne, osoby, inne organizacje i Państwo, wynikający z utraty poufności, integralności lub dostępności informacji. Organizacje dysponują elastycznością w przeprowadzaniu kategoryzacji bezpieczeństwa przy użyciu [NSC 200] w celu ustalenia jednego poziomu wpływu dla systemu opartego na koncepcji oznaczania najwyższego poziomu wpływu na informację w celu ustalenia trzech wartości wpływu, które mogą się różnić dla każdego z atrybutów bezpieczeństwa w zakresie poufności, integralności i dostępności. Proces kategoryzacji bezpieczeństwa jest przeprowadzany przez właściciela systemu i właściciela informacji lub władającego informacją we współpracy i współdziałaniu z wyższymi liderami i kadrą kierowniczą odpowiedzialnymi za misję, funkcję biznesową lub zarządzanie ryzykiem. Współpraca i współdziałanie pomaga zapewnić, że poszczególne systemy są kategoryzowane w oparciu

o misję i cele biznesowe organizacji. Właściciel systemu i właściciel informacji lub władający informacją biorą pod uwagę wyniki szacowania ryzyka związanego z bezpieczeństwem (oraz szacowania ryzyka związanego z prywatnością podczas przetwarzania danych osobowych przez system), jako część decyzji o kategoryzacji bezpieczeństwa. Decyzja ta jest zgodna ze strategią zarządzania ryzykiem. Wyniki procesu kategoryzacji mają wpływ na wybór środków bezpieczeństwa systemu. Informacje o kategoryzacji bezpieczeństwa są dokumentowane w planie bezpieczeństwa systemu lub dołączane do niego, jako załącznik i mogą być przywoływane w planie ochrony prywatności, gdy system przetwarza dane osobowe.

Wyniki kategoryzacji bezpieczeństwa systemu mogą być dalej udoskonalane przez organizację w celu ułatwienia ustalania priorytetów dla systemów o tym samym poziomie wpływu (zob. Zadanie P-6). Wyniki priorytetyzacji na poziomie wpływu prowadzonej przez organizację mogą być wykorzystane do pomocy właścicielom systemów w kontrolowaniu wyboru i dostosowywaniu systemu.

Referencje: [NSC 199]; [NSC 200]; [NSC 800-30]; [SP 800-39] (poziom systemowy); [SP 800-59]; [NSC 800-60 cz. 1]; [NSC 800-60 cz. 2]; [SP 800-160 cz. 1] (Procesy definiowania potrzeb i wymagań zainteresowanych stron oraz definiowania wymagań systemowych); [IR 8179]; [CNSSI 1253]; [NIST CSF] (Podstawowy [Funkcja identyfikacji]).

PRZEGLĄD I ZATWIERDZENIE KATEGORYZACJI BEZPIECZEŃSTWA

ZADANIE C-3 Przegląd i zatwierdzenie wyników kategoryzacji bezpieczeństwa i decyzji.

Potencjalne dane wejściowe: Poziomy wpływu określone dla każdego typu informacji i dla każdego atrybutu bezpieczeństwa (poufność, integralność, dostępność); kategoryzacja bezpieczeństwa oparta na oznaczeniu najwyższego poziomu wpływu na informację; lista aktywów o wysokiej wartości dla organizacji.

Oczekiwane wyniki: Zatwierdzenie kategoryzacji bezpieczeństwa systemu.

Podstawowa odpowiedzialność: AO lub AODR; SAOP.[75]

Role wspierające: SAORM lub RE; CIO; SAISO.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: W przypadku systemów informatycznych, które przetwarzają dane osobowe, SAOP dokonuje przeglądu prywatności i zatwierdza wyniki kategoryzacji bezpieczeństwa oraz podejmuje decyzję przed dokonaniem przeglądu przez osobę autoryzującą. Wyniki kategoryzacji bezpieczeństwa i decyzje dotyczące bezpieczeństwa[76] są weryfikowane przez AO lub AODR w celu zapewnienia, że kategoria bezpieczeństwa wybrana dla systemu informatycznego jest zgodna z misją i funkcjami biznesowymi organizacji oraz potrzebą odpowiedniej ochrony tych misji i funkcji. Osoba autoryzująca lub pełnomocnik osoby autoryzującej dokonuje przeglądu wyników kategoryzacji i decyzji z perspektywy całej organizacji, w tym sposobu, w jaki decyzja ta jest zgodna z decyzjami dotyczącymi kategoryzacji wszystkich innych systemów organizacyjnych. Osoba autoryzująca współpracuje z SAORM lub RE w celu zapewnienia, że decyzja kategoryzacyjna systemu jest zgodna ze strategią zarządzania ryzykiem w organizacji i spełnia wymagania dotyczące aktywów o wysokiej wartości. W ramach procesu zatwierdzania, osoba autoryzująca może przedstawić właścicielowi systemu konkretne wytyczne dotyczące wszelkich ograniczeń w podstawowych działaniach związanych z dostosowaniem systemu do potrzeb, które występują na etapie *Wyboru* RMF (zob. Zadanie S-2). Jeżeli decyzja o kategoryzacji bezpieczeństwa nie zostanie zatwierdzona, właściciel systemu rozpoczyna kroki w celu powtórzenia procesu kategoryzacji i ponownie przedstawia skorygowane wyniki osobie autoryzującej lub wyznaczonemu przedstawicielowi. Informacje o rejestracji systemu są

[75] SAOP uczestniczy w ustalaniu, czy informacje przetwarzane przez system informatyczny są uważane za dane osobowe, oraz uczestniczy w przeglądzie i kategoryzacji takich systemów.
[76] Obowiązki SAOP zostały szczegółowo opisane w przepisach RODO i ustawie o ochronie danych osobowych.

następnie aktualizowane o zatwierdzone informacje o kategoryzacji bezpieczeństwa (zob. Zadanie P-18).

Referencje: [NSC 199]; [NSC 800-30]; [SP 800-39] (Poziom organizacji); [SP 800-160 cz. 1] (Proces definiowania potrzeb i wymagań zainteresowanych stron); [CNSSI 1253]; [CSF NIST] (Podstawowy [Funkcja identyfikacji]).

3.3 WYBÓR

CEL

Celem etapu ***Wybór*** jest wybranie, dopasowanie i udokumentowanie zabezpieczeń niezbędnych do ochrony systemu informatycznego i organizacji, współmiernych do ryzyka działań i aktywów organizacji, osób, innych organizacji i Państwa.

WYBÓR ZADAŃ

Tabela 4 zawiera podsumowanie zadań i oczekiwanych wyników dla etapu W*ybór* RMF. Przedstawiono również obowiązujące konstrukcje Ram Cyberbezpieczeństwa.

TABELA 4: WYBÓR ZADAŃ I WYNIKÓW

Zadania	Wyniki
ZADANIE S-1 **WYBÓR ZABEZPIECZEŃ**	• Wybrane zabezpieczenia bazowe niezbędne do ochrony systemu współmiernej do ryzyka. [*Ramy Cyberbezpieczeństwa*: **Profil**]

Zadania	Wyniki
ZADANIE S-2 **DOSTOSOWYWANIE ZABEZPIECZEŃ**	• Zabezpieczenia są dostosowane do potrzeb organizacji, co pozwala na stworzenie przystosowanych do jej potrzeb zabezpieczeń bazowych. [Ramy Cyberbezpieczeństwa: **Profil**]
ZADANIE S-3 **PRZYDZIAŁ ZABEZPIECZEŃ**	• Zabezpieczenia są oznaczone, jako zabezpieczenia specyficzne dla danego systemu, hybrydowe lub wspólne. • Zabezpieczenia są przydzielone do poszczególnych elementów systemu (tj. sprzętu, zasobów fizycznych lub ludzkich). [*Ramy Cyberbezpieczeństwa:* **Profil**; **PR.IP**]
ZADANIE S-4 **DOKUMENTACJA WDROŻENIA PLANOWANYCH ZABEZPIECZEŃ**	• Zabezpieczenia i związane z nimi działania dostosowujące są udokumentowane w planach bezpieczeństwa i ochrony prywatności lub równoważnych dokumentach. [*Ramy Cyberbezpieczeństwa:* **Profile**]
ZADANIE S-5 **STRATEGIA CIĄGŁEGO MONITOROWANIA SYSTEMU**	• Opracowywana jest strategia ciągłego monitorowania systemu, która odzwierciedla strategię zarządzania ryzykiem organizacyjnym. [*Ramy Cyberbezpieczeństwa:* **ID.GV**; **DE.CM**]

Zadania	Wyniki
ZADANIE S-6 **PRZEGLĄD I ZATWIERDZENIE PLANU**	• Plany bezpieczeństwa i ochrony prywatności odzwierciedlające wybór zabezpieczeń niezbędnych do ochrony systemu i środowiska pracy współmiernych do ryzyka są zweryfikowane i zatwierdzone przez osobę autoryzującą.

WYBÓR ZABEZPIECZEŃ

ZADANIE S-1 Wybór zabezpieczeń systemu i środowiska pracy.

Potencjalne dane wejściowe: Kategoryzacja bezpieczeństwa; wyniki szacowania ryzyka na poziomie organizacji i systemu; informacje o elementach systemu; inwentaryzacja elementów systemu; wykaz wymagań w zakresie bezpieczeństwa i ochrony prywatności przypisanych do systemu, elementów systemu i środowiska pracy; wykaz wymagań kontraktowych przypisanych do zewnętrznych dostawców systemu lub elementu systemu; analiza wpływu biznesowego lub analiza krytyczności; strategia zarządzania ryzykiem; polityka bezpieczeństwa i ochrony prywatności organizacji; organizacyjne zatwierdzone lub nakazane zabezpieczenia bazowe lub nakładki; Profile Ram Cyberbezpieczeństwa.

Oczekiwane wyniki: Zabezpieczenia wybrane dla systemu i środowiska pracy.

Podstawowa odpowiedzialność: SO; CCP.

Role wspierające: AO lub AODR; IO/S; SSE; PE; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Istnieją dwa podejścia, które mogą być wykorzystane do wstępnego wyboru zabezpieczeń: podejście wyboru *zabezpieczeń bazowych* lub podejście wyboru zabezpieczeń *tworzonych przez organizację.* Podejście wyboru zabezpieczeń bazowych wykorzystuje

podstawowe mechanizmy zabezpieczeń, które są wstępnie zdefiniowanymi zestawami zabezpieczeń specjalnie zebranymi w celu zaspokojenia potrzeb ochrony grupy, organizacji lub wspólnoty interesów. Zabezpieczenia bazowe służą, jako punkt wyjścia dla ochrony prywatności osób fizycznych, informacji oraz systemów informatycznych. Zabezpieczenia bazowe znajdują się w [SP 800-53B]. Kategoryzacja bezpieczeństwa systemu (zob. Zadanie C-2) oraz wymagania bezpieczeństwa wynikające z potrzeb ochrony interesariuszy, przepisów prawnych, rozporządzeń, regulacji, polityk, dyrektyw, instrukcji i standardów (zob. Zadanie P-15) mogą pomóc w wyborze zabezpieczeń bazowych. Szacowanie ryzyka związanego z ochroną prywatności (zob. Zadanie P-14) oraz wymogów ochrony prywatności wynikających z potrzeb w zakresie ochrony interesariuszy, przepisów prawnych, rozporządzeń, polityk, dyrektyw, instrukcji i standardów (zob. zadanie P-15) może być pomocna przy wyborze poziomów odniesienia w zakresie zabezpieczeń prywatności. Programy ochrony prywatności wykorzystują zabezpieczenia bazowe w zakresie bezpieczeństwa i ochrony prywatności do zarządzania zagrożeniami odnoszącymi się do prywatności wynikającymi zarówno z nieautoryzowanej działalności lub zachowania systemu, jak i z autoryzowanych działań. Po wybraniu wstępnie zdefiniowanych zabezpieczeń bazowych, organizacje dostosowują podstawowe mechanizmy zabezpieczeń zgodnie z dostarczonymi wskazówkami (zob. Zadanie S-2). Podejście polegające na wyborze zabezpieczeń bazowych może zapewnić spójność w szerokim zakresie interesów.

Podejście do wyboru zabezpieczeń tworzonych przez organizację różni się od podejścia do wyboru zabezpieczeń bazowych, ponieważ organizacja nie rozpoczyna od wstępnie zdefiniowanego zabezpieczeń bazowych. Organizacja używa raczej swojego własnego procesu selekcji do wyboru zabezpieczeń. Może to być konieczne, gdy system jest wysoce wyspecjalizowany (np. system uzbrojenia lub urządzenia medyczne) lub ma ograniczony cel lub zakres (np. inteligentny licznik). W takich sytuacjach bardziej efektywny i opłacalny może być dla organizacji wybór konkretnego zestawu zabezpieczeń systemu (tj. podejście oddolne), zamiast rozpoczynania od predefiniowanego zestawu zabezpieczeń z szeroko

zakrojonego zestawu zabezpieczeń bazowych, a następnie eliminowania zabezpieczeń poprzez proces dostosowywania (tj. podejście odgórne).

Zarówno w podejściu wyboru zabezpieczeń bazowych, jak i w podejściu wyboru zabezpieczeń tworzonych przez organizację, organizacje opracowują stosownie zdefiniowany zestaw wymagań dotyczących bezpieczeństwa i ochrony prywatności, wykorzystując proces inżynierii systemów oparty na cyklu życia (np. [ISO 15288] i [SP 800-160 V.1 cz. 1], jak opisano w kroku RMF *Przygotowanie zadań – poziom organizacyjny*, Zadanie P-15. Proces ten generuje zestaw wymagań, które mogą być wykorzystane do prowadzenia i informowania o wyborze zestawu zabezpieczeń w celu spełnienia wymagań (niezależnie od tego, czy organizacja zaczyna od zabezpieczeń bazowych, czy tworzy zestaw zabezpieczeń z własnego procesu wyboru). Podobnie, organizacje mogą wykorzystać [NIST CSF] do opracowania Profili Ram Cyberbezpieczeństwa reprezentujące zestaw specyficznych dla organizacji wymagań dotyczących bezpieczeństwa i ochrony prywatności - a tym samym ukierunkowując i informując o wyborze zabezpieczeń z [NSC 800-53]. Dostosowywanie może być również wymagane w podejściu wyboru zabezpieczeń tworzonych przez organizację (zob. Zadanie S-2). Organizacje nie muszą wybierać jednego podejścia do wyboru zabezpieczeń dla każdego ze swoich systemów, ale zamiast tego mogą stosować różne podejścia, zależnie od okoliczności.

Referencje: [NSC 199]; [NSC 200]; [NSC 800-30]; [NSC 800-53]; [SP 800-53B]; [SP 800-160 V.1 cz. 1] (Definicja wymagań systemowych, definicja architektury i procesy definicji projektu); [SP 800-161] (Odpowiedzi i rozdział 3); [IR 8062]; [IR 8179]; [CNSSI 1253]; [NIST CSF] (podstawowe funkcje [identyfikowania, ochrony, wykrywania, reagowania, odzyskiwania]; profile).

DOSTOSOWYWANIE ZABEZPIECZEŃ

ZADANIE S-2 Dostosowywanie wybranego zabezpieczenia do systemu i środowiska pracy.

Potencjalne dane wejściowe: Wstępne zestawy minimalnych zabezpieczeń; wyniki szacowania ryzyka na poziomie organizacji i systemu; informacje o elementach systemu; inwentaryzacja elementów systemu; lista wymagań w zakresie bezpieczeństwa i ochrony prywatności przypisanych do systemu, elementów systemu i środowiska pracy; analiza wpływu biznesowego lub analiza krytyczności; strategia zarządzania ryzykiem; polityka bezpieczeństwa i ochrony prywatności organizacji; zatwierdzone lub nakazane nakładki.

Oczekiwane wyniki: Lista dostosowanych zabezpieczeń systemu i środowiska pracy (tj. dostosowane zabezpieczenia bazowe).

Podstawowa odpowiedzialność: SO; CCP.

Role wspierające: AO lub AODR; IO/S; SSE; PE; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Po wybraniu odpowiednich zabezpieczeń bazowych, organizacje dostosowują je do różnych czynników (np. misji lub funkcji biznesowych, zagrożeń, ryzyka związanego z bezpieczeństwem i prywatnością (w tym ryzyka związanego z łańcuchem dostaw), rodzaju systemu lub tolerancji na ryzyko). Proces dostosowywania obejmuje identyfikację i wyznaczenie zabezpieczeń wspólnych w zestawach minimalnych zabezpieczeń (zob. Zadanie P-5); zastosowanie rozważań dotyczących możliwości pozostałych podstawowych mechanizmów zabezpieczeń; wybór mechanizmów zabezpieczeń kompensujących, jeśli jest to konieczne; przypisanie wartości do zdefiniowanych przez organizację parametrów zabezpieczeń za pomocą oświadczeń dotyczących przypisania lub wyboru; uzupełnienie zabezpieczeń bazowych o dodatkowe mechanizmy bezpieczeństwa; oraz dostarczenie informacji dotyczących specyfikacji w celu wdrożenia zabezpieczeń.[77] Organizacje określają ilość szczegółów, które należy uwzględnić w uzasadnieniach lub przesłankach wymaganych przy podejmowaniu decyzji o dostosowaniu. Na przykład uzasadnienie lub przesłanka decyzji

[77] Proces dostosowywania jest szczegółowo opisany w [NSC 800-53B].

dotyczących zakresu decyzji związanych z systemem o dużym poziomie wpływu lub aktywem o dużej wartości może wymagać większej szczegółowości niż podobne decyzje dotyczące systemu o małym poziomie wpływu. Ustalenia takie są zgodne z misją i funkcjami biznesowymi organizacji, potrzebami interesariuszy oraz wszelkimi stosownymi przepisami prawa, rozporządzeniami, regulacjami, dyrektywami i zasadami. Zabezpieczenia związane z SDLC i SCRM stanowią podstawę do określenia, czy system informatyczny jest odpowiedni do celu[78] i czy musi być odpowiednio dostosowany.

Organizacje wykorzystują szacowanie ryzyka do informowania i kierowania procesem dostosowania. Informacje o zagrożeniach wynikające z szacowania ryzyka bezpieczeństwa dostarczają informacji o zdolnościach, zamiarach i celach przeciwnika, które mogą mieć wpływ na decyzje organizacji dotyczące wyboru środków bezpieczeństwa, w tym związanych z nimi kosztów i korzyści. Szacowanie ryzyka związanego z ochroną prywatności, w tym czynniki kontekstowe, również będzie miało wpływ na dostosowanie, gdy system informatyczny przetwarza informacje z zakresu ochrony prywatności. Wyniki szacowania ryzyka są również wykorzystywane przy określaniu zabezpieczeń wspólnych w celu ustalenia, czy środki bezpieczeństwa dostępne do celów dziedziczenia spełniają wymogi bezpieczeństwa i ochrony prywatności dotyczące systemu i środowiska jego działania. Jeżeli mechanizmy wspólnych zabezpieczeń dostarczane przez organizację nie zapewniają odpowiedniej ochrony systemów, które je dziedziczą, właściciele systemów mogą albo uzupełnić zabezpieczenia wspólne o mechanizmy specyficzne dla danego systemu lub mechanizmy hybrydowe w celu osiągnięcia wymaganego poziomu ochrony, albo zalecić osobie autoryzującej akceptację większego ryzyka. Organizacje mogą również rozważyć organizacyjnie zarządzane lub zatwierdzone nakładki, dostosowane zabezpieczenia bazowe lub Profile Ram Cyberbezpieczeństwa podczas dostosowywania zabezpieczeń (zob.: Zadanie P-4).

[78] [ISO 15288] opisuje przydatność do celu, jako wynik procesu walidacji w SDLC, który pokazuje, poprzez ocenę usług przedstawionych interesariuszom, że został stworzony "właściwy" system zaspokajający potrzeby klienta.

Referencje: [NSC 199]; [NSC 200]; [NSC 800-30]; [NSC 800-53]; [SP 800-53B]; [SP 800-160 cz. 1] (Definicja wymagań systemowych, definicja architektury i procesy definiowania projektu); [SP 800-161] (Reagowanie i rozdział 3); [IR 8179]; [CNSSI 1253]; [CSF NIST] (Funkcje podstawowe [identyfikacja, ochrona, wykrywanie, reagowanie, odzyskiwanie]; Profil).

PRZYDZIAŁ ZABEZPIECZEŃ

ZADANIE S-3 Przydzielenie środków bezpieczeństwa i ochrony prywatności do systemu i środowiska pracy.

Potencjalne dane wejściowe: Kategoryzacja bezpieczeństwa; wyniki szacowania ryzyka na poziomie organizacji i systemu; polityka organizacyjna w zakresie rejestracji systemu; architektura korporacyjna; architektury bezpieczeństwa i ochrony prywatności; wymagania w zakresie bezpieczeństwa i ochrony prywatności; wykaz wymagań w zakresie bezpieczeństwa i ochrony prywatności przypisanych do systemu, elementów systemu i środowiska pracy; wykaz dostawców zabezpieczeń wspólnych i zestawienie zabezpieczeń wspólnych dostępnych do celów dziedziczenia; opis systemu; informacje o elementach systemu; spis elementów systemu; odpowiednie ustawy, rozporządzenia, dyrektywy, regulacje i zasady.

Oczekiwane wyniki: Lista środków bezpieczeństwa i ochrony prywatności przypisanych do systemu, elementów systemu i środowiska pracy.

Podstawowa odpowiedzialność: SA; PA; SSO; SPO.

Role wspierające: CIO; AO lub AODR; BO; SAISO; SAOP; SO.

Faza rozwoju cyklu życia systemu: Nowy - Inicjowanie (koncepcja; definiowanie wymagań).

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Organizacja wyznacza środki bezpieczeństwa, jako specyficzne dla systemu, hybrydowe lub wspólne i przydziela je do elementów systemu (tj. urządzeń, zasobów fizycznych lub ludzkich) odpowiedzialnych za zapewnienie bezpieczeństwa lub ochrony

prywatności. Środki bezpieczeństwa są przydzielane do systemu lub organizacji zgodnie z jej architekturą korporacyjną i architekturą bezpieczeństwa lub ochrony prywatności oraz przydzielonymi wymogami w zakresie bezpieczeństwa i ochrony prywatności. Nie wszystkie zabezpieczenia muszą być przypisane do każdego elementu systemu. Zabezpieczenia zapewniające określoną zdolność w zakresie bezpieczeństwa lub ochrony prywatności są przydzielane tylko do tych elementów systemu, które wymagają tej zdolności. Kategoryzacja bezpieczeństwa, szacowanie ryzyka związanego z ochroną prywatności, architektury bezpieczeństwa i prywatności oraz alokacja elementów sterujących współpracują ze sobą, aby pomóc w osiągnięciu odpowiedniej równowagi między zabezpieczeniami i ochroną prywatności, a misją systemu.

Wymagania dotyczące bezpieczeństwa i ochrony prywatności przypisane do systemu, elementów systemu oraz środowiska pracy (zob. Zadanie P-17) prowadzą i informują o przypisaniu zabezpieczeń do elementów systemu. Zabezpieczenia wspólne, które są udostępniane przez organizację w ramach etapu przygotowania RMF *Przygotowanie na poziomie organizacji* (zob. Zadanie P-5), są wybierane do dziedziczenia; wybierane są również zabezpieczenia hybrydowe. Wspólne mechanizmy bezpieczeństwa spełniają wymogi bezpieczeństwa i ochrony prywatności przydzielone organizacji i zapewniają zdolność ochrony, która jest dziedziczona przez jeden lub więcej systemów. Zabezpieczenia hybrydowe spełniają wymogi bezpieczeństwa i ochrony prywatności przypisane do systemu i organizacji oraz zapewniają zdolność ochrony, która jest częściowo dziedziczona przez jeden lub więcej systemów. Dodatkowo, zabezpieczenia specyficzne systemu spełniają wymagania bezpieczeństwa i ochrony prywatności przypisane do systemu i zapewniają zdolność ochrony tego systemu. Zabezpieczenia mogą być przypisane do konkretnych elementów systemu, a nie do każdego elementu w ramach systemu. Na przykład, specyficzne dla systemu elementy sterujące związane z zarządzaniem logami audytowymi mogą być przypisane do serwera zarządzania logami i nie muszą być zaimplementowane na każdym elemencie systemu.

Referencje: [SP 800-39] (Organizacja, misja/proces biznesowy i poziomy systemu); [SP 800-64]; [SP 800-160 cz. 1] (Definicja wymagań systemowych, definicja architektury i procesy definicji projektu); [NIST CSF] (Podstawowe [Funkcja identyfikacji]; Profile); [OMB FEA].

DOKUMENTACJA WDROŻENIA PLANOWANYCH ZABEZPIECZEŃ

ZADANIE S-4 Dokumentowanie zabezpieczeń systemu i środowiska pracy w planach bezpieczeństwa i ochrony prywatności.

Potencjalne dane wejściowe: Kategoryzacja bezpieczeństwa; wyniki szacowania ryzyka na poziomie organizacji i systemu (bezpieczeństwo, prywatność i/lub łańcuch dostaw); informacje o elementach systemu; inwentaryzacja elementów systemu; analiza wpływu biznesowego lub krytyczności; lista wymogów bezpieczeństwa i prywatności przypisanych do systemu, elementów systemu i środowiska działania; strategia zarządzania ryzykiem; lista wybranych zabezpieczeń systemu i środowiska działania; bezpieczeństwo organizacyjne, prywatność i zasady SCRM.

Oczekiwane wyniki: Plany bezpieczeństwa i ochrony prywatności systemu.

Podstawowa odpowiedzialność: SO; CCP.

Role wspierające: AO lub AODR; IO/S; SSE; PE; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Plany bezpieczeństwa i ochrony prywatności zawierają przegląd wymagań dotyczących bezpieczeństwa i ochrony prywatności dla systemu oraz zabezpieczeń wybranych w celu spełnienia tych wymagań. Plany opisują zamierzone zastosowanie każdego wybranego zabezpieczenia w kontekście systemu z wystarczającym poziomem szczegółowości, aby prawidłowo wprowadzić zabezpieczenie i następnie ocenić jego skuteczność. Dokumentacja zabezpieczeń opisuje sposób realizacji zabezpieczeń specyficznych dla systemu i zabezpieczeń hybrydowych oraz plany i oczekiwania dotyczące

funkcjonalności systemu. Opis zawiera planowane dane wejściowe, oczekiwane zachowanie i oczekiwane wyniki, w stosownych przypadkach, zazwyczaj w odniesieniu do tych zabezpieczeń, które zostały wdrożone w komponentach sprzętowych, programowych lub układowych systemu. Zabezpieczenia wspólne są również określone w planach. Nie ma wymogu dostarczenia szczegółów implementacji dla odziedziczonych zabezpieczeń wspólnych. Szczegóły te są raczej przedstawiane w planach dla dostawców zabezpieczeń wspólnych i są udostępniane właścicielom systemu. W przypadku zabezpieczeń hybrydowych organizacja określa w planach na poziomie systemu te części zabezpieczeń, które są dostarczane przez dostawcę zabezpieczenia wspólnego oraz te części zabezpieczeń, które są wdrażane na poziomie systemu.

Organizacje mogą opracować skonsolidowany plan, który zawiera plany bezpieczeństwa i ochrony prywatności lub utrzymać odrębne plany. W przypadku opracowywania skonsolidowanego planu, programy ochrony prywatności współpracują z programami bezpieczeństwa, aby zapewnić, że plan odzwierciedla wybór środków bezpieczeństwa, które zapewniają ochronę w zakresie zarządzania poufnością, integralnością i dostępnością danych osobowych; oraz określa role i obowiązki w zakresie wdrażania, oceny i monitorowania zabezpieczeń. W przypadku odrębnych planów bezpieczeństwa systemu i planów ochrony prywatności, organizacje odsyłają do zabezpieczeń we wszystkich planach, aby pomóc w zachowaniu odpowiedzialności i świadomości. Uprawniony personel organizacji dokonuje przeglądu i zatwierdza plan ochrony prywatności (lub plan zintegrowany) przed przekazaniem planu do przeglądu osobie autoryzującej lub wyznaczonemu przedstawicielowi (zob. Zadanie S-6). Organizacje mogą udokumentować wybór zabezpieczeń i dostosowanie informacji w dokumentach równoważnych z planami bezpieczeństwa i ochrony prywatności, na przykład w inżynierii systemów lub artefaktach lub dokumentach dotyczących cyklu życia systemu.

Dokumentacja planowanych wdrożeń zabezpieczeń pozwala na śledzenie decyzji przed i po wdrożeniu systemu. W miarę możliwości organizacje odwołują się do istniejącej dokumentacji (przez dostawców lub inne organizacje, które zastosowały te same lub

podobne systemy lub elementy systemu), korzystają ze zautomatyzowanych narzędzi wsparcia oraz koordynują działania w całej organizacji w celu zmniejszenia nadmiarowości oraz zwiększenia efektywności i opłacalności dokumentacji zabezpieczającej. Dokumentacja odnosi się również do zależności od platformy i zawiera wszelkie dodatkowe informacje niezbędne do opisania, w jaki sposób wymagana zdolność ma być osiągnięta na poziomie szczegółowości wystarczającym do wsparcia wdrażania i oceny zabezpieczeń. Dokumentacja dotycząca wdrożeń zabezpieczeń jest zgodna z najlepszymi praktykami w zakresie rozwoju sprzętu i oprogramowania oraz dziedzin inżynierii bezpieczeństwa systemów i prywatności, a także z ustalonymi zasadami i procedurami dotyczącymi dokumentowania działań w SDLC. W pewnych sytuacjach środki bezpieczeństwa mogą być wdrażane w sposób stwarzający zagrożenie dla prywatności. Program ochrony prywatności obsługuje dokumentowanie zagrożeń prywatności oraz implementacje mające na celu ich ograniczenie.

W przypadku zabezpieczeń opartych na mechanizmach, organizacje korzystają ze specyfikacji funkcjonalnych dostarczonych lub możliwych do uzyskania od producentów, sprzedawców i integratorów systemów. Obejmuje to wszelką dokumentację, która może wspomóc organizację podczas opracowywania, wdrażania, oceny i monitorowania mechanizmów bezpieczeństwa. W przypadku niektórych zabezpieczeń organizacje uzyskują informacje na temat wdrażania zabezpieczeń od odpowiednich jednostek organizacyjnych (np. biur ochrony fizycznej, biur obsługi obiektów, biur zarządzania dokumentacją i biur zasobów ludzkich). Ponieważ architektura korporacyjna oraz architektury bezpieczeństwa i ochrony prywatności ustanowione przez instrukcje organizacyjne informują o podejściu organizacyjnym stosowanym do planowania i wdrażania zabezpieczeń, dokumentowanie procesu pomaga zapewnić identyfikowalność w spełnianiu wymogów bezpieczeństwa i ochrony prywatności.

Referencje: [NSC 199]; [NSC 200]; [NSC 800-18]; [NSC 800-30]; [NSC 800-53]; [SP 800-64]; [SP 800-160 cz. 1]. (definiowanie wymagań systemowych, definiowanie architektury i procesy definiowania projektu); [SP 800-161] (reagowanie i rozdział 3); [IR 8179]; [CNSSI 1253]; [CSF NIST] (funkcje podstawowe [identyfikacja, ochrona, wykrywanie, reagowanie, odzyskiwanie]; Profil).

STRATEGIA CIĄGŁEGO MONITOROWANIA SYSTEMU

ZADANIE S-5 Opracowanie i wdrożenie na poziomie systemowym strategii monitorowania skuteczności zabezpieczeń, która jest spójna z organizacyjną strategią ciągłego monitorowania i stanowi jej uzupełnienie.

Potencjalne dane wejściowe: Strategia zarządzania ryzykiem organizacyjnym; strategia ciągłego monitorowania organizacji; wyniki szacowania ryzyka na poziomie organizacji i systemu; plany bezpieczeństwa i ochrony prywatności; polityka bezpieczeństwa i ochrony prywatności organizacji.

Oczekiwane wyniki: Strategia ciągłego monitorowania systemu, w tym czasowe uruchamianie bieżących autoryzacji.

Podstawowa odpowiedzialność: SO; CCP.

Role wspierające: SAORM lub RE; CIO; SAISO; SAOP; AO lub AODR; IO/S; SA; PA; SSE; PE; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie.
Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Ważnym aspektem zarządzania ryzykiem jest stałe monitorowanie zabezpieczeń przeprowadzanych w ramach systemu informatycznego lub przez niego dziedziczonych. Skuteczna strategia ciągłego monitorowania na poziomie systemu jest opracowywana i wdrażana w koordynacji ze strategią organizacyjną ciągłego monitorowania na początku SDLC (tj. podczas wstępnego projektowania systemu lub podejmowania decyzji o zakupie). Strategia ciągłego monitorowania na poziomie systemu jest spójna ze strategią ciągłego

monitorowania organizacji i stanowi jej uzupełnienie. Strategia na poziomie systemowym dotyczy monitorowania tych zabezpieczeń, dla których monitoring nie jest przewidziany w ramach strategii ciągłego monitorowania i wdrażania w organizacji. Strategia na poziomie systemowym określa częstotliwość monitorowania zabezpieczeń, których nie obejmuje strategia na poziomie organizacji oraz określa podejście, które należy zastosować do oceny tych zabezpieczeń. Strategia ciągłego monitorowania na poziomie systemu, zgodna ze strategią monitorowania organizacji, określa sposób monitorowania zmian w systemie i środowisku działania[79]; sposób przeprowadzania szacowania ryzyka; oraz wymogi dotyczące sprawozdawczości w zakresie bezpieczeństwa i ochrony prywatności, w tym odbiorców sprawozdań. Strategia ciągłego monitorowania na poziomie systemu może być włączona do planów bezpieczeństwa i ochrony prywatności.[80]

W przypadku zabezpieczeń, które nie są objęte strategią organizacyjną stałego monitorowania, strategia stałego monitorowania na poziomie systemu określa kryteria ustalania częstotliwości monitorowania zabezpieczeń po wdrożeniu oraz plan bieżącej oceny tych zabezpieczeń. Kryteria są ustalane przez właściciela systemu lub dostawcę zabezpieczeń wspólnych we współpracy z innymi jednostkami organizacji (np. AO lub AODR; SAORM lub RE; SAISO; SAOP; oraz CIO). Kryteria częstotliwości na poziomie systemu odzwierciedlają priorytety organizacyjne i znaczenie systemu dla działalności i aktywów organizacji, osób, innych organizacji i Państwa. Zabezpieczenia, które są zmienne (tzn. tam, gdzie

[79] Zmiany w środowisku operacyjnym (w tym w łańcuchu dostaw) mogą stwarzać podatności (np. Dostępność łatek do oprogramowania, zmiany własności dostawców świadczących usługi, konserwacja, naprawa części lub inne wsparcie).

[80] Strategia Ciągłego Monitorowania Prywatności (ang. Privacy Continuous Monitoring - PCM) obejmuje wszystkie dostępne środki ochrony prywatności wdrożone w całej organizacji na wszystkich poziomach zarządzania ryzykiem (tj. Organizacja, misja/proces biznesowy i system). Strategia ta zapewnia stałe monitorowanie zabezpieczeń poprzez przypisanie każdemu zabezpieczeniu określonemu przez organizację częstotliwości oceny, która jest wystarczająca do zapewnienia zgodności z obowiązującymi wymogami w zakresie ochrony prywatności oraz do zarządzania ryzykiem w zakresie ochrony prywatności. Jeżeli w trakcie opracowywania nowego systemu istnieje potrzeba stworzenia lub wykorzystania zabezpieczeń w zakresie ochrony prywatności nieujętych w strategii PCM, przeprowadzana jest konsultacja z inspektorem danych osobowych w celu ustalenia, czy jest ona odpowiednia dla proponowanego przypadku zastosowania. W przypadku podjęcia decyzji o wdrożeniu nowego zabezpieczenia w zakresie ochrony prywatności, strategia PCM organizacji jest aktualizowana w celu uwzględnienia nowego zabezpieczenia z częstotliwością monitorowania określoną przez organizację.

zabezpieczenie lub wdrożenie zabezpieczenia najprawdopodobniej zmieni się w czasie),[81] krytyczne dla niektórych aspektów potrzeb ochrony organizacji lub określone w planach i etapach działania, mogą wymagać częstszej oceny. Podejście do ocen zabezpieczeń podczas ciągłego monitorowania może obejmować ponowne wykorzystanie procedur oceny i wyników, które wspierały pierwotną decyzję o zezwoleniu; wykrycie statusu elementów systemu; oraz analizę danych historycznych i operacyjnych.

Osoba autoryzująca lub pełnomocnik osoby autoryzującej zatwierdza strategię stałego monitorowania oraz minimalną częstotliwość, z jaką każde zabezpieczenie ma być monitorowane. Zatwierdzenie strategii można uzyskać w połączeniu z zatwierdzeniem planu bezpieczeństwa i ochrony prywatności. Monitorowanie zabezpieczeń rozpoczyna się na początku fazy operacyjnej SDLC i trwa przez fazę usuwania (utylizacji).

Referencje: [NSC 800-30]; [SP 800-39] (Organizacja, misja lub proces biznesowy, poziomy systemu); [NSC 800-53]; [NSC 800-53A]; [SP 800-137]; [SP 800-161]; [IR 8011 v1]; [CNSSI 1253]; [NIST CSF] (Podstawowy [funkcja wykrywania]).

PRZEGLĄD I ZATWIERDZENIE PLANU

ZADANIE S-6 Przegląd i zatwierdzenie planów bezpieczeństwa i ochrony prywatności systemu i środowiska pracy.

Potencjalne dane wejściowe: Plany bezpieczeństwa i ochrony prywatności; wyniki szacowania ryzyka na poziomie organizacji i systemu.

Oczekiwane wyniki: Plany bezpieczeństwa i ochrony prywatności zatwierdzone przez osobę autoryzującą.

[81] Zmienność jest najbardziej rozpowszechniona w zabezpieczeniach zaimplementowanych w elementach sprzętu, oprogramowania i firmware'u systemu. Na przykład, wymiana lub aktualizacja systemu operacyjnego, systemu baz danych, aplikacji lub routera sieciowego może spowodować zmianę zabezpieczeń dostarczanych przez dostawcę lub producenta oryginalnego sprzętu. Ustawienia konfiguracyjne mogą również wymagać wprowadzenia zmian w zakresie misji organizacyjnych, funkcji biznesowych, zagrożeń, ryzyka i tolerancji na ryzyko.

Podstawowa odpowiedzialność: AO lub AODR.

Role wspierające: SAORM lub RE; CIO; CAO; SAISO; SAOP.

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Przegląd planu bezpieczeństwa i ochrony prywatności przez AO lub AODR wspomaganego przez SAORM lub RE, CIO, SAISO i SAOP, określa, czy plany są kompletne, spójne i spełniają określone wymagania dotyczące bezpieczeństwa i ochrony prywatności systemu. W oparciu o wyniki tego przeglądu, osoba autoryzująca lub pełnomocnik osoby autoryzującej może zalecić zmiany w planach bezpieczeństwa i ochrony prywatności. Jeśli plany te są nie do zaakceptowania, właściciel systemu lub dostawca usług wspólnych dokonuje odpowiednich zmian w planach. Jeśli plany są możliwe do zaakceptowania, osoba autoryzująca lub pełnomocnik osoby autoryzującej zatwierdza plany.

Przyjęcie planów bezpieczeństwa i ochrony prywatności stanowi ważny etap w procesie SDLC i zarządzania ryzykiem. Osoba autoryzująca lub pełnomocnik osoby autoryzującej, poprzez zatwierdzenie planów, wyraża zgodę na zestaw zabezpieczeń (tj. zabezpieczenia specyficzne dla systemu, hybrydowe lub wspólne) oraz opis proponowanego wdrożenia zabezpieczeń w celu spełnienia wymogów bezpieczeństwa i ochrony prywatności systemu i środowiska, w którym system funkcjonuje.[82] Zatwierdzenie planów pozwala na przejście procesu zarządzania ryzykiem do etapu *Wdrożenie* RMF. Zatwierdzenie planów określa również poziom wysiłków niezbędnych do pomyślnego zakończenia pozostałych etapów realizacji etapów RMF i stanowi podstawę specyfikacji bezpieczeństwa i ochrony prywatności w odniesieniu do nabycia systemu lub poszczególnych elementów systemu.

Referencje: [NSC 800-30]; [NSC 800-53]; [SP 800-160 cz. 1] (Definicja wymagań systemowych, Architektura, Procesy definiowania i projektowania).

[82] Po wstępnym przeglądzie i zatwierdzeniu planu bezpieczeństwa systemu przez osobę autoryzującą, wszelkie dalsze działania związane z autoryzacją (np. Reautoryzacje lub bieżące autoryzacje) stanowią nieodłączny element przeglądu planu bezpieczeństwa systemu, ponieważ jest on zawarty w pakiecie autoryzacyjnym.

3.4 WDROŻENIE

CEL

Celem etapu **Wdrożenie** jest wdrożenie zabezpieczeń w planach bezpieczeństwa i ochrony prywatności systemu i organizacji oraz udokumentowanie w zestawie minimalnych zabezpieczeń konkretnych danych szczegółowych dotyczących wdrożenia zabezpieczeń.

WDROŻENIE ZADAŃ

Tabela 5 zawiera podsumowanie zadań i oczekiwanych wyników etapu *Wdrażanie* RMF.

Przedstawiono również obowiązujące konstrukcje Ram Cyberbezpieczeństwa.

TABELA 5: WDROŻENIE ZADAŃ I WYNIKI

Zadania	Wyniki
ZADANIE I-1 **WDROŻENIE ZABEZPIECZEŃ**	• Wdrożone są zabezpieczenia określone w planach bezpieczeństwa i ochrony prywatności. [*Ramy Cyberbezpieczeństwa*: **PR.IP-1**] • Metodologie bezpieczeństwa systemów i inżynierii prywatności są wykorzystywane do wdrażania zabezpieczeń w planach bezpieczeństwa systemów i ochrony prywatności. [*Ramy Cyberbezpieczeństwa*: **PR.IP-2**]

Zadania	Wyniki
ZADANIE I-2 **AKTUALIZACJA INFORMACJI O REALIZACJI ZABEZPIECZEŃ**	• Udokumentowane są zmiany w planowanym wdrożeniu zabezpieczeń. [*Ramy Cyberbezpieczeństwa*: **PR.IP-1**] • Plany bezpieczeństwa i ochrony prywatności są aktualizowane w oparciu o informacje uzyskane w trakcie przeprowadzania zabezpieczeń. [*Ramy Cyberbezpieczeństwa*: **profil**]

WDROŻENIE ZABEZPIECZEŃ

ZADANIE I-1 Wdrożenie zabezpieczeń w ramach planów bezpieczeństwa i ochrony prywatności.

Potencjalne dane wejściowe: Zatwierdzone plany bezpieczeństwa i ochrony prywatności; dokumenty projektowe systemu; polityka i procedury bezpieczeństwa i ochrony prywatności w organizacji; analizy wpływu biznesowego lub krytyczności; informacje dotyczące architektury korporacyjnej; informacje dotyczące architektury bezpieczeństwa; informacje dotyczące architektury prywatności; wykaz wymagań w zakresie bezpieczeństwa i ochrony prywatności przypisanych do systemu, elementów systemu oraz środowiska pracy; informacje dotyczące elementów systemu; inwentaryzacja elementów systemu; wyniki szacowania ryzyka na poziomie organizacji i systemu.

Oczekiwane wyniki: Wdrożone zabezpieczenia.

Podstawowa odpowiedzialność: SO; CCP.

Role wspierające: IO/S; SA; PA; SSE; PE; SSO; SPO; EA; SA.

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie; Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Organizacje wdrażają zabezpieczenia opisane w planach bezpieczeństwa i ochrony prywatności. Wdrożenie zabezpieczeń jest zgodne z architekturą korporacyjną organizacji i związanymi z nią konfiguracjami bezpieczeństwa i ochrony prywatności. Organizacje wykorzystują najlepsze praktyki podczas wdrażania zabezpieczeń, w tym metodologie, koncepcje i zasady dotyczące bezpieczeństwa systemów i inżynierii prywatności. Szacowanie ryzyka prowadzi i informuje o decyzjach dotyczących kosztów, korzyści i kompromisów w zakresie ryzyka przy stosowaniu różnych technologii lub zasad wdrażania zabezpieczeń. Organizacje zapewniają również, że obowiązkowe ustawienia konfiguracyjne są tworzone i wdrażane w elementach systemu zgodnie z obowiązującymi przepisami i polityką organizacyjną. W przypadku, gdy organizacje nie mają bezpośredniej kontroli nad tym, jakie zabezpieczenia są wdrażane w elementach systemu, na przykład w produktach komercyjnych (*ang. commercial off-the-shelf – COTS*), organizacje rozważają zastosowanie elementów systemu, które zostały przetestowane, ocenione lub zatwierdzone przez autoryzowane, niezależne, zewnętrzne instytucje oceniające. Testy, oceny i weryfikacje dotyczą produktów w określonych konfiguracjach i w izolacji[83]; wdrożenie zabezpieczeń dotyczy sposobu, w jaki produkt jest zintegrowany z systemem przy zachowaniu funkcjonalności i wiarygodności.

Organizacje zajmują się również, w stosownych przypadkach, wymogami dotyczącymi wiarygodności podczas wdrażania zabezpieczeń. Wymagania dotyczące wiarygodności zabezpieczeń są ukierunkowane na działania, które wykonują programiści i personel wdrażający zabezpieczenia w celu zwiększenia poziomu pewności, że zabezpieczenia są wdrażane prawidłowo, działają zgodnie z założeniami i przynoszą pożądane rezultaty w odniesieniu do spełniania wymogów bezpieczeństwa i ochrony prywatności systemu.

[83] Izolację należy rozumieć, jako badanie produktu w oderwaniu od środowiska, w którym ma pracować.

Wymagania w zakresie wiarygodności dotyczą jakości projektowania, opracowywania i wdrażania zabezpieczeń.[84]

W przypadku zabezpieczeń wspólnych odziedziczonych przez system, Inżynierowie bezpieczeństwa systemów i ochrony prywatności, wspierani przez personel ds. bezpieczeństwa i ochrony prywatności, koordynują działania z dostawcą zabezpieczeń wspólnych w celu określenia najbardziej odpowiedniego sposobu wdrożenia zabezpieczeń wspólnych. Właściciele systemów mogą odwoływać się do pakietów autoryzacyjnych przygotowanych przez dostawców zabezpieczeń wspólnych przy ustalaniu adekwatności zabezpieczeń wspólnych dziedziczonych przez ich systemy. W trakcie wdrażania można stwierdzić, że zabezpieczenia wspólne uprzednio wybrane do dziedziczenia przez system nie spełniają określonych wymogów bezpieczeństwa lub ochrony prywatności systemu. W przypadku zabezpieczeń wspólnych, które nie spełniają wymogów dotyczących systemu dziedziczącego zabezpieczenia lub gdy zabezpieczenia wspólne mają niedopuszczalne braki, właściciele systemu określają zabezpieczenia wyrównawcze lub uzupełniające, które należy wdrożyć. Właściciele systemów mogą uzupełniać zabezpieczenia wspólne o środki bezpieczeństwa specyficzne dla danego systemu lub zabezpieczenia hybrydowe w celu osiągnięcia wymaganej ochrony swoich systemów lub mogą zaakceptować większe ryzyko za potwierdzeniem przyjęcia i zgodą organizacji. W ramach szacowania ryzyka można określić, w jaki sposób luki w wymogach dotyczących bezpieczeństwa lub ochrony prywatności między systemami i zabezpieczeniami wspólnymi wpływają na ryzyko związane z systemem oraz w jaki sposób uszeregować pod względem ważności konieczność przeprowadzania zabezpieczeń kompensujących lub uzupełniających w celu ograniczenia określonego ryzyka.

Zgodnie z elastycznością dozwoloną przy realizacji zadań w RMF, organizacje przeprowadzają wstępne oceny zabezpieczeń podczas opracowywania i wdrażania systemu. Przeprowadzanie takich ocen równolegle z fazami rozwoju i wdrażania SDLC ułatwia wczesną identyfikację braków i stanowi efektywną kosztowo metodę inicjowania działań

[84] [NSC 800-53] zawiera listę środków bezpieczeństwa i ochrony prywatności związanych z wiarygodnością.

naprawczych. Problemy wykryte podczas tych ocen mogą być przekazywane do upoważnionych osób celem ich usunięcia. Wyniki wstępnych ocen zabezpieczeń mogą być również wykorzystane podczas etapu autoryzacji, aby uniknąć opóźnień lub kosztownego powtarzania ocen. Wyniki oceny, które są następnie ponownie wykorzystywane w innych fazach SDLC, spełniają wymagania dotyczące ponownego wykorzystania ustalone przez organizację.[85]

Referencje: [NSC 200]; [NSC 800-30]; [NSC 800-53]; [NSC 800-53A]; [SP 800-160 cz. 1] (Implementacja, integracja, weryfikacja i procesy przejściowe); [SP 800-161]; [IR 8062]; [IR 8179].

AKTUALIZACJA INFORMACJI O REALIZACJI ZABEZPIECZEŃ

ZADANIE I-2 Dokumentowanie zmian w planowanych wdrożeniach zabezpieczeń w stosunku do zaimplementowanych dotychczas zabezpieczeń.

Potencjalne dane wejściowe: Plany bezpieczeństwa i ochrony prywatności; informacje pochodzące z funkcjonowania zabezpieczeń.

Oczekiwane wyniki: Plany bezpieczeństwa i ochrony prywatności uaktualnione o szczegóły wykonawcze umożliwiające ich stosowanie przez podmioty oceniające zabezpieczenia; zestaw minimalnych zabezpieczeń systemu.

Podstawowa odpowiedzialność: SO; CCP.

Role wspierające: IO/S; SA; PA; SSE; PE; SSO; SPO; EA; SA.

[85] Informacje na temat oceny i ponownego wykorzystania wyników oceny można znaleźć w etapie Ocena RMF oraz w publikacji [NSC 800-53A].

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie; Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Pomimo zawarcia szczegółowych informacji na temat wdrożenia zabezpieczeń w planach bezpieczeństwa i ochrony prywatności oraz w dokumentach projektowych systemu, nie zawsze możliwe jest wdrożenie tych zabezpieczeń zgodnie z planem. W związku z tym, w miarę wprowadzania zabezpieczeń, plany bezpieczeństwa i ochrony prywatności są aktualizowane o szczegóły wdrażanych środków bezpieczeństwa. Aktualizacje zawierają poprawione opisy wdrożonych zabezpieczeń, w tym zmiany planowanych nakładów, oczekiwanego zachowania i oczekiwanych wyników, z wystarczającymi szczegółami, aby wspomóc ocenę zabezpieczeń. Udokumentowanie informacji o zaimplementowanym zabezpieczeniu jest niezbędne do zapewnienia możliwości określenia, kiedy nastąpią zmiany w zabezpieczeniu, czy zmiany te są autoryzowane, oraz wpływu tych zmian na bezpieczeństwo i prywatność systemu i organizacji.

Referencje: [NSC 800-53]; [SP 800-128]; [SP 800-160 cz. 1] (Implementacja, integracja, weryfikacja i przejście, Procesy zarządzania konfiguracją).

3.5 OCENA

CEL

Celem etapu ***OCENA*** jest ustalenie, czy środki bezpieczeństwa wybrane do wdrożenia są zaimplementowane prawidłowo, działają zgodnie z założeniami i dają pożądany rezultat w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatn ości systemu i organizacji.

OCENA ZADAŃ

Tabela 6 zawiera podsumowanie zadań i oczekiwanych wyników dla etapu *Oceny* RMF.

Przedstawiono również obowiązujące konstrukcje Ram Cyberbezpieczeństwa.

TABELA 6: OCENA ZADAŃ I WYNIKÓW

Zadania	Wyniki
ZADANIE A-1 **WYBÓR PODMIOTU OCENIAJĄCEGO**	• Do przeprowadzenia oceny zabezpieczeń wybierana jest podmiot oceniający lub zespół podmiot oceniający. • Osiągany jest odpowiedni poziom niezależności wybranej podmiotu podmiot oceniający lub zespołu podmiot oceniający.
ZADANIE A-2 **PLAN OCENY**	• Dokumentacja potrzebna do przeprowadzenia oceny jest dostarczana podmiotowi oceniającemu lub zespołowi podmiotowi oceniającemu. • Opracowywane i dokumentowane są plany oceny bezpieczeństwa i ochrony prywatności. • Plany oceny bezpieczeństwa i prywatności są poddawane przeglądowi i zatwierdzane w celu ustalenia oczekiwań dotyczących oceny zabezpieczeń i wymaganego poziomu nakładu.
ZADANIE A-3 **OCENA ZABEZPIECZEŃ**	• Ocena zabezpieczeń przeprowadzana jest zgodnie z planami oceny bezpieczeństwa i ochrony prywatności. • Rozważane są możliwości ponownego wykorzystania wyników poprzednich ocen

	w celu zapewnienia terminowości i opłacalności procesu zarządzania ryzykiem. • W celu zwiększenia szybkości, skuteczności i wydajności oceny zabezpieczeń wprowadzana jest optymalizacja wykorzystania systemów automatyzacji.
ZADANIE A-4 **SPRAWOZDANIA Z OCENY**	• Sporządzane są sprawozdania z oceny bezpieczeństwa i ochrony prywatności, przedstawiające ustalenia i zalecenia.
ZADANIE A-5 **DZIAŁANIA NAPRAWCZE**	• Podejmowane są działania naprawcze mające na celu usunięcie braków w zabezpieczeniach wdrożonych w systemie i środowisku pracy. • Plany bezpieczeństwa i ochrony prywatności są aktualizowane w celu odzwierciedlenia zmian w realizacji zabezpieczeń dokonanych w oparciu o oceny i późniejsze działania naprawcze. [*Ramy Cyberbezpieczeństwa*: **Profil**]
ZADANIE A-6 **PLAN I ETAPY DZIAŁAŃ**	• Opracowywany jest plan i etapy działań określające plany naprawcze dotyczące niedopuszczalnych zagrożeń zidentyfikowanych w sprawozdaniach z oceny bezpieczeństwa i ochrony prywatności. [*Ramy Cyberbezpieczeństwa:* **ID.RA-6**]

WYBÓR PODMIOTU OCENIAJĄCEGO

ZADANIE A-1 Wybór odpowiedniego podmiot oceniający lub zespołu podmiot oceniający do przeprowadzenia danego rodzaju oceny zabezpieczeń, która ma zostać przeprowadzona.

Potencjalne dane wejściowe: Bezpieczeństwo, prywatność i plany SCRM; informacje dotyczące zarządzania programem zabezpieczeń; dokumentacja zabezpieczeń wspólnych; bezpieczeństwo organizacyjne i plany programów ochrony prywatności; strategia SCRM; dokumentacja projektu systemu; informacje dotyczące przedsiębiorstwa, bezpieczeństwa i architektury prywatności; bezpieczeństwo, prywatność i zasady oraz procedury SCRM mające zastosowanie do systemu.

Oczekiwane wyniki: Wybór podmiotu podmiot oceniający lub zespołu podmiot oceniający odpowiedzialnego za przeprowadzenie oceny zabezpieczeń.

Podstawowa odpowiedzialność: AO lub AODR.

Role wspierające: CIO; SAISO; SAOP.

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie; Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Organizacje biorą pod uwagę zarówno wiedzę techniczną, jak i poziom niezależności wymagany przy wyborze osób oceniających zabezpieczenia.[86] Organizacje dbają o to, by podmioty oceniające zabezpieczenia posiadały wymagane umiejętności i wiedzę techniczną, pozwalającą opracowywać skuteczne plany oceny i przeprowadzać oceny zarządzania programem, zabezpieczeń właściwych dla danego systemu, zabezpieczeń hybrydowych i wspólnych, stosownie do potrzeb. Obejmuje to ogólną wiedzę na temat

[86] Niektóre organizacje mogą wybrać osoby oceniające zabezpieczenia przed etapem Oceny RMF w celu wsparcia oceny zabezpieczeń przeprowadzanych możliwie jak najwcześniej w trakcie cyklu życia systemu. Wczesna identyfikacja i wybór osób oceniających pozwala organizacjom na zaplanowanie działań oceniających, w tym uzgodnienie zakresu oceny. Organizacje wdrażające podejście inżynierii bezpieczeństwa systemów mogą również skorzystać z możliwości wczesnego wyboru podmiotów oceniających w celu wsparcia działań weryfikacyjnych i oceniających, które mają miejsce w trakcie całego cyklu życia systemu.

koncepcji i podejść w zakresie zarządzania ryzykiem, jak również wszechstronną wiedzę i doświadczenie w zakresie wdrażanych komponentów sprzętu, oprogramowania i oprogramowania sprzętowego. W organizacjach, w których zdolność do oceny jest zarządzana centralnie, SAISO może być odpowiedzialny za wybór i zarządzanie osobami oceniającymi środki bezpieczeństwa lub zespołami oceniającymi systemy organizacyjne. Ponieważ zabezpieczenia mogą być wdrażane w celu osiągnięcia celów w zakresie bezpieczeństwa i ochrony prywatności, organizacje biorą pod uwagę niezbędny stopień współpracy pomiędzy podmiotem oceniającymi środki bezpieczeństwa i ochrony prywatności.

Organizacje mogą przeprowadzić samoocenę zabezpieczeń lub skorzystać z usług niezależnego personelu podmiot oceniający zabezpieczenia. Niezależny podmiot oceniający to osoba lub grupa, która może przeprowadzić bezstronną ocenę. Bezstronność oznacza, że podmioty oceniające zabezpieczenia są wolne od postrzeganych lub rzeczywistych konfliktów interesów w odniesieniu do określania skuteczności zabezpieczeń lub rozwoju, funkcjonowania oraz zarządzania systemem, zabezpieczeń wspólnych lub programu zarządzania zabezpieczeniami. Osoba autoryzująca określa poziom niezależności podmiotu oceniającego w oparciu o obowiązujące prawo, zarządzenia, dyrektywy, regulacje, politykę lub standardy. Osoba autoryzująca współpracuje z CIO, SAOP i SAISO, aby pomóc w podejmowaniu decyzji dotyczących niezależności osób oceniających i informowaniu o podjętych decyzjach.

SPO jest odpowiedzialny za określenie metodologii oceny i metryk w celu ustalenia, czy zabezpieczenia w zakresie ochrony prywatności są wdrażane prawidłowo, działają zgodnie z założeniami i są wystarczające do zapewnienia zgodności z obowiązującymi wymogami w zakresie ochrony prywatności i zarządzania ryzykiem w zakresie ochrony prywatności. SAOP jest odpowiedzialny za przeprowadzanie oceny zabezpieczeń prywatności i dokumentowanie wyników tych ocen. Według uznania organizacji, zabezpieczenia w zakresie ochrony prywatności mogą być oceniane przez niezależną osobę autoryzującą. Jednakże, we wszystkich przypadkach, SAOP jest odpowiedzialny za program ochrony

prywatności organizacji, w tym za wszelkie funkcje związane z ochroną prywatności wykonywane przez niezależnych podmiot oceniających. SAOP jest odpowiedzialny za dostarczanie informacji o ochronie prywatności osobie autoryzującej.

Referencje: [NSC 199]; [NSC 800-30]; [NSC 800-53A]; [SP 800-55].

PLAN OCENY

ZADANIE A-2 Opracowanie, przegląd i zatwierdzenie planów oceny wdrożonych zabezpieczeń.

Potencjalne dane wejściowe: Bezpieczeństwo, prywatność i plany SCRM; informacje dotyczące programu zarządzania zabezpieczeniami; dokumentacja zabezpieczeń wspólnych; bezpieczeństwo organizacyjne i plany programów ochrony prywatności; strategia SCRM; dokumentacja projektu systemu; informacje dotyczące łańcucha dostaw; informacje dotyczące przedsiębiorstwa, bezpieczeństwa i architektury prywatności; bezpieczeństwo, prywatność i zasady oraz procedury SCRM mające zastosowanie do systemu.

Oczekiwane wyniki: Plany oceny bezpieczeństwa i prywatności zatwierdzone przez osobę autoryzującą.

Podstawowa odpowiedzialność: AO lub AODR; CA.

Role wspierające: SAISO; SAOP; SO; CCP; IO/S; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie; Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Plany oceny bezpieczeństwa i prywatności są opracowywane przez podmioty oceniające zabezpieczenia w oparciu o informacje dotyczące wdrażania zawarte w planach bezpieczeństwa i ochrony prywatności, dokumentację programu zarządzania zabezpieczeniami oraz dokumentację zabezpieczeń wspólnych. Organizacje mogą zdecydować się na opracowanie jednego, zintegrowanego planu oceny bezpieczeństwa i ochrony prywatności dla systemu lub organizacji. Zintegrowany plan oceny określa role

i obowiązki w zakresie oceny zabezpieczeń. Plany oceny zawierają również cele oceny zabezpieczeń i szczegółowe procedury oceny dla każdego zabezpieczenia. Plany oceny odzwierciedlają rodzaj oceny, jaką przeprowadza organizacja, w tym na przykład: testy rozwojowe i ocenę; niezależną weryfikację i walidację; audyty, w tym łańcucha dostaw; oceny wspierające system i zabezpieczenia wspólne oraz ponowne odnawianie autoryzacji zabezpieczeń; oceny programu zarządzania zabezpieczeniami; ciągły monitoring; oraz oceny przeprowadzane po działaniach naprawczych.

Plany oceny są przeglądane i zatwierdzane przez osobę autoryzującą lub wyznaczonego pełnomocnika w celu zapewnienia, że plany są zgodne z celami organizacji w zakresie bezpieczeństwa i ochrony prywatności; wykorzystują procedury, metody, techniki, narzędzia i automatyzację w celu wsparcia stałego monitorowania i zarządzania ryzykiem w czasie zbliżonym do rzeczywistego; oraz są opłacalne. Zatwierdzone plany oceny określają oczekiwania w zakresie oceny zabezpieczeń oraz poziom wysiłków związanych z oceną. Zatwierdzone plany oceny pomagają zapewnić stosowanie odpowiednich zasobów w celu określenia skuteczności zabezpieczeń, zapewniając jednocześnie niezbędny poziom zaufania przy dokonywaniu takich ustaleń. Jeśli zabezpieczenia są realizowane przez zewnętrznego dostawcę poprzez umowy, porozumienia międzyorganizacyjne, porozumienia branżowe, porozumienia licencyjne lub porozumienia dotyczące łańcucha dostaw, organizacja może zażądać od dostawcy planów oceny bezpieczeństwa i ochrony prywatności oraz wyników oceny lub dowodów.

Referencje: [NSC 800-53A]; [SP 800-160 cz. 1] (Procesy weryfikacji i walidacji); [SP 800-161]; [IR 8011 v1].

OCENA ZABEZPIECZEŃ

ZADANIE A-3 Ocena zabezpieczeń zgodnie z procedurami oceny opisanymi w planach oceny.

Potencjalne dane wejściowe: Plany oceny bezpieczeństwa i ochrony prywatności; plany bezpieczeństwa i ochrony prywatności; zewnętrzne wyniki oceny lub audytu (jeśli dotyczy).

Oczekiwane wyniki: Zakończone oceny zabezpieczeń i związane z nimi ewidencje przeprowadzonych ocen.

Podstawowa odpowiedzialność: CA.

Role wspierające: AO lub AODR; SO; CCP; IO/S; SAISO; SAOP; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie; Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Oceny zabezpieczeń określają stopień, w jakim wybrane zabezpieczenia są realizowane prawidłowo, działają zgodnie z założeniami i przynoszą pożądany rezultat w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatności systemu i organizacji. Właściciel systemu, dostawca zabezpieczeń wspólnych i/lub organizacja polegają na umiejętnościach technicznych i wiedzy fachowej podmiotów oceniających, aby ocenić wdrożone mechanizmy bezpieczeństwa z wykorzystaniem procedur oceny określonych w planach oceny i przedstawić zalecenia dotyczące sposobu reagowania na niedociągnięcia środków bezpieczeństwa w celu zmniejszenia lub wyeliminowania zidentyfikowanych podatności lub niedopuszczalnych zagrożeń. SAOP pełni funkcję podmiotu podmiot oceniający zabezpieczenia w zakresie ochrony prywatności i jest odpowiedzialny za przeprowadzenie wstępnej oceny zabezpieczeń w zakresie ochrony prywatności przed uruchomieniem systemu, a następnie za okresową ocenę zabezpieczeń z częstotliwością wystarczającą do zapewnienia zgodności z wymogami dotyczącymi ochrony prywatności i zarządzania zagrożeniami dla prywatności. [87] Zabezpieczenia wprowadzane w celu osiągnięcia zarówno celów w zakresie bezpieczeństwa, jak i prywatności, mogą wymagać pewnego stopnia współpracy pomiędzy podmiotem oceniającymi bezpieczeństwo i prywatność. Ustalenia podmiotu podmiot oceniający stanowią rzeczowe sprawozdanie na

[87] SAOP może delegować funkcje związane z oceną, zgodnie z obowiązującymi zasadami.

temat tego, czy zabezpieczenia funkcjonują zgodnie z założeniami i czy podczas oceny wykryto jakiekolwiek podatności[88] w zabezpieczeniach.

Oceny zabezpieczeń pojawiają się w SDLC tak wcześnie, jak to możliwe, najlepiej w fazie rozwoju. Tego typu oceny są określane, jako testy i oceny rozwojowe i potwierdzają, że zabezpieczenia są wdrażane prawidłowo i są zgodne z ustaloną architekturą bezpieczeństwa informacji i ochrony prywatności. Testy rozwojowe i oceny obejmują, na przykład, przegląd projektu i kodu, testy regresji i skanowanie aplikacji. Braki wykryte na wczesnym etapie SDLC mogą być rozwiązane w bardziej ekonomiczny sposób. Oceny mogą być potrzebne przed wyborem źródła podczas procesu zakupu, aby ocenić potencjalnych dostawców lub usługodawców przed zawarciem przez organizację umów lub kontraktów na rozpoczęcie fazy rozwojowej. Wyniki ocen zabezpieczeń przeprowadzonych podczas SDLC mogą być również wykorzystane (zgodnie z kryteriami ponownego wykorzystania ustalonymi przez organizację) podczas procesu autoryzacji w celu uniknięcia niepotrzebnych opóźnień lub kosztownych powtórzeń ocen. Organizacje mogą zmaksymalizować wykorzystanie automatyzacji do przeprowadzania ocen zabezpieczeń w celu zwiększenia szybkości, skuteczności i wydajności ocen oraz wsparcia ciągłego monitorowania bezpieczeństwa i ochrony prywatności systemów organizacyjnych.

Stosowanie i ocena zabezpieczeń w całym procesie rozwoju mogą być właściwe dla powtarzających się procesów rozwoju. W przypadku stosowania iteracyjnych procesów rozwojowych (np. rozwój zwinny), ocena iteracyjna może być przeprowadzana po zakończeniu każdego cyklu. Podobny proces jest stosowany do oceny środków bezpieczeństwa w komercyjnych produktach informatycznych, które są wykorzystywane w systemie. Organizacje mogą podjąć decyzję o rozpoczęciu oceny zabezpieczeń przed całkowitym wdrożeniem wszystkich środków bezpieczeństwa w planach bezpieczeństwa

[88] Za podatności uważa się jedynie niedociągnięcia w zakresie zabezpieczeń, które mogą być wykorzystywane przez agentów (aktorów) zagrożeń.

i ochrony prywatności. Ten rodzaj oceny przyrostowej jest odpowiedni, jeśli jest to bardziej efektywne lub opłacalne.

Zabezpieczenia wspólne (tj. zabezpieczenia, które są dziedziczone przez system) są oceniane oddzielnie (przez osoby oceniające ustanawiane przez podmioty świadczące usługi zabezpieczeń wspólnych lub organizację) i nie muszą być oceniane, jako część oceny na poziomie systemu.

Organizacje zapewniają, że podmioty oceniające zabezpieczenia mają dostęp do systemu informatycznego i środowiska działania, w którym realizowane są zabezpieczenia oraz do dokumentacji, zapisów, artefaktów, wyników badań i innych materiałów potrzebnych do oceny zabezpieczeń. Obejmuje to zabezpieczenia wdrażane przez zewnętrznych dostawców poprzez umowy, porozumienia międzyorganizacyjne, uzgodnienia dotyczące kierunków działalności, umowy licencyjne lub uzgodnienia dotyczące łańcucha dostaw. Podmiot oceniający posiadają wymagany stopień niezależności, określony przez osobę autoryzującą. Niezależność asesora podczas procesu stałego monitorowania ułatwia ponowne wykorzystanie wyników oceny w celu wsparcia bieżących upoważnień i ponownych upoważnień.

Chcąc uczynić proces zarządzania ryzykiem bardziej efektywnym i opłacalnym, organizacje mogą zdecydować się na ustalenie rozsądnych i odpowiednich kryteriów ponownego wykorzystywania wyników oceny w ramach polityki oceny w skali całej organizacji lub w planach programów bezpieczeństwa i ochrony prywatności. Na przykład, ostatni audyt systemu mógł dostarczyć informacji o skuteczności wybranych zabezpieczeń. Inną możliwością ponownego wykorzystania wcześniejszych wyników oceny mogą być programy zewnętrzne, które testują i oceniają cechy bezpieczeństwa i prywatności komercyjnych produktów informatycznych. Jeżeli dostępne są wcześniejsze wyniki oceny uzyskane od producenta lub dostawcy systemu, podmiot oceniający zabezpieczenie może, w odpowiednich okolicznościach, włączyć te wyniki do oceny. Ponadto, jeśli implementacja zabezpieczeń została oceniona podczas innych form oceny na wcześniejszych etapach SDLC

(np. testy jednostkowe, testy funkcjonalne, testy akceptacyjne), organizacje mogą rozważyć potencjalne ponowne wykorzystanie tych wyników w celu ograniczenia dublowania wysiłków. I wreszcie, wyniki oceny mogą być ponownie wykorzystane do wspierania wzajemności, na przykład, wyniki oceny wspierające wydanie zezwolenia na użytkowanie (zob. Załącznik F). Dodatkowe informacje dotyczące ponownego wykorzystania wyników oceny są dostępne w publikacji [NSC 800-53A].

Referencje: [NSC 800-53A]; [SP 800-160 cz. 1] (Procesy weryfikacji i walidacji); [IR 8011 v1].

SPRAWOZDANIA Z OCENY

ZADANIE A-4 Przygotowanie sprawozdań z oceny dokumentujących ustalenia i zalecenia wynikające z oceny zabezpieczeń.

Potencjalne dane wejściowe: Zakończone oceny zabezpieczeń i związane z nimi ewidencje oceny.

Oczekiwane wyniki: Ukończone raporty z oceny bezpieczeństwa i ochrony prywatności, zawierające szczegółowe ustalenia i zalecenia podmiotu podmiot oceniający.

Podstawowa odpowiedzialność: CA.

Role wspierające: SO; CCP; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie; Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Wyniki ocen środków bezpieczeństwa i ochrony prywatności, w tym zalecenia dotyczące skorygowania niedociągnięć we wprowadzonych zabezpieczeniach, są dokumentowane w sprawozdaniach z oceny[89] przez podmioty oceniające zabezpieczenia. Organizacje mogą opracować jeden, zintegrowany raport z oceny bezpieczeństwa i ochrony prywatności. Raporty oceniające są kluczowymi dokumentami w systemie lub pakiecie

[89] Jeżeli raporty porównawcze spełniają wymogi dotyczące tego, co ma być zawarte w sprawozdaniu z oceny, wówczas raport porównawczy stanowiłby sprawozdanie z oceny.

wspólnych zabezpieczeń, które są opracowywany w celu autoryzacji przez osoby autoryzujące. Raporty oceniające zawierają informacje oparte na ustaleniach podmiotów oceniających, niezbędne do określenia skuteczności zabezpieczeń wdrożonych w ramach systemu informatycznego lub przez niego dziedziczonych. Raporty oceniające opracowywane przez osobę autoryzującą są ważnym czynnikiem określającym ryzyko dla działalności i majątku organizacji, osób, innych organizacji i Państwa. Format i poziom szczegółowości przedstawiony w sprawozdaniach z oceny jest odpowiedni dla rodzaju przeprowadzonej oceny zabezpieczeń, na przykład badania i oceny rozwojowej; niezależnej weryfikacji i walidacji; niezależnych ocen wspomagających system informatyczny lub autoryzacje / ponowne autoryzacje zabezpieczeń wspólnych; samooceny; ocen po działaniach naprawczych; niezależnych ocen lub audytów; oraz ocen podczas ciągłego monitorowania. Format sprawozdania może być również określony przez organizację.

Wyniki oceny zabezpieczeń uzyskane w trakcie cyklu rozwoju systemu są dokumentowane w raporcie okresowym i włączane do końcowych sprawozdań z oceny bezpieczeństwa i ochrony prywatności. Opracowanie raportów okresowych, które dokumentują wyniki oceny z odpowiednich faz SDLC, wzmacnia koncepcję, że raporty oceniające są dokumentami ewoluującymi. Raporty okresowe są wykorzystywane, w stosownych przypadkach, do informowania o końcowym raporcie podmiotem oceniającym. Organizacje mogą zdecydować się na opracowanie streszczenia wyników oceny zabezpieczeń. Streszczenie dostarcza upoważnionym oraz zainteresowanym osobom w organizacji skróconą wersję raportów podmiot oceniających, która zawiera streszczenie oceny, ustalenia i zalecenia dotyczące usunięcia braków w zabezpieczeniach.

Referencje: [NSC 800-53A]; [SP 800-160 cz. 1] (Procesy weryfikacji i walidacji).

DZIAŁANIA NAPRAWCZE

ZADANIE A-5 Przeprowadzenie wstępnych działań korygujących w zakresie środków bezpieczeństwa i ponownej oceny skorygowanych zabezpieczeń.

Potencjalne dane wejściowe: Kompletne raporty z oceny bezpieczeństwa i ochrony prywatności wraz z wnioskami i zaleceniami; plany bezpieczeństwa i ochrony prywatności; plany oceny bezpieczeństwa i ochrony prywatności; wyniki szacowania ryzyka na poziomie organizacji i systemu.

Oczekiwane wyniki: Zakończenie wstępnych działań naprawczych w oparciu o raporty z oceny bezpieczeństwa i prywatności; zmiany we wdrożeniach ponownie ocenionych przez zespół podmiot oceniający; zaktualizowane raporty z oceny bezpieczeństwa i ochrony prywatności; zaktualizowane plany bezpieczeństwa i ochrony prywatności, w tym zmiany we wdrożeniach zabezpieczeń.

Podstawowa odpowiedzialność: SO; CCP; CA.

Role wspierające: AO lub AODR; SAISO; SAOP; SAORM lub RE; IO/S; SSE; PE; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy - Rozwój/Nabycie; Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Raporty z oceny bezpieczeństwa i ochrony prywatności opisują braki w zabezpieczeniach, których nie można było usunąć w trakcie opracowywania systemu lub które zostały wykryte po jego opracowaniu. Takie niedociągnięcia w zakresie zabezpieczeń mogą prowadzić do zagrożeń dla bezpieczeństwa i prywatności (w tym zagrożeń dla łańcucha dostaw). Wyniki uzyskane podczas oceny zabezpieczeń dostarczają informacji, które ułatwiają reagowanie na ryzyko w oparciu o organizacyjną tolerancję na ryzyko i priorytety. Osoba autoryzująca, w porozumieniu i koordynacji z właścicielami systemu i innym personelem organizacji, może zdecydować, że niektóre ustalenia stanowią znaczące, niedopuszczalne ryzyko i wymagają natychmiastowych działań naprawczych. Dodatkowo, możliwe i praktyczne może być przeprowadzenie wstępnych działań naprawczych w związku z wynikami oceny, które mogą być szybko i łatwo naprawione przy użyciu istniejących zasobów.

Jeżeli zostaną podjęte wstępne działania naprawcze, podmioty oceniające zabezpieczenia ponownie oceniają zabezpieczenia. Ponowna ocena zabezpieczeń określa zakres, w jakim naprawione środki bezpieczeństwa są wykonywane prawidłowo, działają zgodnie z założeniami i przynoszą pożądany rezultat w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatności systemu i organizacji. Podmioty oceniające zabezpieczenia aktualizują sprawozdania z oceny o ustalenia z ponownej oceny, ale nie zmieniają pierwotnych wyników oceny. Plany bezpieczeństwa i ochrony prywatności są aktualizowane w oparciu o wyniki ocen zabezpieczeń i podjęte wszelkie działania naprawcze. Zaktualizowane plany odzwierciedlają stan zabezpieczeń po wstępnej ocenie oraz wszelkie zmiany wprowadzone przez właściciela systemu lub dostawcę zabezpieczeń wspólnych w odniesieniu do zaleceń dotyczących działań naprawczych. Po zakończeniu oceny zabezpieczeń, plany bezpieczeństwa i ochrony prywatności zawierają dokładny opis wdrożonych mechanizmów bezpieczeństwa, w tym zabezpieczeń kompensacyjnych.

Organizacje mogą przygotować dodatek do raportów z oceny bezpieczeństwa i ochrony prywatności, który daje właścicielom systemów i dostawcom zabezpieczeń wspólnych możliwość zareagowania na wstępne wyniki oceny. Uzupełnienie może zawierać, na przykład, informacje dotyczące wstępnych działań naprawczych podjętych przez właścicieli systemów lub dostawców zabezpieczeń wspólnych w odpowiedzi na wyniki oceny. W uzupełnieniu można również przedstawić właścicielowi systemu lub dostawcom zabezpieczeń wspólnych perspektywy dotyczące ustaleń. Może to obejmować dostarczenie dodatkowych materiałów wyjaśniających, odrzucenie niektórych ustaleń i poprawienie dokumentacji. Uzupełnienie nie zmienia, ani nie wpływa na wstępne ustalenia podmiotu podmiot oceniający przedstawione w sprawozdaniach. Informacje przedstawione w uzupełnieniu są rozpatrywane przez upoważniony personel przy podejmowaniu decyzji o autoryzacji opartej na analizie ryzyka. Organizacje wdrażają proces mający na celu określenie wstępnych działań, które należy podjąć w związku z niedociągnięciami zabezpieczeń stwierdzonymi podczas oceny. Proces ten może dotyczyć podatności i zagrożeń, wyników fałszywie dodatnich i innych czynników, które dostarczają użytecznych

informacji osobom autoryzującym w zakresie bezpieczeństwa i ochrony prywatności systemu i organizacji, w tym bieżącej skuteczności zabezpieczeń specyficznych dla systemu, hybrydowych i wspólnych. Proces rozwiązywania problemów może również zapewnić, że tylko istotne elementy zostaną zidentyfikowane i przeniesione do planu i etapów działań.

Ustalenia z oceny zabezpieczeń na poziomie systemu mogą wymagać aktualizacji szacowania ryzyka systemowego i szacowania ryzyka organizacyjnego.[90] Uaktualnione szacowanie ryzyka oraz wszelkie informacje przekazane przez wyższego rangą lidera odpowiedzialnego za zarządzanie ryzykiem lub wykonawcę (funkcję) ryzyka, określają wstępne działania naprawcze oraz priorytety tych działań. Właściciele systemów i dostawcy zabezpieczeń wspólnych mogą zdecydować, w oparciu o ocenę ryzyka systemowego lub organizacyjnego, że pewne ustalenia są nieistotne i nie stanowią istotnego zagrożenia dla bezpieczeństwa lub ochrony prywatności. Takie ustalenia są zachowywane w raportach z oceny bezpieczeństwa i ochrony prywatności oraz monitorowane na etapie monitorowania. Osoba autoryzująca jest odpowiedzialna za przegląd i zrozumienie ustaleń podmiotu podmiot oceniający oraz za zaakceptowanie zagrożeń dla bezpieczeństwa i prywatności (w tym wszelkich zagrożeń dla łańcucha dostaw), które wynikają z funkcjonowania systemu lub stosowania zabezpieczeń wspólnych.

We wszystkich przypadkach organizacje dokonują przeglądu ustaleń osoby oceniającej w celu określenia znaczenia tych ustaleń oraz tego, czy wymagają one dalszych czynności lub prowadzenia działań naprawczych. Zaangażowanie kadry kierowniczej wyższego szczebla w proces łagodzenia skutków jest konieczne, aby zapewnić, że zasoby organizacji są efektywnie przydzielane zgodnie z priorytetami organizacji - zapewniając zasoby do systemów, które wspierają najbardziej krytyczne misje i funkcje biznesowe lub korygując braki, które stwarzają największe ryzyko.

[90] Szacowanie ryzyka jest przeprowadzane w zależności od potrzeb na poziomie organizacyjnym, misji/biznesu oraz na poziomie systemu w całym SDLC. Szacowanie ryzyka jest określane, jako część kroku Poziom przygotowania organizacji RMF, zadanie P-3 oraz Poziom przygotowania systemu RMF, zadanie P-14.

Referencje: [NSC 800-53A]; [SP 800-160 cz. 1] (Procesy weryfikacji i walidacji).

PLAN I ETAPY DZIAŁAŃ

ZADANIE A-6 Przygotowanie planu działania i głównych etapów w oparciu o ustalenia i zalecenia zawarte w sprawozdaniach z oceny.

Potencjalne dane wejściowe: Uaktualnione raporty oceny bezpieczeństwa i ochrony prywatności; uaktualnione plany bezpieczeństwa i ochrony prywatności; wyniki szacowania ryzyka na poziomie organizacji i systemu; strategia zarządzania ryzykiem organizacyjnym i tolerancja ryzyka.

Oczekiwane wyniki: Plan i etapy działań wyszczególniające ustalenia ze sprawozdań z oceny bezpieczeństwa i ochrony prywatności, które mają zostać naprawione.

Podstawowa odpowiedzialność: SO; CCP.

Role wspierające: IO/S; SSO; SPO; SAISO; SAOP; CA; CAO.

Faza rozwoju cyklu życia systemu: Nowy – Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Plan i etapy działania zawarte są w pakiecie autoryzacyjnym. Plan i etapy działania opisują działania, które są planowane w celu skorygowania braków w zabezpieczeniach zidentyfikowanych podczas oceny mechanizmów bezpieczeństwa i podczas ciągłego monitorowania. Plan i etapy działania obejmują zadania, które mają być wykonane z zaleceniem ukończenia przed lub po autoryzacji systemu; zasoby wymagane do wykonania zadań; etapy działania ustalone w celu wykonania zadań; oraz planowane terminy wykonania planowanych etapów działań. Plan i etapy działań są weryfikowane przez osobę autoryzującą w celu zapewnienia zgodności z planowanymi działaniami naprawczymi mającymi na celu usunięcie zidentyfikowanych niedociągnięć. Jest on następnie wykorzystywany do monitorowania postępów w realizacji działań. Niedociągnięcia są akceptowane przez osobę autoryzującą, jako ryzyko szczątkowe lub są usuwane podczas

oceny lub przed złożeniem pakietu autoryzacyjnego do osobę autoryzującą. Plan i etapy działań nie są konieczne, gdy braki są akceptowane przez osobę autoryzującą, jako ryzyko szczątkowe. Braki wykryte podczas oceny i monitorowania są jednak dokumentowane w sprawozdaniach z oceny, które mogą być zachowane w ramach zautomatyzowanego narzędzia zarządzania bezpieczeństwem/prywatnością i sprawozdawczości w celu utrzymania skutecznej ścieżki audytu. Organizacje opracowują plany i etapy działań w oparciu o wyniki oceny uzyskane z ocen kontrolnych, audytów i ciągłego monitorowania oraz zgodnie z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, politykami, regulacjami, standardami lub wytycznymi.

Organizacje wdrażają spójny proces opracowywania planów i etapów działań, w którym stosuje się jednolite dla całej organizacji, priorytetowe podejście do ograniczania ryzyka. Szacowanie ryzyka ukierunkowuje proces ustalania priorytetów dla pozycji zawartych w planie i etapach działania. Proces ten zapewnia, że plany działania i kluczowe etapy są uwzględniane podczas kategoryzacji bezpieczeństwa systemu oraz ocenach ryzyka w zakresie bezpieczeństwa, prywatności i łańcucha dostaw; konkretnych brakach w zakresie zabezpieczeń; krytyczności zidentyfikowanych braków w zakresie mechanizmów bezpieczeństwa (tj. bezpośredni lub pośredni wpływ, jaki uchybienia mogą mieć na bezpieczeństwo i prywatność systemu, a tym samym na ekspozycję organizacji na ryzyko; lub na zdolność organizacji do wykonywania jej misji lub funkcji biznesowych); oraz proponowane podejście do ograniczania ryzyka w celu wyeliminowania zidentyfikowanych uchybień w zakresie zabezpieczeń (np. priorytetyzacja działań ograniczających ryzyko i alokacja zasobów ograniczających ryzyko). Zasoby ograniczające ryzyko obejmują na przykład personel, nowy sprzęt lub oprogramowanie oraz narzędzia.

Referencje: [NSC 800-30]; [NSC 800-53A]; [SP 800-160 cz. 1] (Procesy weryfikacji i walidacji); [IR 8062].

3.6 AUTORYZACJA

CEL

Celem etapu *Autoryzacji* jest zapewnienie odpowiedzialności organizacyjnej poprzez wymaganie od lidera wyższego szczebla zarządzania określenia, czy ryzyko związane z bezpieczeństwem i prywatnością (w tym ryzyko związane z łańcuchem dostaw) operacji organizacyjnych i aktywów, osób, innych organizacji lub Państwa w oparciu o działanie systemu lub stosowanie zabezpieczeń wspólnych, jest dopuszczalne.

AUTORYZACJA ZADAŃ

Tabela 7 zawiera podsumowanie zadań i oczekiwanych wyników dla etapu *Autoryzacja* RMF.

Przedstawiono również obowiązujące konstrukcje Ram Cyberbezpieczeństwa.

TABELA 7: AUTORYZACJA ZADAŃ I WYNIKÓW

Zadania	Wyniki
ZADANIE R-1 **PAKIET AUTORYZACYJNY**	• Pakiet autoryzacyjny jest opracowywany w celu przedłożenia go osobie autoryzującej.
ZADANIE R-2 **ANALIZA I OKREŚLENIE RYZYKA**	• Ustalenie ryzyka przez osobę autoryzującą, które odzwierciedla strategię zarządzania ryzykiem, w tym tolerancję ryzyka.
ZADANIE R-3 **REAKCJA NA RYZYKO**	• Zapewnienie reakcji na określone ryzyko. [*Ramy Cyberbezpieczeństwa:* **ID.RA-6**]

Zadania	Wyniki
ZADANIE R-4 **DECYZJA AUTORYZUJĄCA**	• Zatwierdza się lub odmawia autoryzacji systemu lub zabezpieczeń wspólnych.
ZADANIE R-5 **SPRAWOZDANIA Z AUTORYZACJI**	• Decyzje autoryzacyjne, istotne podatności i ryzyka są zgłaszane kierownictwu organizacji.

PAKIET AUTORYZACYJNY

ZADANIE R-1 Skompletowanie pakietu autoryzacyjnego i przedłożenie go osobie autoryzującej w celu podjęcia decyzji o autoryzacji.

Potencjalne dane wejściowe: Plany bezpieczeństwa i ochrony prywatności; sprawozdania z oceny bezpieczeństwa i ochrony prywatności; plan i etapy działania; dowody potwierdzające ocenę lub inna dokumentacja, w zależności od potrzeb.

Oczekiwane wyniki: Pakiet autoryzacyjny (z podsumowaniem), który może być wygenerowany z narzędzia zarządzania bezpieczeństwem lub ochroną prywatności[91] w celu przesłania do osoby autoryzującej.

Podstawowa odpowiedzialność: SO; CCP; SAOP[92].

Role Wspierające: SSO; SPO; SAISO; CA.

[91] Organizacje są zachęcane do maksymalnego wykorzystania zautomatyzowanych narzędzi w procesie przygotowania, opracowywania i przekazywania pakietów autoryzacyjnych oraz informacji dotyczących bezpieczeństwa i ochrony prywatności wspierających proces autoryzacji. Wiele dostępnych na rynku narzędzi do zarządzania ryzykiem i zgodnością (*ang. Governance, risk, and compliance* - GRC) może być stosowanych w celu ograniczenia lub wyeliminowania dokumentacji w formie papierowej.

[92] SAOP jest aktywny w zakresie systemów informatycznych przetwarzających informacje z zakresu ochrony danych osobowych.

Faza rozwoju cyklu życia systemu: Nowy – Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Pakiety autoryzacyjne zawierają plany bezpieczeństwa i ochrony prywatności, raporty z oceny bezpieczeństwa i ochrony prywatności, plany i etapy działań oraz podsumowanie. Dodatkowe informacje mogą być zawarte w pakiecie autoryzacyjnym na życzenie osoby autoryzującej. Organizacje utrzymują kontrolę wersji i zmian w miarę aktualizacji informacji zawartych w pakiecie autoryzacyjnym. Dostarczanie na bieżąco aktualizacji planów, raportów podmiot oceniających oraz planów i etapów działań wspiera koncepcję zarządzania ryzykiem w czasie zbliżonym do rzeczywistego oraz bieżącą autoryzację i w razie potrzeby może być wykorzystane do działań autoryzacyjnych.

SAOP dokonuje przeglądu pakietu autoryzacyjnego dla systemów przetwarzających dane osobowe w celu zapewnienia zgodności z obowiązującymi wymogami w zakresie ochrony prywatności i zarządzania ryzykiem w zakresie ochrony prywatności, przed dokonaniem autoryzacji przez personel podejmujący decyzje dotyczące określenia ryzyka i akceptacji.

Informacje zawarte w pakiecie autoryzacyjnym są wykorzystywane przez upoważniony personel do podejmowania świadomych, opartych na ryzyku decyzji. W przypadku, gdy zabezpieczenia są wdrażane przez zewnętrznego dostawcę poprzez umowy, porozumienia międzyorganizacyjne, porozumienia branżowe, umowy licencyjne lub porozumienia dotyczące łańcucha dostaw, organizacja zapewnia, że informacje potrzebne do podejmowania decyzji opartych na ryzyku są udostępniane przez dostawcę.

Pakiet autoryzacyjny może zostać dostarczony osobie autoryzującej w formie papierowej lub elektronicznej lub może zostać wygenerowany przy użyciu automatycznego narzędzia do zarządzania bezpieczeństwem/prywatnością i raportowania. Organizacje mogą korzystać ze zautomatyzowanych narzędzi wsparcia przy przygotowywaniu i zarządzaniu treścią pakietu autoryzacyjnego. Zautomatyzowane narzędzia wsparcia stanowią skuteczne narzędzie do utrzymywania i aktualizacji informacji dla osób autoryzujących w zakresie bieżącego bezpieczeństwa i ochrony prywatności systemów informatycznych w organizacji.

Jeżeli system informatyczny jest w trakcie bieżącej autoryzacji, pakiet autoryzacyjny jest przedstawiany autoryzującemu personelowi za pomocą automatycznych raportów w celu dostarczenia informacji w możliwie najbardziej efektywny i terminowy sposób.[93] Informacje, które mają być przedstawione osobie autoryzującej w raportach podmiot oceniających, są generowane w formacie i z częstotliwością określoną przez organizację, z wykorzystaniem informacji z programów ciągłego monitorowania bezpieczeństwa informacji i ochrony prywatności.

Sprawozdania z oceny przedstawione osobie autoryzującej zawierają informacje o brakach w zabezpieczeniach specyficznych dla danego systemu, hybrydowych i wspólnych (tj. innych niż zadowalające ustalenia określone przez podmiot oceniających). Osoba autoryzująca korzysta ze zautomatyzowanych narzędzi zarządzania bezpieczeństwem / prywatnością oraz sprawozdawczości lub innych zautomatyzowanych metod, gdy tylko jest to możliwe, w celu uzyskania dostępu do planów bezpieczeństwa i ochrony prywatności oraz planów i etapów działań. Dokumenty upoważniające są aktualizowane z częstotliwością określoną przez organizację przy użyciu zautomatyzowanych lub ręcznych procesów, zgodnie z celami zarządzania ryzykiem w organizacji.[94]

Referencje: [OMB A-130]; [NSC 800-18]; [SP 800-160 cz. 1] (Proces zarządzania ryzykiem); [SP 800-161] (Plany SCRM).

[93] Pomimo, że celem jest pełna automatyzacja wszystkich składników pakietu autoryzacyjnego, organizacje mogą znajdować się w różnych stanach przejścia do w pełni zautomatyzowanego stanu, tzn. Pewne sekcje pakietu autoryzacyjnego są dostępne za pomocą środków automatycznych, a inne sekcje są dostępne tylko za pomocą środków ręcznych.

[94] Organizacje decydują o poziomie szczegółowości i formacie prezentacji informacji dotyczących bezpieczeństwa i ochrony prywatności, które są udostępniane osobie autoryzującej z wykorzystaniem automatyzacji. Decyzje o poziomie szczegółowości i formacie są podejmowane w oparciu o potrzeby organizacyjne z automatyczną prezentacją informacji o bezpieczeństwie i ochronie prywatności, dostosowaną do potrzeb decyzyjnych osób autoryzujących. Na przykład, szczegółowe informacje dotyczące bezpieczeństwa i ochrony prywatności mogą być generowane i gromadzone na poziomie operacyjnym organizacji, a następnie analizowane, filtrowane i przedstawiane osobom autoryzującym w formacie podsumowującym lub wyróżnionym za pomocą automatyzacji.

ANALIZA I OKREŚLENIE RYZYKA

ZADANIE R-2 Analiza i określenie ryzyka związanego z działaniem lub użytkowaniem systemu lub zapewnieniem zabezpieczeń wspólnych.

Potencjalne dane wejściowe: Pakiet autoryzacyjny; dowody potwierdzające ocenę lub inna wymagana dokumentacja; informacje dostarczone przez wyższy personel odpowiedzialny za zarządzanie ryzykiem lub wykonawca (funkcja) ryzyka; strategia zarządzania ryzykiem organizacyjnym i tolerancja ryzyka; wyniki szacowania ryzyka na poziomie organizacji i systemu.

Oczekiwane wyniki: Określenie ryzyka.

Podstawowa odpowiedzialność: AO lub AODR.

Role wspierające: SAORM lub RE; SAISO; SAOP.

Faza rozwoju cyklu życia systemu: Nowy – Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Osoba autoryzująca lub pełnomocnik osoby autoryzującej, we współpracy z personelem wyższego szczebla ds. bezpieczeństwa informacji organizacji i personelem wyższego szczebla ds. ochrony prywatności (w przypadku systemów informatycznych przetwarzających dane osobowe), analizuje informacje zawarte w pakiecie autoryzacyjnym dostarczonym przez podmiot oceniający, właściciela systemu lub dostawcę zabezpieczeń wspólnych i finalizuje określenie ryzyka. W celu zapewnienia dokładnego zrozumienia ryzyka przez osobę autoryzującą może być konieczna dodatkowa wymiana informacji z podmiotem oceniającym zabezpieczenia, właścicielem systemu lub dostawcą zabezpieczeń wspólnych.

Szacowanie ryzyka stosowane jest w celu dostarczenia informacji[95], które mogą mieć wpływ na analizę i określenie ryzyka. SAORM lub RE może dostarczyć dodatkowych informacji

[95] [NSC 800-30] zawiera wytyczne dotyczące przeprowadzania szacowania ryzyka dla bezpieczeństwa. [IR 8062] zawiera informacje na temat szacowania ryzyka związanego z ochroną prywatności i związanych z nim czynników ryzyka.

osobie autoryzującej, które są brane pod uwagę przy ostatecznym ustalaniu ryzyka dla operacji organizacyjnych i aktywów, osób, innych organizacji i Państwa, wynikającego z działania lub wykorzystania systemu lub zapewnienia zabezpieczeń wspólnych. Dodatkowe informacje mogą obejmować, na przykład, tolerancję na ryzyko organizacyjne, zależności pomiędzy systemami i zabezpieczeniami, misję i wymagania biznesowe, krytyczność misji lub funkcji biznesowych wspieranych przez system, lub strategię zarządzania ryzykiem.

Osoba autoryzująca analizuje informacje dostarczone przez wyższy rangą personel odpowiedzialny za zarządzanie ryzykiem lub wykonawcę (funkcję) ryzyka oraz informacje dostarczone przez właściciela systemu lub dostawcę zabezpieczeń wspólnych w pakiecie autoryzacyjnym przy określaniu ryzyka. Wszelkie dodatkowe informacje dostarczone przez personel wyższego szczebla odpowiedzialny za zarządzanie ryzykiem lub wykonawcę (funkcję) ryzyka są dokumentowane i włączane, w zakresie, w jakim jest to istotne, jako część decyzji autoryzacyjnej (zob. Zadanie R-4). Osoba autoryzująca może również skorzystać ze zautomatyzowanego narzędzia do zarządzania bezpieczeństwem/prywatnością i sprawozdawczości w celu dokonania adnotacji na temat danych wejściowych dotyczących zarządzania ryzykiem lub wprowadzenie danych dotyczących zarządzania ryzykiem (funkcji).

W przypadku, gdy system działa na podstawie bieżącej autoryzacji, zadanie określenia ryzyka praktycznie nie ulega zmianie. Osoba autoryzująca analizuje odpowiednie informacje dotyczące bezpieczeństwa i ochrony prywatności dostarczane przez zautomatyzowane narzędzie do zarządzania bezpieczeństwem/prywatnością i raportowania w celu określenia aktualnej pozycji systemu w zakresie bezpieczeństwa i ochrony prywatności.

Referencje: [OMB A-130]; [NSC 800-30]; [SP 800-39] (Organizacja, misja/proces biznesowy i poziomy systemu); [SP 800-137]; [SP 800-160 cz. 1] (Proces zarządzania ryzykiem); [IR 8062].

REAKCJA NA RYZYKO

ZADANIE R-3 Określenie i wdrożenie preferowanego sposobu postępowania w odpowiedzi na określone ryzyko.

Potencjalne dane wejściowe: Pakiet autoryzacyjny; określenie ryzyka; wyniki szacowania ryzyka na poziomie organizacji i systemu.

Oczekiwane wyniki: Reakcje na określone ryzyko.

Podstawowa odpowiedzialność: AO lub AODR.

Role wspierające: SAORM lub RE; SAISO; SAOP; SO lub CCP; IO/S; SSE; PE; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy – Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Po przeanalizowaniu i określeniu ryzyka, organizacje mogą reagować na ryzyko na różne sposoby, w tym poprzez akceptację ryzyka i jego ograniczanie. Istniejące wyniki szacowania ryzyka oraz techniki szacowania ryzyka mogą być wykorzystane w celu określenia preferowanego sposobu reagowania na ryzyko.[96] W przypadku, gdy reakcja na ryzyko polega na jego ograniczeniu, planowane działania ograniczające są włączane do planu działania i monitorowane przy użyciu planu i etapów działań. Po ograniczeniu ryzyka podmioty oceniające zabezpieczenia ponownie oceniają zabezpieczenia. Ponowna ocena zabezpieczeń określa zakres, w jakim skorygowane zabezpieczenia są prawidłowo wdrażane, funkcjonują zgodnie z założeniami i przynoszą pożądane rezultaty w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatności w odniesieniu do systemu i organizacji. Podmioty oceniające zabezpieczenia aktualizują sprawozdania z oceny o ustalenia z ponownej oceny, ale nie zmieniają pierwotnych wyników oceny. Plany bezpieczeństwa i ochrony prywatności są aktualizowane w oparciu o wyniki ocen zabezpieczeń i wszelkie podjęte działania naprawcze. Zaktualizowane plany odzwierciedlają stan zabezpieczeń po wstępnej ocenie

[96] [SP 800-39] zawiera dodatkowe informacje na temat reakcji na ryzyko.

oraz wszelkie zmiany wprowadzone przez właściciela systemu lub dostawcę zabezpieczeń wspólnych w odniesieniu do zaleceń dotyczących działań naprawczych.

Po zakończeniu ponownej oceny zabezpieczeń, plany bezpieczeństwa i ochrony prywatności zawierają dokładny opis wdrożonych zabezpieczeń, w tym zabezpieczeń kompensacyjnych. Gdy reakcją na ryzyko jest akceptacja, niedociągnięcia stwierdzone podczas procesu oceny pozostają udokumentowane w sprawozdaniach z oceny bezpieczeństwa i prywatności i są monitorowane pod kątem zmian czynników ryzyka. Ponieważ osoba autoryzująca jest jedynym podmiotem, który może zaakceptować ryzyko, jest ona odpowiedzialna za przegląd raportów podmiot oceniających i planów i etapów działania i ustalenie, czy zidentyfikowane ryzyko musi zostać złagodzone przed autoryzacją. Decyzje dotyczące najwłaściwszego sposobu reagowania na ryzyko mogą obejmować pewną formę ustalania priorytetów. Niektóre rodzaje ryzyka mogą być bardziej niepokojące dla organizacji niż inne rodzaje ryzyka. W takim przypadku konieczne może być przeznaczenie większej ilości zasobów na działania związane z ryzykiem o wyższym priorytecie w porównaniu z ryzykiem o niższym priorytecie. Ustalanie priorytetów reakcji na ryzyko nie oznacza, że ryzyka o niższym priorytecie są ignorowane. Oznacza to, że na rozwiązywanie problemów związanych z ryzykiem o niższym priorytecie przeznacza się mniej zasobów lub, że problemy związane z ryzykiem o niższym priorytecie są rozwiązywane później. Kluczową częścią procesu decyzyjnego opartego na ryzyku jest uznanie, że niezależnie od reakcji na ryzyko, pozostaje pewien stopień ryzyka rezydualnego. Organizacje określają dopuszczalne stopnie ryzyka szczątkowego w oparciu o tolerancję ryzyka organizacyjnego.

Referencje: [NSC 800-30]; [SP 800-39] (Organizacja, misja/proces biznesowy i poziomy systemu); [SP 800-160 cz. 1] (Proces zarządzania ryzykiem); [IR 8062]; [IR 8179]; [CSF NIST] (Podstawowa [funkcja identyfikacji]).

DECYZJA AUTORYZUJĄCA

ZADANIE R-4 Ustalenie, czy ryzyko wynikające z działania lub stosowania systemu informatycznego, albo zapewnienia lub stosowania zabezpieczeń wspólnych, jest dopuszczalne.

Potencjalne dane wejściowe: Reakcje na określone ryzyko.

Oczekiwane wyniki: Upoważnienie do działania, zezwolenie na użytkowanie, zabezpieczenia wspólne; odmowa upoważnienia do działania, odmowa zezwolenie na użytkowanie, odmowa używania zabezpieczenia wspólnego.

Podstawowa odpowiedzialność: AO.

Role wspierające: SAORM lub RE; CIO; SAISO; SAOP; AODR.

Faza rozwoju cyklu życia systemu: Nowy – Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Jednoznaczna akceptacja ryzyka należy do obowiązków osoby autoryzującej i nie może być delegowana na inny personel w organizacji. Osoba autoryzująca bierze pod uwagę wiele czynników przy podejmowaniu decyzji, czy ryzyko dla działalności organizacji (w tym misja, funkcje, wizerunek i reputacja) i jej aktywów, osób, innych organizacji lub Państwo jest dopuszczalne. Równowaga między względami bezpieczeństwa i prywatności, a misją i potrzebami biznesowymi ma zasadnicze znaczenie dla podjęcia decyzji o autoryzacji opartej na dopuszczalnym ryzyku. Osoba autoryzująca wydaje decyzję autoryzacyjną dla systemu lub dla wyznaczonych przez organizację zabezpieczeń wspólnych po zapoznaniu się z informacjami zawartymi w pakiecie autoryzacyjnym, wkładem innych komórek organizacyjnych (zob. Zadanie R-2) oraz innymi istotnymi informacjami, które mogą mieć wpływ na decyzję autoryzacyjną. Pakiet autoryzacyjny dostarcza najbardziej aktualnych informacji na temat bezpieczeństwa i ochrony prywatności systemu lub zabezpieczeń wspólnych.

Osoba autoryzująca konsultuje się z SAORM lub RM przed podjęciem ostatecznej decyzji w sprawie autoryzacji systemu informatycznego lub zabezpieczeń wspólnych. Ze względu na potencjalnie znaczące zależności pomiędzy systemami organizacyjnymi oraz z systemami zewnętrznymi, decyzje autoryzacyjne dla poszczególnych systemów uwzględniają bieżące ryzyko szczątkowe, plany i etapy działania organizacji oraz tolerancję organizacji na ryzyko.

Decyzja o autoryzacji jest przekazywana przez osobę autoryzującą właścicielowi systemu lub dostawcy zabezpieczeń wspólnych oraz odpowiednio innemu personelowi organizacyjnemu.[97] Decyzja autoryzacyjna zawiera również zasady i warunki udzielenia upoważnienia do działania; datę wygaśnięcia zezwolenia lub częstotliwość udzielania zezwoleń; informacje przekazywane przez wyższy rangą personel odpowiedzialny za zarządzanie ryzykiem lub wykonawcę (funkcję) ryzyka, o ile jest przewidziana; a w przypadku zabezpieczeń wspólnych - poziom wpływu systemu wspierany przez zabezpieczenia wspólne.

W przypadku systemów, decyzja o autoryzacji wskazuje właścicielowi systemu, czy jest on uprawniony do obsługi lub do użytkowania, czy też nie jest on uprawniony do obsługi lub do użytkowania. W przypadku zabezpieczeń wspólnych, decyzja o autoryzacji wskazuje dostawcy zabezpieczeń wspólnych oraz właścicielom systemów dziedziczących, czy system jest upoważniony, czy też nie jest upoważniony, do stosowania zabezpieczeń wspólnych. Zasady i warunki autoryzacji zabezpieczeń wspólnych zawierają opis wszelkich szczególnych ograniczeń lub restrykcji nałożonych na działanie systemu lub zabezpieczenia, które muszą być przestrzegane przez właściciela systemu lub dostawcę zabezpieczeń wspólnych.

Data wygaśnięcia autoryzacji jest ustalana przez osobę autoryzującą i wskazuje datę wygaśnięcia upoważnienia. Organizacje mogą nie podawać daty wygaśnięcia autoryzacji (zezwolenie stałe), o ile system działa na podstawie bieżącej autoryzacji, czyli program

[97] Zachęca się organizacje do stosowania w miarę możliwości zautomatyzowanych narzędzi do zarządzania bezpieczeństwem/prywatnością i raportowania, do opracowywania pakietów autoryzacyjnych dla systemów i wspólnych kontroli oraz do utrzymywania tych pakietów podczas bieżącej autoryzacji. Zautomatyzowane narzędzia mogą znacznie obniżyć koszty dokumentacji, zapewnić większą szybkość i skuteczność w generowaniu ważnych informacji dla decydentów, a także zapewnić bardziej efektywne środki aktualizacji krytycznych informacji dotyczących zarządzania ryzykiem. Uznaje się, że niektóre elementy sterowania nie sprzyjają stosowaniu narzędzi automatycznych i dlatego w takich sytuacjach dopuszczalne są metody ręczne.

ciągłego monitorowania jest wystarczająco solidny i dojrzały, aby dostarczyć osobie autoryzującej informacji niezbędnych do prowadzenia bieżących działań w zakresie określania ryzyka i akceptacji ryzyka w odniesieniu do bezpieczeństwa i prywatności systemu oraz bieżącej skuteczności zabezpieczeń stosowanych w ramach systemu i przez niego dziedziczonych.

Decyzja o autoryzacji jest dołączona do pakietu autoryzacyjnego i przekazywana do właściciela systemu lub dostawcy zabezpieczeń wspólnych. Po otrzymaniu decyzji o autoryzacji i pakietu autoryzacyjnego, właściciel systemu lub dostawca zabezpieczeń wspólnych potwierdza i wprowadza w życie warunki autoryzacji. Organizacja zapewnia, że pakiet autoryzacyjny, w tym decyzja o autoryzacji systemów i zabezpieczeń wspólnych, jest udostępniany personelowi organizacji (np. właścicielom systemów dziedziczących zabezpieczenia wspólne; CIO; SAORM lub RM; SAISO; SAOP; oraz SSPO). Osoba autoryzująca weryfikuje na bieżąco w ramach stałego monitorowania (zob. Zadanie M-2), czy właściciel systemu lub dostawca zabezpieczeń wspólnych przestrzega ustalonych warunków autoryzacji.

W przypadku, gdy system działa na podstawie stałego zezwolenia, osoba autoryzująca nadal ponosi odpowiedzialność za jednoznaczne zrozumienie i zaakceptowanie ryzyka związanego z dalszym funkcjonowaniem lub korzystaniem z systemu lub dalszym zapewnianiem zabezpieczeń wspólnych. W przypadku bieżącej autoryzacji, częstotliwość autoryzacji jest podawana zamiast daty zakończenia autoryzacji. Osoba autoryzująca dokonuje przeglądu informacji z określoną w czasie częstotliwością autoryzacji zdefiniowaną przez organizację, jako część strategii ciągłego monitorowania i określa, czy ryzyko kontynuowania działania systemu lub zapewnienia zabezpieczeń wspólnych pozostaje do przyjęcia. Jeśli ryzyko pozostaje do zaakceptowania, osoba autoryzująca potwierdza akceptację zgodnie z procesami organizacyjnymi. Jeśli ryzyko nie jest akceptowalne, osoba autoryzująca wskazuje, że ryzyko nie jest już akceptowalne i wymaga dalszej reakcji na ryzyko lub całkowitej odmowy autoryzacji.

Organizacja określa poziom formalności w procesie komunikowania i potwierdzania ciągłej akceptacji ryzyka przez osobę autoryzującą. Osoba autoryzująca może nadal ustanawiać i przekazywać szczegółowe warunki, które właściciel systemu lub dostawca zabezpieczeń wspólnych musi stosować w celu uzyskania dalszego upoważnienia do działania, dalszego upoważnienia do zabezpieczeń wspólnych lub dalszego zezwolenie na użytkowanie. Zasady i warunki autoryzacji mogą być przekazywane za pomocą narzędzia do automatycznego zarządzania i raportowania, jako część decyzji o autoryzacji automatycznej.

Jeżeli oceny zabezpieczeń są przeprowadzane przez wykwalifikowanych podmiot oceniających o wymaganym poziomie niezależności, wyniki oceny potwierdzają bieżącą autoryzację i mogą być zastosowane do ponownego upoważnienia. Polityka organizacyjna dotycząca bieżących upoważnień i autoryzacji jest zgodna z przepisami prawa, rozporządzeniami, dyrektywami, rozporządzeniami i politykami.

Załącznik F zawiera dodatkowe wskazówki dotyczące decyzji autoryzacyjnych, rodzajów autoryzacji oraz przygotowania pakietów autoryzacyjnych.

Referencje: [SP 800-39] (Organizacja, misja/proces biznesowy i poziomy systemu); [SP 800-160 cz. 1] (Proces zarządzania ryzykiem).

SPRAWOZDANIA Z AUTORYZACJI

ZADANIE R-5 Zgłoszenie decyzji o zezwoleniu oraz wszelkich niedoskonałościach zabezpieczeń, które stanowią znaczące zagrożenie dla bezpieczeństwa lub prywatności.

Potencjalne dane wejściowe: Decyzja o autoryzacji.

Oczekiwane wyniki: Raport wskazujący decyzję autoryzacyjną dla systemu lub zestawu zabezpieczeń wspólnych; adnotacja o statusie autoryzacji w rejestrze systemu organizacyjnego.

Podstawowa odpowiedzialność: AO lub AODR.

Role wspierające: SO lub CCP; IO/S; SSO; SPO; SAISO; SAOP.

Faza rozwoju cyklu życia systemu: Nowy – Wdrożenie/Ocena.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Osoby autoryzujące zgłaszają decyzje autoryzacyjne dotyczące systemów i zabezpieczeń wspólnych wyznaczonemu personelowi organizacyjnemu, tak, aby poszczególne decyzje dotyczące ryzyka mogły być postrzegane w kontekście zagrożenia bezpieczeństwa i ochrony prywatności w całej organizacji dla operacji i aktywów organizacji, osób, innych organizacji i Państwa. Zgłaszanie ma miejsce tylko w sytuacjach, w których organizacje przekazały funkcje autoryzacyjne poziomom organizacyjnym poniżej kierownika jednostki organizacyjnej. Osoby autoryzujące zgłaszają również możliwe do wykorzystania braki (tj. podatności) w systemie lub zabezpieczeniach, odnotowane podczas oceny i ciągłego monitorowania, które stanowią znaczące zagrożenie dla bezpieczeństwa lub prywatności. Organizacje określają, a ich polityka organizacyjna odzwierciedla, co stanowi istotne zagrożenie dla bezpieczeństwa lub prywatności w zakresie raportowania. Braki, które stanowią znaczące słabości i ryzyko, można zgłaszać za pomocą Podkategorii, Kategorii i Funkcji w [NIST CSF]. Decyzje o autoryzacji mogą być śledzone i odzwierciedlane w ramach procesu rejestracji w całym systemie według uznania organizacji (zob. Zadanie P-18).

Referencje: [SP 800-39] (Organizacja, misja/proces biznesowy oraz poziomy systemu); [SP 800-160 cz. 1] (Zarządzanie decyzjami oraz procesy oceny i kontroli projektu); [CSF NIST] (podstawowe funkcje [identyfikacja, ochrona, wykrywanie, reagowanie, funkcje odzyskiwania]).

3.7 MONITOROWANIE

CEL

Celem etapu ***Monitorowanie*** jest utrzymanie stałej świadomości sytuacyjnej w zakresie bezpieczeństwa i ochrony prywatności systemu informatycznego i organizacji w celu wsparcia decyzji dotyczących zarządzania ryzykiem.

MONITOROWANIE ZADAŃ

Tabela 8 zawiera podsumowanie zadań i oczekiwanych wyników dla etapu *Monitorowanie RMF.*

Przedstawiono również obowiązujące konstrukcje Ram Cyberbezpieczeństwa.

TABELA 8: MONITOROWANIE ZADAŃ I WYNIKÓW

Zadania	Wyniki
ZADANIE M-1 **ZMIANY SYSTEMOWE I ŚRODOWISKOWE**	• System informatyczny i środowisko pracy są monitorowane zgodnie ze strategią ciągłego monitorowania. [*Ramy Cyberbezpieczeństwa*: **DE.CM**; **ID.GV**]
ZADANIE M-2 **OCENY BIEŻĄCE**	• Bieżące oceny skuteczności zabezpieczeń prowadzone są zgodnie ze strategią ciągłego monitorowania. [*Ramy Cyberbezpieczeństwa:* **ID.SC-4**]

Zadania	Wyniki
ZADANIE M-3 **BIEŻĄCA REAKCJA NA RYZYKO**	• Wyniki działań z zakresu ciągłego monitorowania są analizowane i podejmowane są stosowne działania korygujące. [*Ramy Cyberbezpieczeństwa:* **RS.AN**]
ZADANIE M-4 **AKTUALIZACJE PAKIETÓW AUTORYZACYJNYCH**	• Dokumenty dotyczące zarządzania ryzykiem są aktualizowane w oparciu o ciągłe działania monitorujące. [*Ramy Cyberbezpieczeństwa:* **RS.IM**]
ZADANIE M-5 **SPRAWOZDAWCZOŚĆ W ZAKRESIE BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**	• Wprowadzenie procesu zgłaszania stanu bezpieczeństwa i prywatności osobie autoryzującej oraz wyższemu personelowi i kierownictwu.
ZADANIE M-6 **BIEŻĄCA AUTORYZACJA**	• Osoba autoryzująca na bieżąco dokonuje autoryzacji, wykorzystując wyniki ciągłych działań monitorujących oraz informuje o zmianach w określaniu ryzyka i decyzjach akceptacyjnych.
ZADANIE M-7 **UTYLIZACJA SYSTEMU**	• W razie potrzeby opracowywana i wdrażana jest strategia utylizacji (likwidacji) systemu.

ZMIANY SYSTEMOWE I ŚRODOWISKOWE

ZADANIE M-1 Monitorowanie systemu informatycznego i jego środowisko pracy pod kątem zmian, które mają wpływ na bezpieczeństwo i prywatność systemu.

Potencjalne dane wejściowe: Strategia organizacyjna stałego monitorowania; polityka i procedury zarządzania konfiguracją organizacyjną; polityka organizacyjna i procedury postępowania z nieautoryzowanymi zmianami w systemie; plany bezpieczeństwa i ochrony prywatności; wnioski/zatwierdzenia zmian w konfiguracji; dokumentacja projektowa systemu; raporty z oceny bezpieczeństwa i ochrony prywatności; plany i etapy; informacje uzyskiwane z narzędzi automatycznego i ręcznego monitorowania.

Oczekiwane wyniki: Zaktualizowane plany bezpieczeństwa i ochrony prywatności; zaktualizowane plany i etapy działań; zaktualizowane raporty z oceny bezpieczeństwa i ochrony prywatności.

Podstawowa odpowiedzialność: SO lub CCP; SAISO; SAOP.

Role wspierające: SAORM lub RE; AO lub AODR; IO/S; SSO; SPO.

Faza rozwoju cyklu życia systemu: Nowy – Eksploatacja/Utrzymanie.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Systemy i środowiska pracy znajdują się w ciągłym stanie zmian wraz ze zmianami technologii zachodzącymi w elementach lub maszynach, czynnikach ludzkich oraz fizycznych lub środowiskowych. Do zmian w elementach technologii lub maszyn zalicza się na przykład modernizację sprzętu, oprogramowania lub oprogramowania sprzętowego; do zmian w czynnikach ludzkich zalicza się na przykład rotację personelu lub zmniejszenie jego liczby; natomiast do zmian w otoczeniu elementów fizycznych i środowiskowych zalicza się na przykład zmiany lokalizacji obiektu lub fizycznej kontroli dostępu chroniącej obiekt. Zmiany wprowadzane przez dostawców zewnętrznych mogą być trudne do wykrycia. Zdyscyplinowane i ustrukturyzowane podejście do zarządzania, kontroli i dokumentowania zmian w systemach i środowiskach działania oraz przestrzeganie warunków autoryzacji jest

zasadniczym elementem programów bezpieczeństwa i ochrony prywatności. Organizacje ustanawiają procesy zarządzania konfiguracją i zabezpieczeniami w celu wsparcia zarządzania konfiguracją i zmianami.[98]

Wspólne działania w ramach organizacji mogą powodować zmiany w systemach lub środowisku pracy i mogą mieć znaczący wpływ na bezpieczeństwo i prywatność systemów. Przykładem może być instalacja lub utylizacja sprzętu, wprowadzanie zmian w konfiguracji oraz instalowanie łatek poza ustalonym procesem kontroli zmian konfiguracji. Nieautoryzowane zmiany mogą wystąpić z powodu celowych ataków ze strony przeciwników lub nieumyślnych błędów autoryzowanego personelu. Oprócz przestrzegania ustalonego procesu zarządzania konfiguracją, organizacje monitorują systemy pod kątem nieautoryzowanych zmian i analizują informacje o nieautoryzowanych zmianach, które wystąpiły, w celu ustalenia pierwotnej przyczyny nieautoryzowanej zmiany. Oprócz monitorowania nieautoryzowanych zmian, organizacje stale monitorują systemy i środowiska pracy pod kątem wszelkich autoryzowanych zmian, które mają wpływ na prywatność systemów.[99]

Po ustaleniu pierwotnej przyczyny nieautoryzowanej zmiany (lub autoryzowanej zmiany, która wpływa na prywatność systemu), powinna nastąpić stosowna reakcja organizacji (zob. Zadanie M-3). Na przykład, jeżeli główna przyczyna nieautoryzowanej zmiany zostanie uznana za atak przeciwnika, można podjąć wiele działań, takich jak wywołanie procesu reakcji na incydent, dostosowanie narzędzi do wykrywania i zapobiegania włamaniom oraz konfiguracji zapory sieciowej, lub wdrożenie dodatkowych lub silniejszych środków bezpieczeństwa w celu zmniejszenia ryzyka przyszłych ataków. W przypadku stwierdzenia, że przyczyną nieautoryzowanej zmiany jest nieprzestrzeganie przez personel ustalonych

[98] [SP 800-128] zawiera wytyczne dotyczące zarządzania konfiguracją zorientowaną na bezpieczeństwo (ang. Security-focused configuration management - seccm). Należy pamiętać, że proces seccm opisany w [SP 800-128] obejmuje powiązany z nim etap monitorowania.

[99] Informacje na temat rozróżnienia między autoryzowanym i nieautoryzowanym zachowaniem systemu można znaleźć w omówieniu bezpieczeństwa i prywatności w Sekcji 2.3.

procesów zarządzania konfiguracją, uzasadnione może być przeprowadzenie szkolenia naprawczego dla niektórych osób.

Referencje: [NSC 800-30]; [SP 800-128]; [SP 800-137]; [IR 8062].

OCENY BIEŻĄCE

Zadanie M-2 Ocena zabezpieczeń zaimplementowanych w ramach systemu i dziedziczonych przez system zgodnie ze strategią ciągłego monitorowania.

Potencjalne dane wejściowe: Strategia stałego monitorowania na poziomie organizacji i strategia stałego monitorowania systemu (jeśli dotyczy); plany bezpieczeństwa i ochrony prywatności; plany oceny bezpieczeństwa i ochrony prywatności; raporty z oceny bezpieczeństwa i ochrony prywatności; plany i etapy działania; informacje uzyskane z narzędzi monitorowania automatycznego i ręcznego; wyniki szacowania ryzyka na poziomie organizacji i systemu; wyniki oceny zewnętrznej lub audytu (jeśli dotyczy).

Oczekiwane wyniki: Uaktualnione raporty z oceny bezpieczeństwa i prywatności.

Podstawowa odpowiedzialność: CA.

Role wspierające: AO lub AODR; SO lub CCP; IO/S; SSO; SPO; SAISO; SAOP.

Faza rozwoju cyklu życia systemu: Nowy – Eksploatacja/Utrzymanie.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Po wprowadzeniu autoryzacji wstępnej systemu lub zabezpieczeń wspólnych, organizacja na bieżąco ocenia wszystkie zabezpieczenia. Bieżąca ocena skuteczności zabezpieczeń jest częścią ciągłego monitorowania działalności organizacji. Częstotliwość monitorowania każdego zabezpieczenia opiera się na strategii ciągłego monitorowania organizacji (zob. Zadanie P-7) i może być uzupełniona strategią ciągłego monitorowania na poziomie systemu (zob. Zadanie S-5). Monitorowane jest także przestrzeganie warunków określonych przez osobę autoryzującą w ramach decyzji upoważniającej (zob. Zadanie M-1). Bieżąca ocena zabezpieczeń jest kontynuowana, ponieważ informacje generowane

w ramach ciągłego monitorowania są korelowane, analizowane i raportowane do wyższych rangą liderów.

W przypadku oceny bieżącej zabezpieczeń, podmiot oceniający mają wymagany stopień niezależności, określony przez osobę autoryzującą. Niezależność podmiot oceniający podczas stałego monitorowania wprowadza efektywność do procesu i może pozwolić na ponowne wykorzystanie wyników oceny na poparcie stałego zezwolenia oraz gdy wymagana jest reautoryzacja.

Aby spełnić wymóg corocznej oceny bezpieczeństwa, organizacje mogą korzystać z wyników ocen zabezpieczeń, które miały miejsce podczas autoryzacji, bieżącej autoryzacji lub reautoryzacji; podczas ciągłego monitorowania; lub podczas testowania i oceny systemów w ramach SDLC lub audytu (pod warunkiem, że wyniki oceny są aktualne, istotne dla określenia skuteczności zabezpieczeń i uzyskane przez podmioty oceniające zabezpieczenia z wymaganym stopniem niezależności). Istniejące wyniki oceny są ponownie wykorzystywane zgodnie z polityką ponownego wykorzystywania ustaloną przez organizację i w razie potrzeby uzupełniane o dodatkowe oceny. Ponowne wykorzystanie wyników oceny jest pomocne w osiągnięciu efektywnego kosztowo programu bezpieczeństwa, który jest w stanie dostarczyć dowodów niezbędnych do określenia pozycji bezpieczeństwa systemów informatycznych i organizacji. Wreszcie, wykorzystanie automatyzacji do wspierania oceny zabezpieczeń ułatwia zwiększenie częstotliwości, ilości i zakresu ocen.

Referencje: [NSC 800-53A]; [SP 800-137]; [SP 800-160 cz. 1] (Procesy weryfikacji, walidacji, eksploatacji i obsługi technicznej); [IR 8011 v1].

BIEŻĄCA REAKCJA NA RYZYKO

Zadanie M-3 Reakcja na ryzyko na podstawie wyników trwających działań monitorujących, szacowania ryzyka i zaległych pozycji w planach i etapach działania.

Potencjalne dane wejściowe: Raporty z oceny bezpieczeństwa i ochrony prywatności; wyniki szacowania ryzyka na poziomie organizacji i systemu; plany bezpieczeństwa i ochrony prywatności; plany i etapy działań.

Oczekiwane wyniki: Działania ograniczające ryzyko lub decyzje dotyczące akceptacji ryzyka; zaktualizowane raporty z oceny bezpieczeństwa i prywatności.

Podstawowa odpowiedzialność: AO; SO; CCP.

Role wspierające: SAORM lub RE; SAOP; AODR; IO/S; SSO; SPO; SSE; PE; SA; PA.

Faza rozwoju cyklu życia systemu: Nowy – Eksploatacja/Utrzymanie.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Informacje dotyczące oceny opracowane przez osobę oceniającą podczas stałego monitorowania są przekazywane właścicielowi systemu i dostawcy zabezpieczeń wspólnych w zaktualizowanych sprawozdaniach z oceny lub za pośrednictwem sprawozdań ze zautomatyzowanego zarządzania bezpieczeństwem/prywatnością i narzędzi sprawozdawczych. Osoba autoryzująca określa właściwą reakcję w zakresie ryzyka na wyniki oceny lub zatwierdza odpowiedzi zaproponowane przez właściciela systemu i dostawcę zabezpieczeń wspólnych. Właściciel systemu i dostawca zabezpieczeń wspólnych wdrażają następnie odpowiednią reakcję na ryzyko. Po zaakceptowaniu reakcji na ryzyko, ustalenia pozostają udokumentowane w raportach z oceny bezpieczeństwa i prywatności oraz są monitorowane pod kątem zmian czynników ryzyka. Kiedy reakcja na ryzyko jest łagodzona, planowane działania łagodzące są włączane do planów działania i są śledzone przy użyciu planów i etapów działania. Na wniosek osoby autoryzującej, podmioty oceniające zabezpieczenia mogą przedstawić zalecenia dotyczące działań zaradczych. Zalecenia dotyczące działań naprawczych mogą być również przedstawione za pomocą zautomatyzowanego narzędzia zarządzania bezpieczeństwem/prywatnością i sprawozdawczości. Organizacyjne szacowanie ryzyka (Zadanie P-3) oraz wyniki szacowania ryzyka na poziomie systemu (Zadanie P-14) wskazują i informują o decyzjach dotyczących bieżącej reakcji na ryzyko. Mechanizmy bezpieczeństwa, które zostały zmodyfikowane,

udoskonalone lub dodane w ramach bieżącej reakcji na ryzyko, są ponownie oceniane przez podmioty oceniające zabezpieczenia w celu zapewnienia, że nowe, zmodyfikowane lub udoskonalone środki bezpieczeństwa zostały wdrożone prawidłowo, działają zgodnie z założeniami i przynoszą pożądane rezultaty w odniesieniu do spełniania wymogów bezpieczeństwa i ochrony prywatności systemu.

Referencje: [NSC 800-30]; [NSC 800-53]; [NSC 800-53A]; [SP 800-137]; [SP 800-160 cz. 1] (proces zarządzania ryzykiem); [IR 8011 v1]; [IR 8062]; [NIST CSF] (podstawowa [funkcja odpowiedzi]).

AKTUALIZACJE PAKIETÓW AUTORYZACYJNYCH

Zadanie M-4 Aktualizacja planów, sprawozdań z oceny oraz planów i etapów działań na podstawie wyników procesu ciągłego monitorowania.

Potencjalne dane wejściowe: Raporty z oceny bezpieczeństwa i ochrony prywatności; wyniki szacowania ryzyka na poziomie organizacji i systemu; plany bezpieczeństwa i ochrony prywatności; plany i etapy działań.

Oczekiwane wyniki: Zaktualizowane sprawozdania z oceny bezpieczeństwa i ochrony prywatności; [100] zaktualizowane plany i etapy działania; zaktualizowane wyniki szacowania ryzyka; zaktualizowane plany bezpieczeństwa i ochrony prywatności.

Podstawowa odpowiedzialność: SO; CCP.

Role wspierające: IO/S; SSO; SPO; SAOP; SAISO.

Faza rozwoju cyklu życia systemu: Nowy – Eksploatacja/Utrzymanie.

Istniejący - Eksploatacja/Utrzymanie.

[100] Jeżeli raporty porównawcze spełniają wymogi dotyczące tego, co ma być zawarte w sprawozdaniu z oceny (np. Sprawozdanie wygenerowane z narzędzi zarządzania bezpieczeństwem lub prywatnością i sprawozdawczością), wówczas raporty porównawcze mogą stanowić sprawozdanie z oceny.

Dyskusja: W celu zarządzania ryzykiem w czasie zbliżonym do rzeczywistego, organizacja na bieżąco aktualizuje plany bezpieczeństwa i ochrony prywatności, raporty z oceny bezpieczeństwa i ochrony prywatności oraz plany i etapy działań. Aktualizacje planów odzwierciedlają zmiany w zabezpieczeniach opartych na działaniach ograniczających ryzyko, prowadzonych przez właścicieli systemów lub dostawców zabezpieczeń wspólnych. Aktualizacje sprawozdań z oceny zabezpieczeń odzwierciedlają dodatkowe działania oceniające przeprowadzone w celu określenia skuteczności zabezpieczeń w oparciu o szczegółowe informacje dotyczące wdrażania zawarte w planach. Plany i etapy są aktualizowane w oparciu o postępy poczynione w odniesieniu do bieżących nierozstrzygniętych kwestii; dotyczą zagrożeń dla bezpieczeństwa i prywatności wykrytych w ramach monitorowania skuteczności zabezpieczeń; oraz opisują sposób, w jaki właściciel systemu lub dostawca usług wspólnych zamierza zająć się tymi zagrożeniami. Zaktualizowane informacje zwiększają świadomość bezpieczeństwa i ochrony prywatności systemu oraz zabezpieczeń wspólnych odziedziczonych przez system, wspierając w ten sposób zarządzanie ryzykiem w czasie zbliżonym do rzeczywistego oraz trwający proces autoryzacji.

Częstotliwość aktualizacji informacji dotyczących zarządzania ryzykiem zależy od decyzji właściciela systemu, dostawcy zabezpieczeń wspólnych i osób autoryzujących zgodnie z polityką organizacyjną oraz jest zgodna ze strategiami stałego monitorowania na poziomie organizacji i systemu. Aktualizacje informacji dotyczących bezpieczeństwa i ochrony prywatności systemu oraz zabezpieczeń wspólnych odziedziczonych przez system, są dokładne i terminowe, ponieważ dostarczone informacje wpływają na bieżące działania i decyzje personelu organizacji i innych wyższych rangą liderów w organizacji. Wykorzystanie zautomatyzowanych narzędzi pomocniczych oraz praktyki zarządzania bezpieczeństwem i ochroną prywatności w całej organizacji zapewniają, że osoby autoryzujące mają łatwy dostęp do aktualnej pozycji w zakresie bezpieczeństwa i ochrony prywatności systemu. Gotowy dostęp do aktualnej postawy w zakresie bezpieczeństwa i ochrony prywatności wspiera ciągły monitoring i bieżące autoryzację oraz promuje zarządzanie ryzykiem w czasie prawie rzeczywistym dla operacji i aktywów organizacji, osób, innych organizacji i narodu.

Organizacje zapewniają, że informacje dotyczące celów nadzoru, zarządzania i audytu nie są modyfikowane lub niszczone podczas aktualizacji planów bezpieczeństwa i ochrony prywatności, raportów podmiot oceniających oraz planów i etapów działań. Zapewnienie skutecznej metody śledzenia zmian w systemach poprzez procedury zarządzania konfiguracją jest niezbędne do osiągnięcia przejrzystości i identyfikowalności działań organizacji w zakresie bezpieczeństwa i ochrony prywatności; do uzyskania indywidualnej odpowiedzialności za wszelkie działania w zakresie bezpieczeństwa i prywatności; oraz do zrozumienia pojawiających się trendów w programach bezpieczeństwa i ochrony prywatności organizacji.

Referencje: [NSC 800-30]; [NSC 800-53A].

SPRAWOZDAWCZOŚĆ W ZAKRESIE BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Zadanie M-5 Informuje na bieżąco uprawniony personel i innych przedstawicieli organizacji o stanie bezpieczeństwa i prywatności systemu, zgodnie z organizacyjną strategią ciągłego monitorowania.

Potencjalne dane wejściowe: Raporty z oceny bezpieczeństwa i ochrony prywatności; plany i etapy działania; wyniki szacowania ryzyka na poziomie organizacji i systemu; strategia ciągłego monitorowania na poziomie organizacji i systemu; plany bezpieczeństwa i ochrony prywatności; Profili Ram Cyberbezpieczeństwa.

Oczekiwane wyniki: Raporty dotyczące bezpieczeństwa i prywatności.[101]

Podstawowa odpowiedzialność: SO; CCP; SAISO; SAOP.

Role wspierające: SSO; SPO.

[101] Jeżeli porównywalny raport spełnia wymogi tego, co ma być zawarte w raporcie dotyczącym bezpieczeństwa lub prywatności (np. Raport wygenerowany z narzędzia do zarządzania bezpieczeństwem lub prywatnością i raportowania), wówczas porównywalny raport stanowiłby raport dotyczący stanu ochrony.

Faza rozwoju cyklu życia systemu: Nowy – Eksploatacja/Utrzymanie.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: Wyniki działań monitorujących są dokumentowane i raportowane na bieżąco osobie autoryzującej i innym wybranym przedstawicielom organizacji, zgodnie z organizacyjną strategią ciągłego monitorowania. Inni przedstawiciele organizacji, którzy mogą otrzymywać raporty dotyczące bezpieczeństwa i prywatności, to na przykład CIO, SAISO, SAOP, SAORM lub RE, IO/S, role związane z reagowaniem na incydenty i planowaniem awaryjnym. Sprawozdawczość w zakresie bezpieczeństwa i ochrony prywatności może być uzależniona od zdarzeń, czasu lub zdarzeń i czasu.[102] Raporty dostarczają osobom autoryzującym i innym przedstawicielom organizacji informacji dotyczących bezpieczeństwa i ochrony prywatności w systemach, w tym skuteczności wdrożonych zabezpieczeń. Raporty dotyczące bezpieczeństwa i ochrony prywatności opisują bieżące działania monitorujące prowadzone przez właścicieli systemów lub dostawców zabezpieczeń wspólnych. Raporty zawierają również informacje o zagrożeniach dla bezpieczeństwa i prywatności w systemach i środowiskach działania, wykrytych podczas oceny zabezpieczeń, audytu i ciągłego monitorowania oraz o tym, jak właściciele systemów lub dostawcy zabezpieczeń wspólnych planują przeciwdziałać tym zagrożeniom.

Organizacje dysponują elastycznością w zakresie zakresu, dokładności, formalności, formy i formatu raportów dotyczących bezpieczeństwa i ochrony prywatności. Celem jest sprawna, bieżąca komunikacja z osobą autoryzującą i innymi przedstawicielami organizacji w zależności od potrzeb, przekazująca aktualną postawę w zakresie bezpieczeństwa i ochrony prywatności systemów i środowisk pracy oraz sposób, w jaki obecna postawa wpływa na osoby, misje organizacji i funkcje biznesowe. Raporty dotyczące bezpieczeństwa i ochrony prywatności podsumowują, co najmniej zmiany w planach bezpieczeństwa i ochrony prywatności, raporty z oceny bezpieczeństwa i ochrony prywatności oraz plany

[102] Dodatkowe informacje na temat czasowych i zdarzeniowych uprawnień i sprawozdawczości znajdują się w Załączniku F.

i etapy działań, które nastąpiły od czasu ostatniego raportu. Wykorzystanie przez organizację zautomatyzowanych narzędzi do zarządzania bezpieczeństwem i prywatnością oraz raportowania (np. tablicy ogłoszeń) ułatwia skuteczność i terminowość raportowania postawy bezpieczeństwa i prywatności.

Częstotliwość raportów dotyczących bezpieczeństwa i ochrony prywatności zależy od uznania organizacji i jest zgodna z przepisami i zasadami organizacyjnymi. Raporty pojawiają się w odpowiednich odstępach czasu w celu przekazania informacji na temat bezpieczeństwa i prywatności systemów lub zabezpieczeń wspólnych, ale nie tak często, aby generować niepotrzebną pracę lub wydatki. Osoby autoryzujące korzystają z raportów dotyczących bezpieczeństwa i ochrony prywatności i konsultują się z SAORM lub RE, SAISO i SAOP w celu ustalenia, czy konieczne jest podjęcie działań reautoryzujących.

Raporty dotyczące bezpieczeństwa i ochrony prywatności są oznaczane, chronione i traktowane zgodnie z przepisami i zasadami organizacyjnymi. Raporty dotyczące bezpieczeństwa i zachowania prywatności mogą być wykorzystywane w celu spełnienia wymagań w zakresie raportowania w celu udokumentowania działań naprawczych dotyczących słabości lub braków w zakresie bezpieczeństwa i ochrony prywatności. Raporty dotyczące bezpieczeństwa i ochrony prywatności mają być składane na bieżąco i nie powinny być interpretowane, jako wymagające czasu, wydatków i formalności związanych z informacjami dostarczonymi w celu uzyskania wstępnej autoryzacji. Sprawozdawczość jest prowadzona w sposób efektywny kosztowo, zgodny z osiągnięciem celów sprawozdawczości.

Referencje: [NSC 800-53A]; [SP 800-137]; [NIST CSF] (Funkcje podstawowe [identyfikacja, ochrona, wykrywanie, reagowanie, odzyskiwanie]).

BIEŻĄCA AUTORYZACJA

Zadanie M-6 Bieżący przegląd pozycji systemu w zakresie bezpieczeństwa i ochrony prywatności w celu ustalenia, czy ryzyko jest nadal dopuszczalne.

Potencjalne dane wejściowe: Tolerancja ryzyka; raporty dotyczące bezpieczeństwa i ochrony prywatności; plany i etapy działania; wyniki szacowania ryzyka na poziomie organizacji i systemu; plany dotyczące bezpieczeństwa i ochrony prywatności.

Oczekiwane wyniki: Określenie ryzyka; bieżące upoważnienie do działania, bieżące zezwolenie na użytkowanie, bieżące zezwolenie na zabezpieczenia wspólne; odmowa bieżącego upoważnienie do działania, odmowa bieżącego zezwolenia na użytkowanie, odmowa bieżącego zezwolenia na zabezpieczenia wspólne.

Podstawowa odpowiedzialność: AO.

Role wspierające: SAORM lub RE; CIO; SAISO; SAOP; AODR.

Faza rozwoju cyklu życia systemu: Nowy – Eksploatacja/Utrzymanie.

Istniejący - Eksploatacja/Utrzymanie.

Dyskusja: W celu zastosowania podejścia polegającego na stałej autoryzacji, organizacje wprowadzają proces stałego monitorowania na poziomie organizacji i systemu w celu stałej oceny wdrożonych zabezpieczeń.[103] Ustalenia lub wyniki procesu ciągłego monitorowania dostarczają użytecznych informacji dla osób autoryzujących do podejmowania decyzji w oparciu o ryzyko w czasie niemalże rzeczywistym. Zgodnie ze wskazówkami zawartymi w Zadaniu R-4, osoba autoryzująca lub pełnomocnik osoby autoryzującej na bieżąco dokonuje przeglądu pozycji w zakresie bezpieczeństwa i ochrony prywatności systemu (w tym skuteczności wdrożonych zabezpieczeń) w celu określenia bieżącego ryzyka dla działań i majątku organizacji, osób, innych organizacji i Państwa. Osoba autoryzująca określa, czy obecne ryzyko jest akceptowalne i przekazuje odpowiednie wskazówki właścicielowi systemu lub dostawcy zabezpieczeń wspólnych. Osoba autoryzująca może stwierdzić, że ryzyko pozostaje na poziomie akceptowalnym dla dalszej działalności lub że ryzyko nie jest już na poziomie akceptowalnym dla dalszej działalności i może wydać odmowę:

[103] Dodatkowe informacje na temat bieżących zezwoleń i stałego monitorowania znajdują się w Załączniku F.

upoważnienia do działania systemu, zezwolenia na użytkowanie lub zezwolenia na zabezpieczenia wspólne.

Ryzyko może ulec zmianie na podstawie informacji podanych w raportach dotyczących bezpieczeństwa i ochrony prywatności, ponieważ raporty mogą wskazywać na zmiany czynników ryzyka dla bezpieczeństwa lub prywatności. Ustalenie, w jaki sposób zmieniające się warunki wpływają na ryzyko organizacyjne i indywidualne, jest niezbędne do zarządzania ryzykiem związanym z prywatnością i utrzymania odpowiedniego poziomu bezpieczeństwa. Przeprowadzając bieżące określanie ryzyka i akceptację ryzyka, osoby autoryzujące mogą utrzymywać system i zabezpieczenia wspólne w czasie oraz przechodzić do bieżących autoryzacji. Działania związane z ponownym udzielaniem zezwoleń odbywają się wyłącznie zgodnie z przepisami lub zasadami organizacyjnymi. Osoba autoryzująca przekazuje zaktualizowane wyniki określania ryzyka i akceptacji ryzyka wyższemu rangą przedstawicielowi odpowiedzialnemu w organizacji za zarządzanie ryzykiem lub organowi zarządzającemu ryzykiem (funkcja).

Wykorzystanie zautomatyzowanych narzędzi pomocniczych do przechwytywania, organizowania, kwantyfikowania, wizualnego przedstawiania i utrzymywania bezpieczeństwa i ochrony prywatności informacji promuje zarządzanie ryzykiem w czasie niemal rzeczywistym w odniesieniu do postawy ryzyka w organizacji. Wykorzystanie metryk i pulpitów nawigacyjnych zwiększa zdolność organizacji do podejmowania decyzji opartych na ryzyku poprzez zautomatyzowaną konsolidację danych i dostarczanie danych decydentom na różnych szczeblach organizacji w łatwym do zrozumienia formacie.

Referencje: [NSC 800-30]; [SP 800-39] (Organizacja, misja/proces biznesowy i poziomy systemu); [SP 800-55]; [SP 800-160 cz. 1] (Proces zarządzania ryzykiem); [IR 8011 v1]; [IR 8062].

UTYLIZACJA SYSTEMU

Zadanie M-7 Wdrożenie strategii utylizacji systemu i przeprowadzenie wymaganych czynności w przypadku usunięcia systemu z eksploatacji.

Potencjalne dane wejściowe: Plany bezpieczeństwa i ochrony prywatności; wyniki szacowania ryzyka na poziomie organizacji i systemu; inwentaryzacja składników systemu.

Oczekiwane wyniki: Strategia utylizacji; zaktualizowana inwentaryzacja elementów systemu; zaktualizowane plany bezpieczeństwa i ochrony prywatności.

Podstawowa odpowiedzialność: SO.

Role wspierające: AO lub AODR; IO/S; SSO; SPO; SAORM lub RE; SAISO; SAOP.

Faza rozwoju cyklu życia systemu: Nowy – nie dotyczy.

Istniejący – Utylizacja (likwidacja).

Dyskusja: Po usunięciu systemu z eksploatacji konieczne jest podjęcie kilku działań z zakresu zarządzania ryzykiem. Organizacje zapewniają wdrożenie zabezpieczeń dotyczących utylizacji systemu. Przykładami mogą być: sanityzacja nośników, zarządzanie konfiguracją i zabezpieczeniami, autentyczność komponentów oraz przechowywanie dokumentacji. Systemy śledzenia i zarządzania organizacją (w tym systemy inwentaryzacji) są aktualizowane w celu wskazania systemu, który jest usuwany z eksploatacji. Raporty dotyczące bezpieczeństwa i ochrony prywatności odzwierciedlają stan bezpieczeństwa i prywatności systemu. Użytkownicy i właściciele aplikacji znajdujących się w usuwanym systemie są powiadamiani w odpowiedni sposób, a wszelkie dziedziczone zabezpieczenia są weryfikowane i oceniane pod kątem wpływu. Zadanie to dotyczy również elementów systemu, które są usuwane z użytkowania. Organizacje usuwające system z eksploatacji aktualizują spis systemów informatycznych w celu odzwierciedlenia tego usunięcia. Właściciele systemów i pracownicy ochrony zapewniają, że systemy są usuwane zgodne z odpowiednimi przepisami, regulacjami, dyrektywami, zasadami i normami.

Referencje: [NSC 800-30]; [SP 800-88]; [IR 8062].

ZAŁĄCZNIK A REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych – na podstawie FIPS 200
NSC 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych 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 800-53	Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informatycznego – na podstawie NIST SP 800-60

LAWS, POLICIES, DIRECTIVES, REGULATIONS, STANDARDS, AND GUIDELINES

LAWS AND EXECUTIVE ORDERS	
[32 CFR 2002.4]	Title 32 Code of Federal Regulations, Sec. 2002.4, *Definitions*. 2018 ed. https://www.govinfo.gov/app/details/CFR-2018-title32-vol6/CFR-2018-title32-vol6-sec2002-4
[40 USC 11331]	Title 40 U.S. Code, Sec. 11331, *Responsibilities for Federal information systems standards*. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331
[44 USC 3301]	Title 44 U.S. Code, Sec. 3301, *Definition of records*. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap33-sec3301
[44 USC 3502]	Title 44 U.S. Code, Sec. 3502, *Definitions*. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapI-sec3502
[44 USC 3552]	Title 44 U.S. Code, Sec. 3552, *Definitions*. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552
[44 USC 3554]	Title 44 U.S. Code, Sec. 3554, *Federal agency responsibilities*. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3554
[44 USC 3601]	Title 44 U.S. Code, Sec. 3601, *Definitions*. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap36-sec3601
[PRIVACT]	Privacy Act (P.L. 93-579), December 1974. https://www.govinfo.gov/app/details/STATUTE-88/STATUTE-88-Pg1896

[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.govinfo.gov/app/details/PLAW-104publ231
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283
[EO 13800]	Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017. https://www.govinfo.gov/app/details/FR-2017-05-16/2017-10004

POLICIES, REGULATIONS, DIRECTIVES, AND INSTRUCTIONS	
[OMB A-123]	Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf
[OMB A-130]	Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[OMB M-13-13]	Office of Management and Budget Memorandum M-13-13, *Open Data Policy-Managing Information as an Asset*, May 2013. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf
[OMB M-17-25]	Office of Management and Budget Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf
[OMB M-19-03]	Office of Management and Budget Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, December 2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf
[CNSSI 1253]	Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[CNSSI 4009]	Committee on National Security Systems Instruction 4009, *Committee on National Security Systems (CNSS) Glossary*, April 2015. https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[CNSSD 505]	Committee on National Security Systems Directive 505, *Supply Chain Risk Management*, August 2017. https://www.cnss.gov/CNSS/issuances/Directives.cfm
[OCIO HVA]	Office of the Federal Chief Information Officer, *The Agency HVA Process*. https://policy.cio.gov/hva/process
[DODI 5200.44]	Department of Defense Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks* (TSN), July 2017. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf

STANDARDS, GUIDELINES, AND REPORTS	
[IEEE 610.12]	Institute of Electrical and Electronics Engineers (IEEE) Std. 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology*, December 1990. https://ieeexplore.ieee.org/iel1/2238/4148/00159342.pdf
[ISO 15026-1]	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15026-1:2013, *Systems and software engineering—Systems and software assurance—Part 1: Concepts and vocabulary*, May 2015. https://www.iso.org/standard/62526.html
[ISO 15288]	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, *Systems and software engineering—Systems life cycle processes*, May 2015. https://www.iso.org/standard/63711.html
[ISO 15408-1]	International Organization for Standardization/International Electrotechnical Commission 15408-1:2009, *Information technology—Security techniques— Evaluation criteria for IT security—Part 1: Introduction and general model*. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
[ISO 15408-2]	International Organization for Standardization/International Electrotechnical Commission 15408-2:2008, *Information technology—Security techniques— Evaluation criteria for IT security—Part 2: Security functional requirements*. https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf
[ISO 15408-3]	International Organization for Standardization/International Electrotechnical Commission 15408-3:2008, *Information technology—Security techniques— Evaluation criteria for IT security—Part 3: Security assurance requirements*. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[ISO 27001]	International Organization for Standardization/International Electrotechnical Commission 27001:2013, *Information Technology—Security techniques—Information security management systems—Requirements*. https://www.iso.org/standard/54534.html
[ISO 29148]	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 29148:2011, *Systems and software engineering—Life cycle processes—Requirements engineering*, December 2011. https://www.iso.org/standard/45171.html
[FIPS 199]	National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. https://doi.org/10.6028/NIST.FIPS.199
[FIPS 200]	National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. https://doi.org/10.6028/NIST.FIPS.200
[SP 800-18]	National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006. https://doi.org/10.6028/NIST.SP.800-18r1
[SP 800-30]	National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012. https://doi.org/10.6028/NIST.SP.800-30r1
[SP 800-39]	National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-47]	National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002. https://doi.org/10.6028/NIST.SP.800-47
[SP 800-53]	National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013. https://doi.org/10.6028/NIST.SP.800-53r4
[SP 800-53A]	National Institute of Standards and Technology Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, July 2008. https://doi.org/10.6028/NIST.SP.800-53Ar4
[SP 800-55]	National Institute of Standards and Technology Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security*, December 2014. https://doi.org/10.6028/NIST.SP.800-55r1
[SP 800-59]	National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003. https://doi.org/10.6028/NIST.SP.800-59
[SP 800-60 v1]	National Institute of Standards and Technology Special Publication 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008. https://doi.org/10.6028/NIST.SP.800-60v1r1
[SP 800-60 v2]	National Institute of Standards and Technology Special Publication 800-60, Volume 2, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices*, August 2008. https://doi.org/10.6028/NIST.SP.800-60v2r1

[SP 800-61]	National Institute of Standards and Technology Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 2012. https://doi.org/10.6028/NIST.SP.800-61r2
[SP 800-64]	National Institute of Standards and Technology Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008. https://doi.org/10.6028/NIST.SP.800-64r2
[SP 800-82]	National Institute of Standards and Technology Special Publication 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015. https://doi.org/10.6028/NIST.SP.800-82r2
[SP 800-88]	National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*, December 2014. https://doi.org/10.6028/NIST.SP.800-88r1
[SP 800-128]	National Institute of Standards and Technology Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011. https://doi.org/10.6028/NIST.SP.800-128
[SP 800-137]	National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011. https://doi.org/10.6028/NIST.SP.800-137
[SP 800-160 v1]	National Institute of Standards and Technology Special Publication 800-160, Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, November 2016. https://doi.org/10.6028/NIST.SP.800-160v1
[SP 800-161]	National Institute of Standards and Technology Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015. https://doi.org/10.6028/NIST.SP.800-161

[SP 800-181]	National Institute of Standards and Technology Special Publication 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, August 2017. https://doi.org/10.6028/NIST.SP.800-181
[IR 8011 v1]	National Institute of Standards and Technology Interagency Report 8011, Volume 1, *Automation Support for Security Control Assessments: Overview*, June 2017. https://doi.org/10.6028/NIST.IR.8011-1
[IR 8062]	National Institute of Standards and Technology Internal Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017. https://doi.org/10.6028/NIST.IR.8062
[IR 8179]	National Institute of Standards and Technology Internal Report 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*, April 2018. https://doi.org/10.6028/NIST.IR.8179

MISCELLANEOUS PUBLICATIONS AND WEBSITES	
[DSB 2013]	Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, January 2013. https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf
[NARA CUI]	National Archives and Records Administration, *Controlled Unclassified Information (CUI) Registry*. https://www.archives.gov/cui
[NARA RECM]	National Archives and Records Administration, *NARA Records Management Guidance and Regulations*. https://www.archives.gov/records-mgmt/policy/guidance-regulations.html
[NIST CSF]	National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), Version 1.1, April 2018. https://www.nist.gov/cyberframework
[OMB FEA]	Office of Management and Budget, *Federal Enterprise Architecture (FEA)*. https://obamawhitehouse.archives.gov/omb/e-gov/fea

ZAŁĄCZNIK B SŁOWNIK

PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA

ZAŁĄCZNIK C AKRONIMY

PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA

ZAŁĄCZNIK D ROLE I OBOWIĄZKI

KLUCZOWI UCZESTNICY PROCESU ZARZĄDZANIA RYZYKIEM

W kolejnych rozdziałach opisano role i obowiązki kluczowych uczestników zaangażowanych w proces zarządzania ryzykiem w organizacji.[104] Uznając, że organizacje mają różne misje, funkcje biznesowe i struktury organizacyjne, mogą występować różnice w nazewnictwie ról związanych z zarządzaniem ryzykiem oraz w podziale odpowiedzialności za zarządzanie ryzykiem pomiędzy pracowników organizacji (np. wiele osób pełniących jedną rolę lub jedna osoba pełniąca wiele ról).[105] Podstawowe funkcje pozostają jednak takie same. Zastosowanie Ram Zarządzania Ryzykiem (RMF) opisanych w niniejszej publikacji jest elastyczne, co pozwala organizacjom na skuteczne realizowanie zamierzonych konkretnych zadań w ramach ich struktur organizacyjnych w celu jak najlepszego zarządzania ryzykiem w zakresie bezpieczeństwa i ochrony prywatności. Wiele ról w zarządzaniu ryzykiem zdefiniowanych w niniejszej publikacji ma swoje odpowiedniki w procesach SDLC prowadzonych przez organizacje. Organizacje dostosowują swoje role w zakresie zarządzania ryzykiem do podobnych (lub uzupełniających) ról zdefiniowanych w SDLC, gdy tylko jest to możliwe.[106]

AUTHORIZING OFFICIAL - AO

AO to osoba lub komórka organizacyjna dokonująca autoryzacji (dalej: *osoba autoryzująca*) polegającej na dopuszczeniu systemu informatycznego do eksploatacji w jednostce organizacyjnej, w tym za dopuszczenie do stosowania zabezpieczeń wspólnych dla wielu systemów. Posiada uprawnienia do formalnego przejęcia odpowiedzialności za obsługę systemu, zapewnienia zabezpieczeń wspólnych dziedziczonych przez systemy organizacyjne

[104] Organizacje mogą określić inne role wspierające proces zarządzania ryzykiem.
[105] Organizacje zapewniają, że nie występuje konflikt interesów przy przydzielaniu tej samej osoby do wielu ról w zarządzaniu ryzykiem. Zob. Krok RMF Przygotowywanie zadań - poziom organizacyjny, Zadanie P-1.
[106] Na przykład, rola SDLC dewelopera systemu lub menedżera programu może być dostosowana do roli właściciela systemu; a rola misji lub właściciela firmy może być dostosowana do roli osoby autoryzującej. [SP 800-64] zawiera wytyczne dotyczące bezpieczeństwa informacji w SDLC.

lub korzystania z systemu, usługi lub aplikacji zewnętrznego dostawcy. Osoba autoryzująca jest jedynym podmiotem organizacyjnym, który może zaakceptować ryzyko związane z bezpieczeństwem i prywatnością operacji organizacyjnych, aktywów organizacyjnych i osób fizycznych. [107] Osoba autoryzująca zazwyczaj posiada nadzór budżetowy nad systemem lub jest odpowiedzialna za misję i/lub operacje biznesowe wspierane przez system. W związku z tym osoby pełniące funkcje osoby autoryzującej zajmują stanowiska kierownicze o poziomie uprawnień współmiernym do zrozumienia i zaakceptowania takiego ryzyka dla bezpieczeństwa i prywatności. Osoba autoryzująca zatwierdza plany, protokoły uzgodnień lub porozumienia, plany i etapy działań oraz określa, czy istotne zmiany w systemach informatycznych lub środowiskach działania wymagają reautoryzacji.

Osoba autoryzująca koordynuje swoje działania z dostawcami zabezpieczeń wspólnych, właścicielami systemów, CIO, SAISO, SAOP, SSPO, CA, SAORM/RE oraz innymi zainteresowanymi stronami podczas procesu autoryzacji. Wraz z rosnącą złożonością procesów misyjnych/biznesowych w organizacji, ustaleniami partnerskimi i korzystaniem z usług wspólnych, możliwe jest, że system może wymagać zaangażowania kilku osób autoryzujących. Jeżeli zachodzi taka konieczność, między współpracującymi osobami autoryzującymi zawierane są umowy, które są udokumentowane w planach bezpieczeństwa i ochrony prywatności. Osoby autoryzujące są odpowiedzialne i rozliczane za działania i funkcje związane z autoryzacją, które są delegowane do AODR i są wykonywane w ustalony sposób.

AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE - AODR

AODR to reprezentant osoby lub komórki organizacyjnej dokonującej autoryzacji (dalej: *pełnomocnik osoby autoryzującej*), który jest uprawniony do działania w imieniu osoby autoryzującej (AO) w celu koordynowania i prowadzenia bieżącej działalności związanej

[107] Odpowiedzialność i rozliczalność osób autoryzujących opisana w [NSC 200] została rozszerzona w [NSC 800-53] o ryzyko dla innych organizacji i Państwa.

z zarządzaniem ryzykiem w odniesieniu do systemów informatycznych i organizacji. Obejmuje to wykonywanie szeregu czynności związanych z realizacją RMF. Jedyną czynnością, która nie może być zlecona AODR przez osobę autoryzującą, jest podjęcie decyzji autoryzującej i podpisanie związanego z nią dokumentu autoryzacji (tj. akceptacji ryzyka).

CHIEF ACQUISITION OFFICER - CAO

CAO to osoba odpowiedzialna za zakupy w jednostce organizacyjnej, wyznaczona przez kierownika jednostki organizacyjnej do udzielania mu oraz innemu personelowi organizacji porad i pomocy w celu zapewnienia realizacji misji organizacji poprzez zarządzanie działaniami związanymi z zakupami. CAO monitoruje realizację działań i programów związanych z nabyciem; ustala czytelne granice kompetencji, rozliczalności i odpowiedzialności za podejmowanie decyzji dotyczących nabycia w ramach organizacji; zarządza kierunkiem i wdrażaniem polityki zakupów organizacji; oraz ustanawia politykę, procedury i praktyki promujące pełną i otwartą konkurencję ze strony stosownych źródeł w celu spełnienia wymagań dotyczących najlepszej oferty, biorąc pod uwagę charakter nabywanych towarów lub usług. CAO koordynuje działania z właścicielami misji lub firm, osobami autoryzującymi, SAO, właścicielami systemów, dostawcami zabezpieczeń wspólnych, SAISO, SAOP oraz RE, w celu zapewnienia, że wymagania dotyczące bezpieczeństwa i prywatności są określone w zamówieniach organizacyjnych i nabywanych towarach i usługach.

CHIEF INFORMATION OFFICER - CIO [108]

CIO to kluczowa osoba w jednostce organizacyjnej odpowiedzialna za technologie informacyjne systemu (z wyłączeniem informacji niejawnych w rozumieniu ustawy o ochronie informacji niejawnych), zwykle członek kierownictwa jednostki organizacyjnej. Jest odpowiedzialna za wyznaczenie *SAISO*; opracowywanie i utrzymywanie polityki, procedur

[108] Jeżeli organizacja nie wyznaczyła formalnego stanowiska CIO, wymagane jest, aby związane z tym obowiązki były wykonywane przez równorzędną osobę w organizacji.

i technik zabezpieczających w celu spełnienia wymagań bezpieczeństwa; nadzorowanie personelu o znaczącej odpowiedzialności za bezpieczeństwo i zapewnienie, że personel jest odpowiednio przeszkolony; pomoc wyższemu personelowi organizacyjnemu w zakresie ich obowiązków związanych z bezpieczeństwem; oraz składanie sprawozdań kierownikowi jednostki organizacyjnej na temat skuteczności programu bezpieczeństwa organizacji, w tym postępów w działaniach naprawczych. CIO, przy wsparciu SAORM, RE, oraz SAISO, ściśle współpracuje z osobami autoryzującymi i AODR, w zapewnieniu, że:

- Skutecznie wdrażany jest w całej organizacji program bezpieczeństwa, którego efektem jest odpowiednie zabezpieczenie wszystkich systemów organizacyjnych i środowisk pracy;
- Kwestie bezpieczeństwa i ochrony prywatności (w tym łańcucha dostaw) związane z zarządzaniem ryzykiem są zintegrowane z cyklami programowania / planowania / budżetowania, architekturą korporacyjną, SDLC i zakupami;
- Systemy organizacyjne i zabezpieczenia wspólne objęte są zatwierdzonymi planami bezpieczeństwa systemu i posiadają aktualne autoryzacje;
- Działania w zakresie bezpieczeństwa wymagane w całej organizacji są realizowane w sposób wydajny, oszczędny i terminowy; oraz
- Istnieje scentralizowane raportowanie działań z zakresu bezpieczeństwa.

CIO i osoba autoryzująca określają przydział środków na ochronę systemów wspierających misję i funkcje biznesowe organizacji w oparciu o priorytety organizacyjne. W przypadku systemów informatycznych, które przetwarzają dane osobowe, CIO i osoba autoryzująca koordynują wszelkie ustalenia dotyczące przydziału zasobów przeznaczonych na ochronę tych systemów z SAOP. W przypadku wybranych systemów, CIO wspólnie z innym personelem wyższego szczebla organizacji może pełnić funkcję osoby autoryzującej lub reautoryzującej.

DOSTAWCA ZABEZPIECZEŃ WSPÓLNYCH - CCP

Dostawca zabezpieczeń wspólnych (*ang. common control provider - CCP)* jest osobą, grupą lub organizacją, która jest odpowiedzialna za wdrożenie, ocenę i monitorowanie zabezpieczeń wspólnych (tj. zabezpieczeń dziedziczonych przez systemy organizacyjne) [109]. Dostawca zabezpieczeń wspólnych jest również odpowiedzialny za zapewnienie dokumentacji zabezpieczeń określonych przez organizację w planach bezpieczeństwa i ochrony prywatności (lub równoważnych dokumentach zalecanych przez organizację); zapewnienie, że wymagane oceny zabezpieczeń wspólnych są przeprowadzane przez wykwalifikowany personel podmiot oceniający o odpowiednim poziomie niezależności; dokumentowanie wyników oceny w sprawozdaniach z oceny zabezpieczeń; oraz sporządzanie planów i etapów działania zabezpieczeń, w których występują niedociągnięcia. Plany bezpieczeństwa i ochrony prywatności, sprawozdania z oceny bezpieczeństwa i ochrony prywatności oraz plany i etapy działania zabezpieczeń wspólnych (lub podsumowanie takich informacji) są udostępniane właścicielom systemów, którzy odziedziczyli zabezpieczenia wspólne, po dokonaniu przeglądu i zatwierdzeniu informacji przez osobę autoryzującą odpowiedzialną za te zabezpieczenia wspólne.

SAOP jest odpowiedzialny za wskazywanie, które zabezpieczenia prywatności mogą być traktowane, jako zabezpieczenia wspólne.[110] Zabezpieczenia prywatności, które są wyznaczone, jako zabezpieczenia wspólne, są udokumentowane w planie programu ochrony prywatności organizacji. SAOP jest odpowiedzialny za nadzór nad zabezpieczeniami wspólnymi, które zostały wprowadzone lub są planowane w celu spełnienia obowiązujących

[109] Organizacje mogą mieć wielu dostawców zabezpieczeń wspólnych, w zależności od tego, w jaki sposób odpowiedzialność za bezpieczeństwo i prywatność jest przypisana całej organizacji. Dostawcami zabezpieczeń wspólnych mogą być właściciele systemów, gdy zabezpieczenia wspólne są rezydentami w ramach systemu organizacyjnego.

[110] Plan programu ochrony prywatności jest formalnym dokumentem zawierającym przegląd programu ochrony prywatności organizacji, w tym opis struktury programu ochrony prywatności; rolę SAOP oraz innych osób zajmujących się ochroną prywatności; strategiczne cele i zadania programu ochrony prywatności; zasoby przeznaczone na program ochrony prywatności; oraz program zarządzania zabezpieczeniami i zabezpieczeniami wspólnymi, istniejący lub planowany w celu spełnienia obowiązujących wymagań dotyczących ochrony prywatności i zarządzania zagrożeniami prywatności.

wymogów dotyczących ochrony prywatności i zarządzania ryzykiem związanym z ochroną prywatności oraz za ocenę tych zabezpieczeń. Według uznania organizacji, zabezpieczenia w zakresie ochrony prywatności, które są wyznaczone, jako zabezpieczenia wspólne, mogą być oceniane przez niezależnego podmiot oceniający. We wszystkich jednak przypadkach, SAOP zachowuje odpowiedzialność za program ochrony prywatności organizacji, w tym za wszelkie funkcje związane z ochroną prywatności wykonywane przez niezależne podmioty oceniające zabezpieczenia. Plany ochrony prywatności i raporty z oceny zabezpieczeń prywatności są udostępniane właścicielom systemów, których systemy dziedziczą zabezpieczenia prywatności wyznaczone, jako zabezpieczenia wspólne.

PODMIOT OCENIAJĄCY ZABEZPIECZENIA - CA

Podmiot oceniający zabezpieczenia (*ang. control assessor - CA)* to osoba, grupa lub organizacja odpowiedzialna za przeprowadzanie kompleksowej oceny wdrożonych zabezpieczeń podstawowych i zabezpieczeń rozszerzonych w celu określenia ich skuteczności (tj. zakresu, w jakim zabezpieczenia są wdrażane prawidłowo, działają zgodnie z założeniami i przynoszą pożądany rezultat w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatności systemu i organizacji). W przypadku systemów ocenia się wdrożone zabezpieczenia specyficzne dla danego systemu oraz wdrożone zabezpieczenia hybrydowe. W przypadku zabezpieczeń wspólnych ocenia się wdrożone zabezpieczenia wspólne i wdrożone wspólne zabezpieczenia hybrydowe. Właściciel systemu i dostawca zabezpieczeń wspólnych opierają się na wiedzy specjalistycznej w zakresie bezpieczeństwa i ochrony prywatności oraz na osądzie podmiotu oceniającego zabezpieczenia, oceniając wdrożone mechanizmy bezpieczeństwa z wykorzystaniem procedur oceny określonych w planach oceny bezpieczeństwa i ochrony prywatności. Do skutecznego przeprowadzenia oceny może być potrzebnych wiele podmiotów oceniających zabezpieczenia, które są zróżnicowane ze względu na swoją wiedzę specjalistyczną w zakresie konkretnych wymogów dotyczących zabezpieczeń lub technologii. Przed rozpoczęciem oceny zabezpieczeń podmioty oceniające zabezpieczenia dokonują przeglądu planów bezpieczeństwa i ochrony

prywatności, aby ułatwić opracowanie planów oceny. Podmioty oceniające zabezpieczenia przedstawiają ocenę wagi niedociągnięć wykrytych w systemie, środowisku działania i wspólnych mechanizmach bezpieczeństwa oraz mogą zalecić działania naprawcze mające na celu usunięcie zidentyfikowanych podatności. W przypadku oceny zabezpieczeń na poziomie systemu, podmioty oceniające zabezpieczenia nie oceniają zabezpieczeń dziedziczonych, a jedynie te części zabezpieczeń hybrydowych, które zostały wdrożone w systemie. Podmioty oceniające zabezpieczenia przygotowują sprawozdania z oceny bezpieczeństwa i ochrony prywatności zawierające wyniki i ustalenia z oceny.

Wymagany poziom niezależności podmiotu oceniającego jest określany przez osobę autoryzującą na podstawie ustaw, rozporządzeń, dyrektyw, regulacji, polityki, standardów lub wytycznych. Jeżeli ocena zabezpieczeń jest przeprowadzana na poparcie decyzji autoryzującej lub trwającej autoryzacji, osoba autoryzująca jednoznacznie określa wymagany stopień niezależności. Niezależność podmiot oceniający jest czynnikiem zachowania bezstronnego i wiarygodnego procesu oceny, określenia wiarygodności wyników oceny oraz zapewnienia, że osoba autoryzująca otrzymuje obiektywne informacje w celu podjęcia świadomej, opartej na ocenie ryzyka decyzji autoryzacyjnej.

SAOP jest odpowiedzialny za ocenę zabezpieczeń prywatności oraz za dostarczenie informacji o prywatności osobie autoryzującej. Według uznania organizacji, zabezpieczenia prywatności mogą być oceniane przez niezależny podmiot oceniający. Jednakże, we wszystkich przypadkach SAOP zachowuje odpowiedzialność za program ochrony prywatności organizacji, w tym za wszelkie funkcje związane z ochroną prywatności wykonywane przez niezależne podmioty oceniające.

ARCHITEKT KORPORACYJNY - EA

Architekt korporacyjny (*ang. enterprise architect - EA)* jest osobą lub grupą odpowiedzialną za współpracę z kierownictwem i ekspertami merytorycznymi w organizacji w celu zbudowania całościowego spojrzenia na misje i funkcje biznesowe organizacji, procesy

misyjne/biznesowe, informacje i zasoby informatyczne. W odniesieniu do bezpieczeństwa informacji i ochrony prywatności, architekci korporacyjni:

- Wdrażają strategię architektury korporacyjnej ułatwiającej efektywne rozwiązania w zakresie bezpieczeństwa i ochrony prywatności;
- Współpracują z architektami bezpieczeństwa informacji i architektami ochrony prywatności i ochrony danych osobowych w celu określenia optymalnego umiejscowienia systemów/elementów systemu w architekturze korporacyjnej oraz zajęcia się kwestiami bezpieczeństwa i ochrony prywatności pomiędzy systemami, a architekturą korporacyjną;
- Pomagają w zmniejszaniu złożoności infrastruktury informatycznej w celu zwiększenia bezpieczeństwa;
- Pomagają w określeniu odpowiednich implementacji zabezpieczeń i zabezpieczeń bazowych, ponieważ odnoszą się one do architektury korporacyjnej;
- Współpracują z właścicielami systemów i osobami autoryzującymi w celu ułatwienia wyznaczania granic autoryzacji i przypisania zabezpieczeń do elementów systemu;
- Funkcjonują w ramach funkcji RE; oraz
- Pomagają w integracji strategii zarządzania ryzykiem organizacyjnym oraz wymogów bezpieczeństwa i ochrony prywatności na poziomie systemu z działaniami programowymi, planistycznymi i budżetowymi, SDLC, procesami nabycia, zarządzaniem ryzykiem bezpieczeństwa i prywatności (w tym łańcuchem dostaw) oraz procesami inżynierii systemów.

KIEROWNIK JEDNOSTKI ORGANIZACYJNEJ - HA

Kierownik jednostki organizacyjnej (*ang. head of agency - HA)* jest odpowiedzialny za zapewnienie ochrony bezpieczeństwa informacji współmiernej do ryzyka związanego z działalnością i aktywami organizacji, osób fizycznych, innych organizacji i Państwa - czyli ryzyka wynikającego z nieautoryzowanego dostępu, wykorzystania, ujawnienia, zakłócenia,

modyfikacji lub zniszczenia informacji zebranych lub utrzymywanych przez organizację lub w jej imieniu; oraz systemów informatycznych wykorzystywanych lub obsługiwanych przez organizację lub kontrahenta organizacji lub inną współpracującą organizację. Kierownik jednostki organizacyjnej jest również osobą odpowiedzialną w organizacji za zapewnienie ochrony interesów prywatności i odpowiedzialnego zarządzania informacjami o charakterze osobistym w ramach organizacji. Kierownik jednostki organizacyjnej dba o to, żeby:

- Procesy zarządzania bezpieczeństwem informacji i ochroną prywatności były zintegrowane z procesami planowania strategicznego i operacyjnego;
- Personel kierowniczy w organizacji zapewniał bezpieczeństwo informacji i systemów wspierających operacje i aktywa będące pod ich kontrolą;
- Wyznaczani byli SAOP odpowiedzialni za zapewnienie zgodności z obowiązującymi wymogami w zakresie ochrony prywatności, zarządzanie ryzykiem związanym z ochroną prywatności oraz program ochrony prywatności organizacji; oraz
- Organizacja dysponowała odpowiednio przeszkolonym personelem, który wspomaga w przestrzeganiu wymogów bezpieczeństwa i ochrony prywatności zawartych w ustawodawstwie, rozporządzeniach wykonawczych, politykach, dyrektywach, instrukcjach, normach i wytycznych.

Kierownik jednostki organizacyjnej określa zaangażowanie organizacyjne i działania niezbędne do skutecznego zarządzania ryzykiem bezpieczeństwa i prywatności oraz ochrony misji i funkcji biznesowych realizowanych przez organizację. Kierownik jednostki organizacyjnej ustanawia odpowiedzialność za bezpieczeństwo i prywatność oraz zapewnia aktywne wsparcie i nadzór nad monitorowaniem i doskonaleniem programów bezpieczeństwa i ochrony prywatności. Zaangażowanie kierownictwa wyższego szczebla w sprawy bezpieczeństwa i prywatności ustanawia poziom należytej staranności w organizacji, który promuje sukces dla misji i procesu biznesowego.

WŁAŚCICIEL INFORMACJI / WŁADAJĄCY INFORMACJĄ – IO/S)

IO/S (*ang. Information Owner* or *Steward – IO/S)* jest osobą w organizacji posiadającą uprawnienia ustawowe, zarządcze lub operacyjne w zakresie określonych informacji oraz jest odpowiedzialny za ustanowienie polityki i procedur regulujących ich wytwarzanie, gromadzenie, przetwarzanie, rozpowszechnianie i usuwanie. W środowiskach wymiany informacji, właściciel / władający informacją jest odpowiedzialny za ustanowienie zasad właściwego wykorzystania i ochrony informacji oraz zachowuje tę odpowiedzialność nawet wtedy, gdy informacje są udostępniane lub dostarczane innym organizacjom. Właściciel / władający informacją przetwarzaną, przechowywaną lub przesyłaną przez system może, ale nie musi, być tą samą osobą, co właściciel systemu. Indywidualny system może zawierać informacje pochodzące od wielu właścicieli / władających informacją. Właściciele/władający informacją dostarczają właścicielom systemów danych wejściowych dotyczących wymogów bezpieczeństwa i ochrony prywatności oraz zabezpieczeń systemów, w których informacje są przetwarzane, przechowywane lub przesyłane.

WŁAŚCICIEL MISJI LUB PROCESU BIZNESOWEGO – BO

Właściciel misji lub procesu biznesowego (*ang. mission* or *business owner - BO)* w organizacji jest kierownikiem wyższego szczebla lub kierownikiem wykonawczym o określonej misji lub kierunku biznesowym, który ma obowiązek zapewnienia bezpieczeństwa lub ochrony prywatności w systemach organizacyjnych wspierających te misje lub obszary działalności. Właściciele misji lub obszarów biznesowych są kluczowymi interesariuszami, którzy odgrywają istotną rolę w ustalaniu misji organizacji i procesów biznesowych oraz potrzeb w zakresie ochrony i wymagań dotyczących bezpieczeństwa i ochrony prywatności, które zapewniają skuteczne wykonywanie misji i prowadzenie działalności biznesowej organizacji. Właściciele misji i procesu biznesowego wnoszą istotny wkład w strategię zarządzania ryzykiem, odgrywają aktywną rolę w SDLC, a także mogą pełnić rolę osoby autoryzującej.

RISK EXECUTIVE (FUNCTION) - RE

Funkcja wykonawcza ds. ryzyka (RE) to osoba (lub grupa osób, kierowana przez wyższego rangą kierownika w jednostce organizacyjnej) odpowiedzialna za zarządzanie ryzykiem. Zapewnia kompleksowe, w całej organizacji, podejście do zarządzania ryzykiem. Służy, jako wspólne źródło zarządzania ryzykiem dla kierowników wyższego szczebla, kadry kierowniczej i menedżerów, właścicieli misji/procesów biznesowych, CIO, SAISO, SAOP, właścicieli systemów, dostawców zabezpieczeń wspólnych, architektów przedsiębiorstw, architektów bezpieczeństwa informacji, inżynierów bezpieczeństwa systemów lub ochrony prywatności i ochrony danych osobowych, SSO lub SPO oraz wszelkich innych interesariuszy zainteresowanych misją/powodzeniem biznesowym organizacji.

RE zapewnia, że względy ryzyka dla systemów (w tym decyzje autoryzacyjne dla tych systemów oraz zabezpieczenia wspólne dziedziczone przez te systemy), są postrzegane z perspektywy całej organizacji w odniesieniu do strategicznych celów i zadań organizacji w zakresie realizacji jej głównych misji i funkcji biznesowych. RE zapewnia, że zarządzanie ryzykiem jest spójne w całej organizacji, odzwierciedla tolerancję na ryzyko organizacyjne i jest rozpatrywane łącznie z innymi rodzajami ryzyka w celu zapewnienia sukcesu misji/biznesu. RE koordynuje swoje działania z personelem wyższego szczebla i kierownictwem wykonawczym, poprzez:

- Ustalenie ról i obowiązków w zakresie zarządzania ryzykiem;
- Opracowanie i wdrożenie *strategii zarządzania ryzykiem w* skali całej organizacji, która zapewnia strategiczną wizję zagrożeń dla bezpieczeństwa organizacji [111] oraz wprowadza

[111] Osoby autoryzujące mogą mieć wąską lub ograniczoną perspektywę w podejmowaniu decyzji autoryzacyjnych bez pełnego zrozumienia lub wyraźnej akceptacji ryzyka ponoszonego w całej organizacji w związku z takimi decyzjami.

i informuje o decyzjach dotyczących ryzyka organizacyjnego (w tym o tym, w jaki sposób ryzyko jest określane, oceniane, obsługiwane i monitorowane w czasie);

- Zapewnienie kompleksowego, obejmującego całą organizację, holistycznego podejścia do podejmowania ryzyka - podejścia, które zapewnia lepsze zrozumienie zintegrowanych działań organizacji;
- Zarządzanie informacjami dotyczącymi zagrożeń, podatności na zagrożenia oraz bezpieczeństwa i ochrony prywatności (w tym ryzyka związanego z łańcuchem dostaw) dla systemów organizacyjnych i środowisk, w których systemy te działają;
- Ustanowienie forum obejmującego całą organizację, na którym rozpatrywane będą wszystkie rodzaje i źródła ryzyka (w tym ryzyko łączne);
- Określanie postaci ryzyka organizacyjnego na podstawie zagregowanego ryzyka wynikającego z działania i użytkowania systemów oraz odpowiednich środowisk działania, za które organizacja jest odpowiedzialna;
- Zapewnienie nadzoru nad działaniami związanymi z zarządzaniem ryzykiem prowadzonymi przez organizacje, aby pomóc w zapewnieniu spójnych i skutecznych decyzji opartych na analizie ryzyka;
- Rozwijanie szeroko rozumianego ryzyka w zakresie strategicznego celu organizacji i ich zintegrowanych działań;
- Ustanowienie skutecznych narzędzi i pełnienie funkcji centralnego punktu przekazywania i dzielenia się informacjami o ryzyku pomiędzy kluczowymi interesariuszami (np. osobami autoryzującymi i innymi kierownikami wyższego szczebla) wewnętrznie i zewnętrznie z organizacjami;
- Określanie stopnia autonomii organizacji podrzędnych dopuszczonych przez organizacje macierzyste w zakresie opracowywania, oceny, reagowania i monitorowania ryzyka;

- Promowanie współpracy i współdziałania między osobami autoryzującymi do podejmowania działań autoryzacyjnych wymagających współodpowiedzialności (np. wspólnych autoryzacji);
- Stworzenie forum obejmującego całą organizację w celu rozważenia wszystkich źródeł ryzyka (w tym ryzyka łącznego) dla operacji i aktywów organizacji, osób, innych organizacji i Państwa;
- Dopilnowanie, aby decyzje dotyczące autoryzacji uwzględniały wszystkie czynniki niezbędne do osiągnięcia misji i sukcesu biznesowego; oraz
- Zapewnienie, że współodpowiedzialność za wspieranie misji organizacyjnych i funkcji biznesowych z wykorzystaniem zewnętrznych dostawców opiera się na odpowiedniej przejrzystości i jest skierowana do odpowiednich organów decyzyjnych.

Funkcja wykonawcza ds. ryzyka (RE) nie posiada określonej struktury organizacyjnej ani formalnej odpowiedzialności przypisanej do jednej osoby lub grupy w organizacji. Kierownicy jednostek organizacyjnych mogą zdecydować o utrzymaniu funkcji wykonawczej ds. ryzyka lub o przekazaniu tej funkcji. Funkcja wykonawcza ds. ryzyka wymaga połączenia umiejętności, wiedzy i perspektyw w celu zrozumienia strategicznych celów i zadań organizacji, misji organizacji / funkcji biznesowych, możliwości i ograniczeń technicznych oraz kluczowych kompetencji i wytycznych, które kształtują działania organizacji. W celu zapewnienia tej niezbędnej kombinacji, funkcja wykonawcza ds. ryzyka może być wypełniana przez jedną osobę lub zespół (wspierany przez ekspertów) lub przez wyznaczoną grupę (np. radę ds. ryzyka, wykonawczy komitet sterujący, wykonawczą radę kierowniczą). Funkcja wykonawcza ds. ryzyka wpisuje się w strukturę zarządzania organizacyjnego, ażeby ułatwić wydajność i skuteczność.

ARCHITEKT BEZPIECZEŃSTWA INFORMACJI LUB OCHRONY PRYWATNOŚCI I OCHRONY DANYCH OSOBOWYCH – SECA/PA

Architekt bezpieczeństwa informacji lub ochrony prywatności i ochrony danych osobowych *(ang. security or privacy architect – SecA/PA)* jest osobą, grupą lub organizacją odpowiedzialną za zapewnienie, że potrzeby w zakresie ochrony interesariuszy i odpowiadające im wymagania systemowe niezbędne do ochrony misji organizacji i funkcji biznesowych oraz prywatności osób są odpowiednio uwzględniane w architekturze korporacyjnej, w tym w modelach referencyjnych, architekturze segmentów i architekturze rozwiązań (systemach wspierających misję i procesy biznesowe). Architekt bezpieczeństwa informacji lub ochrony prywatności i ochrony danych osobowych służy, jako główny łącznik pomiędzy architektem korporacyjnym, a inżynierem bezpieczeństwa systemów lub inżynierem ochrony prywatności i ochrony danych osobowych i współpracuje z właścicielami systemów, dostawcami zabezpieczeń wspólnych oraz SSPO w zakresie przydzielania zabezpieczeń.

Architekt bezpieczeństwa informacji lub ochrony prywatności i ochrony danych osobowych, we współpracy z SSPO, doradzają osobom autoryzującym, CIO, SAORM lub RE, SAISO, SAOP w zakresie szeregu kwestii dotyczących bezpieczeństwa i ochrony prywatności. Przykłady obejmują ustanowienie granic autoryzacji; ustanowienie alarmów bezpieczeństwa lub prywatności; ocenę powagi niedociągnięć w systemie lub mechanizmach bezpieczeństwa; opracowanie planów i etapów działania; tworzenie podejść do ograniczania ryzyka; oraz potencjalnych negatywnych skutków zidentyfikowanych podatności lub zagrożeń dla prywatności.

Jeśli architekt bezpieczeństwa informacji lub ochrony prywatności i ochrony danych osobowych pełnią odrębne role, architekt bezpieczeństwa informacji (SecA) jest generalnie odpowiedzialny za te aspekty architektury korporacyjnej, które chronią informacje i systemy informatyczne przed nieautoryzowaną działalnością lub określają zachowanie systemu w celu zapewnienia poufności, integralności i dostępności. Architekt ochrony prywatności

i ochrony danych osobowych (PA) jest odpowiedzialny za te aspekty architektury korporacyjnej, które zapewniają zgodność z wymogami ochrony prywatności i zarządzają zagrożeniami dla prywatności osób fizycznych związanymi z przetwarzaniem danych osobowych. Obowiązki architekta bezpieczeństwa informacji i ochrony prywatności i ochrony danych osobowych nakładają się na siebie w odniesieniu do tych aspektów architektury korporacyjnej, które chronią bezpieczeństwo danych osobowych.

SENIOR ACCOUNTABLE OFFICIAL FOR RISK MANAGEMENT - SAORM

SAORM to osoba posiadająca wiedzę we wszystkich obszarów jednostki organizacyjnej i jest odpowiedzialna za dostosowanie procesów zarządzania bezpieczeństwem informacji do procesów planowania strategicznego, operacyjnego i budżetowego. Kieruje i zarządza funkcją wykonawczą ds. ryzyka (RE) w organizacji i jest odpowiedzialna za dostosowanie procesów zarządzania ryzykiem w zakresie bezpieczeństwa informacji i ochrony prywatności do procesów planowania strategicznego, operacyjnego i budżetowego. Funkcję SAORM pełni kierownik jednostki organizacyjnej lub osoba przez niego wyznaczona. SAORM określa strukturę organizacyjną i zakres obowiązków osoby odpowiedzialnej za funkcje wykonawcze ds. ryzyka (RE) i w porozumieniu z kierownikiem jednostki organizacyjnej może zachować funkcję wykonawczą ds. ryzyka (RE) lub przekazać tę funkcję innej osobie lub grupie organizacyjnej.

SENIOR AGENCY INFORMATION SECURITY OFFICER - SAISO

SAISO jest osobą w organizacji odpowiedzialną za wspomaganie CIO w wykonywaniu jego obowiązków i pełniącym funkcję głównego łącznika CIO z osobami autoryzującymi, właścicielami systemów, dostawcami zabezpieczeń wspólnych i *SSO*. SAISO jest również odpowiedzialny za koordynację z SAOP w celu zapewnienia koordynacji między programami ochrony prywatności i bezpieczeństwa informacji. SAISO posiada kwalifikacje zawodowe, w tym wykształcenie i doświadczenie, wymagane do zarządzania funkcjami programów bezpieczeństwa; zarządza funkcjami w zakresie bezpieczeństwa, jako podstawowymi obowiązkami; oraz kieruje zespołem, którego misją i zadaniem jest wspieranie organizacji

w osiąganiu godnych zaufania, bezpiecznych informacji i systemów zgodnych z wymogami prawa. SAISO może pełnić funkcję AODR lub osoby oceniającej zabezpieczenia. Organizacje mogą również zamiast nazwy SAISO posługiwać się nazewnictwem (w zależności od kultury organizacyjnej jednostki organizacyjnej): ***Senior Information Security Officer*** (***SISO***) lub ***Chief Information Security Officer*** (***CISO***). Są to kluczowe osoby w jednostce organizacyjnej odpowiedzialne za bezpieczeństwo informacji.

SENIOR AGENCY OFFICIAL FOR PRIVACY - SAOP

SAOP to osoba odpowiedzialna za prywatność i ochronę danych osobowych w jednostce organizacyjnej i zapewnienie zgodności z obowiązującymi wymogami w zakresie ochrony prywatności i zarządzanie ryzykiem w zakresie ochrony prywatności. SAOP odpowiada między innymi za:

- Współpracę z SAISO w celu zapewnienia koordynacji działań w zakresie ochrony prywatności i bezpieczeństwa informacji;
- Przeglądanie i zatwierdzanie kategoryzacji systemów informatycznych, które tworzą, gromadzą, wykorzystują, przetwarzają, przechowują, utrzymują, rozpowszechniają, publikują lub usuwają dane osobowe;
- Określanie, które zabezpieczenia prywatności będą traktowane, jako zarządzane programowo, wspólne, specyficzne dla systemu i hybrydowe zabezpieczenia prywatności;
- Określanie metodologii oceny i metryk w celu ustalenia, czy zabezpieczenia w zakresie ochrony prywatności są wdrażane prawidłowo, działają zgodnie z założeniami i są wystarczające do zapewnienia zgodności z obowiązującymi przepisami w zakresie ochrony prywatności i wymogami odnoszącymi się do zarządzania ryzykiem w zakresie ochrony prywatności;
- Przeglądanie i zatwierdzanie planów ochrony prywatności w systemach informatycznych przed autoryzacją, reautoryzacją lub bieżącą autoryzacją;

- Przeglądanie pakietów autoryzacyjnych systemów informatycznych, które tworzą, gromadzą, wykorzystują, przetwarzają, przechowują, utrzymują, rozpowszechniają, publikują lub usuwają dane osobowe w celu zapewnienia zgodności z wymogami ochrony prywatności i zarządzania zagrożeniami dla prywatności;
- Prowadzenie i dokumentowanie wyników oceny zabezpieczeń w zakresie ochrony prywatności w celu weryfikacji stałej skuteczności wszystkich środków bezpieczeństwa w zakresie ochrony prywatności wybranych i wdrożonych w organizacji; oraz
- Ustanowienie i utrzymywanie programu ciągłego monitorowania prywatności w celu utrzymania stałej świadomości zagrożeń dla prywatności i oceny zabezpieczeń prywatności z częstotliwością wystarczającą do zapewnienia zgodności z wymogami dotyczącymi prywatności i zarządzania zagrożeniami dla prywatności.

ADMINISTRATOR SYSTEMU - SA

Administrator systemu (*ang. system administrator - SA)* jest osobą fizyczną, grupą lub organizacją odpowiedzialną za tworzenie i utrzymywanie systemu lub określonych elementów systemu. Do obowiązków administratora systemu należy na przykład instalacja, konfiguracja i aktualizacja sprzętu i oprogramowania, tworzenie i zarządzanie kontami użytkowników, nadzorowanie lub prowadzenie działań związanych z tworzeniem kopii zapasowych, odzyskiwaniem i odtwarzaniem danych, wdrażanie zabezpieczeń oraz przestrzeganie i egzekwowanie zasad i procedur bezpieczeństwa i ochrony prywatności w organizacji. Rola administratora systemu obejmuje inne typy administratorów systemu (np. administratorów baz danych, administratorów sieci, administratorów stron internetowych i administratorów aplikacji).

WŁAŚCICIEL SYSTEMU - SO

Właściciel systemu (*ang. system owner - SO)* jest osobą w organizacji odpowiedzialną za zaopatrzenie, rozwój, integrację, modyfikacje, eksploatację, utrzymanie i utylizację

systemu.[112] Właściciel systemu jest odpowiedzialny za uwzględnianie interesów operacyjnych społeczności użytkowników (tj. użytkowników, którzy potrzebują dostępu do systemu, aby wypełniać wymagania misji, biznesu lub cele operacyjne) oraz za zapewnienie zgodności z wymogami bezpieczeństwa. Właściciel systemu, we współpracy z osobami odpowiedzialnymi za bezpieczeństwo i prywatność systemu (SSPO), jest odpowiedzialny za opracowywanie i utrzymanie planów bezpieczeństwa i ochrony prywatności oraz zapewnia, że system jest eksploatowany zgodnie z wybranymi i wdrożonymi środkami bezpieczeństwa.

W porozumieniu z właścicielem informacji/władającym informacją, właściciel systemu decyduje, kto ma dostęp do systemu (i z jakimi rodzajami uprawnień lub prawami dostępu).[113] Właściciel systemu dba o to, aby użytkownicy systemu i personel pomocniczy uzyskali odpowiednie szkolenie z zakresu bezpieczeństwa i ochrony prywatności. W oparciu o wskazówki osoby autoryzującej, właściciel systemu informuje personel organizacji o konieczności przeprowadzenia autoryzacji, zapewnia, że zasoby są dostępne dla danego działania oraz zapewnia wymagany dostęp do systemu, informacji i dokumentacji zabezpieczeń, do przeprowadzania oceny przez osoby oceniające zabezpieczenia. Właściciel systemu otrzymuje wyniki oceny bezpieczeństwa i ochrony prywatności od osób oceniających zabezpieczenia. Po podjęciu odpowiednich kroków w celu zmniejszenia lub wyeliminowania luk lub zagrożeń dla bezpieczeństwa i prywatności, właściciel systemu składa pakiet autoryzacyjny i przedkłada go do autoryzacji osobie autoryzującej lub wyznaczonemu przez niego pełnomocnikowi AODR.[114]

[112] Organizacje mogą określać właścicieli systemów, jako menedżerów programów lub właścicieli przedsięwzięć / aktywów.

[113] Odpowiedzialność za podjęcie decyzji o tym, kto ma dostęp do określonych informacji w ramach systemu organizacyjnego (i z jakimi rodzajami uprawnień lub prawami dostępu) może spoczywać na właścicielu/odbiorcy informacji.

[114] Osoba autoryzująca może wyznaczyć osobę inną niż właściciel systemu do opracowania i zebrania informacji do pakietu autoryzacyjnego. W tej sytuacji wyznaczony pełnomocnik AODR koordynuje z właścicielem systemu działania związane z opracowaniem i zebraniem tych informacji.

SYSTEM SECURITY OR PRIVACY OFFICER - SSPO

SSPO to osoba odpowiedzialna za bezpieczeństwo oraz prywatność i ochronę danych osobowych w systemie teleinformatycznym / informatycznym jednostki organizacyjnej. [115]

Osoby te funkcjonują w ścisłej współpracy z właścicielem systemu. SSPO pełni również funkcję głównego doradcy we wszystkich sprawach, technicznych i innych, dotyczących zabezpieczeń systemu. SSPO posiada wiedzę i doświadczenie w zarządzaniu aspektami bezpieczeństwa lub prywatności systemu organizacyjnego, a w wielu organizacjach jest odpowiedzialny za codzienne operacje związane z bezpieczeństwem lub prywatnością systemu. Odpowiedzialność ta może również obejmować między innymi: ochronę fizyczną i ochronę środowiska, bezpieczeństwo osobowe, obsługę incydentów oraz szkolenie i świadomość w zakresie bezpieczeństwa i prywatności.

SSPO może zostać wyznaczony do pomocy w opracowaniu polityki i procedur bezpieczeństwa i ochrony prywatności na poziomie systemu oraz do zapewnienia zgodności z tymi politykami i procedurami. W ścisłej współpracy z właścicielem systemu SSPO często odgrywa aktywną rolę w monitorowaniu systemu i środowiska jego działania, w tym w opracowywaniu i aktualizowaniu planów bezpieczeństwa i ochrony prywatności, zarządzaniu i kontrolowaniu zmian w systemie oraz ocenie wpływu tych zmian na bezpieczeństwo lub prywatność.

W przypadku, gdy SSPO pełni odrębne role w zakresie bezpieczeństwa systemu i ochrony prywatności, ***system security officer*** (**SSO**) jest zasadniczo odpowiedzialny za te aspekty systemu, które chronią informacje i systemy informatyczne przed nieautoryzowaną działalnością lub zachowaniem systemu w celu zapewnienia poufności, integralności i dostępności. ***System privacy officer*** (**SPO)** jest odpowiedzialny za te aspekty systemu, które

[115] Organizacje mogą określić rolę menadżera ds. Bezpieczeństwa systemu lub menadżera ds. Bezpieczeństwa określając mu obowiązki przypisane do SSO lub z odpowiedzialnością za nadzór nad programem bezpieczeństwa. W takich sytuacjach SSO może, według uznania organizacji, raportować bezpośrednio do menadżera ds. Bezpieczeństwa systemu lub menadżera ds. Bezpieczeństwa. Organizacje mogą przydzielić równoważne obowiązki w zakresie ochrony prywatności oddzielnym osobom posiadającym odpowiednią wiedzę merytoryczną.

zapewniają zgodność z wymogami ochrony prywatności i zarządzają ryzykiem utraty prywatności przez osoby fizyczne związanym z przetwarzaniem danych osobowych. Obowiązki SSO i SPO nakładają się na siebie w odniesieniu do tych aspektów systemu, które zapewniają bezpieczeństwo danych osobowych.

UŻYTKOWNIK SYSTEMU - SU

Użytkownik systemu (*ang. system user - SU)* jest osobą fizyczną lub procesem (systemowym) działającym w imieniu osoby fizycznej, która jest uprawniona do dostępu do informacji i systemów informatycznych w celu wykonywania przydzielonych jej obowiązków. Obowiązki użytkownika systemu obejmują między innymi przestrzeganie zasad organizacyjnych, które regulują dopuszczalne użytkowanie systemów organizacyjnych, korzystanie z zasobów informatycznych dostarczonych przez organizację tylko do określonych celów oraz zgłaszanie anomalii lub podejrzanego zachowania systemu.

INŻYNIER BEZPIECZEŃSTWA SYSTEMÓW, OCHRONY PRYWATNOŚCI I DANYCH OSOBOWYCH - SSPE

Inżynier bezpieczeństwa systemów, ochrony prywatności i danych osobowych (*ang. systems security or privacy engineer - SSPE)* to osoba, grupa lub organizacja odpowiedzialna za prowadzenie działań z zakresu bezpieczeństwa systemów lub inżynierii prywatności w ramach SDLC. Inżynieria bezpieczeństwa i prywatności systemów jest procesem, który zdobywa i udoskonala wymagania dotyczące bezpieczeństwa i prywatności systemów oraz zapewnia, że wymagania te są skutecznie zintegrowane z systemami i elementami systemu poprzez architekturę bezpieczeństwa lub prywatności, projektowanie, rozwój i konfigurację. Inżynierowie bezpieczeństwa i ochrony prywatności systemów są częścią zespołu programistów - projektują i rozwijają systemy organizacyjne lub modernizują istniejące systemy wraz z zapewnieniem, że wymagania dotyczące ciągłego monitorowania są uwzględniane na poziomie systemu. Inżynierowie bezpieczeństwa systemów lub ochrony prywatności stosują najlepsze praktyki podczas wdrażania zabezpieczeń, w tym metodologię inżynierii oprogramowania; zasady inżynierii systemów i bezpieczeństwa lub ochrony

prywatności; projektowanie bezpieczne lub zwiększające ochronę prywatności, bezpieczną lub zwiększającą ochronę prywatności architekturę oraz bezpieczne lub zwiększające ochronę prywatności techniki kodowania. Inżynierowie bezpieczeństwa systemów, ochrony prywatności i danych osobowych koordynują działania w zakresie bezpieczeństwa i ochrony prywatności z SAISO, SAOP, architektami bezpieczeństwa i ochrony prywatności, właścicielami systemów, dostawcami zabezpieczeń wspólnych oraz SSPO.

W przypadku, gdy inżynier bezpieczeństwa systemów, ochrony prywatności i danych osobowych (SSPE) pełnią odrębne role, inżynier bezpieczeństwa systemów (*ang.* ***systems security engineer*** *– SSE)* jest zasadniczo odpowiedzialny za działania związane z ochroną informacji i systemów informatycznych przed nieautoryzowaną dzi ałalnością lub zachowaniem systemu w celu zapewnienia poufności, integralności i dostępności. Inżynier ochrony prywatności i danych osobowych (*ang.* ***systems privacy engineer – SPE***) jest odpowiedzialny za czynności związane z zapewnieniem zgodności z wymaganiami w zakresie ochrony prywatności i zarządzaniem zagrożeniami dla prywatności osób fizycznych związanymi z przetwarzaniem danych osobowych. Obowiązki inżyniera bezpieczeństwa systemów oraz inżyniera ochrony prywatności i danych osobowych nakładają się na siebie w odniesieniu do aspektów architektury korporacyjnej, które chronią bezpieczeństwo danych osobowych.

ZAŁĄCZNIK E ZESTAWIENIE ZADAŃ RMF

ZADANIA, OBOWIĄZKI I ROLE POMOCNICZE RMF

PRZYGOTOWANIE ZADAŃ, PODSTAWOWA ODPOWIEDZIALNOŚĆ I ROLE POMOCNICZE

TABELA E-1

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
Poziom organizacji		
Zadanie P-1 **Role zarządzające ryzykiem** Identyfikacja i przypisanie poszczególnych osób do określonych ról związanych z zarządzaniem ryzykiem w zakresie bezpieczeństwa i ochrony prywatności.	• HA • CIO • SAOP	• AO LUB AODR • SAORM / RE • SAISO
Zadanie P-2 **Strategia zarządzania ryzykiem** Ustalenie strategii zarządzania ryzykiem dla organizacji, która obejmuje określenie tolerancji ryzyka.	• HA	• SAORM / RE • CIO • SAISO • SAOP

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
Zadanie P-3 **Szacowanie ryzyka - organizacja** Ocena zagrożeń bezpieczeństwa i prywatności w całej organizacji oraz bieżąca aktualizacja wyników szacowania ryzyka.	• SAORM / RE • SAISO • SAOP	• CIO • AO LUB AODR • BO
Zadanie P-4 **Dostosowywanie przez organizację zabezpieczeń bazowych i profili ram cyberbezpieczeństwa (opcjonalnie)** Ustanowienie, udokumentowanie i opublikowanie dostosowanych przez organizację zabezpieczeń bazowych i/lub Profili Ram Cyberbezpieczeństwa.	• BO • SAORM / RE	• CIO • AO LUB AODR • SAISO • SAOP
Zadanie P-5 **Identyfikacja zabezpieczeń wspólnych** Zidentyfikowanie, udokumentowanie i opublikowanie zabezpieczeń wspólnych, które są dostępne do dziedziczenia przez systemy organizacji.	• SAISO • SAOP	• BO • SAORM / RE • CIO • AO LUB AODR • CCP • BO

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
Zadanie P-6 **Priorytetyzacja na poziomie wpływu (opcjonalnie)** Priorytetyzacja systemów organizacji o tym samym poziomie wpływu.	• SAORM / RE	• SAISO • SAOP • BO • HA • CIO • AO LUB AODR
Zadanie P-7 **Strategia ciągłego monitorowania – organizacja** Opracowanie i wdrożenie w całej organizacji strategii ciągłego monitorowania skuteczności zabezpieczeń.	• SAORM / RE	• CIO • SAISO • SAOP • BO • SO • AO LUB AODR
Poziom systemu		
Zadanie P-8 **Misja lub przedmiot działalności** Określenie misji, funkcji biznesowych oraz procesów biznesowych, które system ma wspierać.	• BO	• AO LUB AODR • BO • AO LUB AODR • CIO • SAISO • SAOP

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
Zadanie P-9 **Interesariusze systemu** Określenie podmiotów, które są zainteresowane zaprojektowaniem, opracowaniem, wdrożeniem, oceną, eksploatacją, utrzymaniem lub wycofaniem systemu.	• BO • HA	• CIO • AO LUB AODR • IO/S • SAISO • SAOP • CAO
Zadanie P-10 **Identyfikacja aktywów** Identyfikacja aktywów, które wymagają ochrony.	• BO	• AO LUB AODR • BO • IO/S • SAISO • SAOP • SA
Zadanie P-11 **Granica autoryzacji** Ustalenie granicy autoryzacji systemu.	• AO	• CIO • BO • BO • SAISO • SAOP • EA

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
Zadanie P-12 **Typ informacji** Określanie typów informacji, które mają być przetwarzane, przechowywane i przekazywane przez system.	• SO • IO/S	• SSO • SPO • BO
Zadanie P-13 **Cykl życia informacji** Określenie i zrozumienie wszystkich etapów cyklu życia informacji dla każdego typu informacji przetwarzanych, przechowywanych lub przesyłanych przez system.	• SAOP • SO • IO/S	• CIO • BO • SA • PA • EA • SSE • PA
Zadanie P-14 **System szacowania ryzyka** Szacowanie ryzyka na poziomie systemu i bieżąca aktualizacja wyników szacowania ryzyka.	• BO • SSO • SPO	• SAORM / RE • AO LUB AODR • BO • IO/S • SSO

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
Zadanie P-15 **Definicja wymagań** Zdefiniowanie wymagań dotyczących bezpieczeństwa i ochrony prywatności systemu oraz środowiska pracy.	• BO • BO • IO/S • SPO	• AO LUB AODR • SAISO • SAOP • SSO • CAO • SA • PA • EA
Zadanie P-16 **Architektura korporacyjna** Ustalenie umiejscowienia systemu w architekturze korporacyjnej	• BO • EA • EA • PA	• CIO • AO LUB AODR • SAISO • SAOP • SO • IO/S
Zadanie P-17 **Przydział wymagań** Przydzielenie wymagań dotyczących bezpieczeństwa i ochrony prywatności do systemu i środowiska pracy.	• SA • PA • SSO • SPO	• CIO • AO LUB AODR • BO • SAISO • SAOP • BO

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
Zadanie P-18 **Rejestracja systemu** Rejestracja systemu w programie organizacyjnym lub biurach zarządzających.	• SO	• BO • CIO • SSO • SPO

KATEGORYZACJA ZADAŃ, PODSTAWOWA ODPOWIEDZIALNOŚĆ I ROLE POMOCNICZE

TABELA E-2

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE C-1 **Opis systemu** Udokumentować charakterystykę systemu.	• BO	• AO LUB AODR • IO/S • SSO • SPO
ZADANIE C-2 **Kategoryzacja bezpieczeństwa** Skategoryzować system i udokumentować wyniki kategoryzacji bezpieczeństwa.	• BO • IO/S	• SAORM / RE • CIO • SAISO • AO LUB AODR • SSO • SPO
ZADANIE C-3 **Przegląd i zatwierdzanie kategorii bezpieczeństwa** Przegląd i zatwierdzenie wyników kategoryzacji bezpieczeństwa i decyzji.	• AO lub AODR • SAOP	• SAORM / RE • CIO • SAISO

WYBÓR ZADAŃ, PODSTAWOWA ODPOWIEDZIALNOŚĆ I ROLE POMOCNICZE

TABELA E-3

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE S-1 **Wybór zabezpieczeń** Wybór zabezpieczeń systemu i środowiska pracy.	• BO • CCP	• AO LUB AODR • IO/S • SSE • PA • SSO • SPO
ZADANIE S-2 **Dostosowywanie zabezpieczeń** Dostosowywanie wybranego zabezpieczenia do systemu i środowiska pracy.	• BO • CCP	• AO LUB AODR • IO/S • SSE • PA • SSO • SPO
ZADANIE S-3 **Przydział zabezpieczeń** Przydzielenie środków bezpieczeństwa i ochrony prywatności do systemu i środowiska pracy.	• SA • PA • SSO • SPO	• CIO • AO LUB AODR • BO • SAISO • SAOP • SO

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE S-4 **Dokumentacja wdrożenia planowanych zabezpieczeń** Dokumentowanie zabezpieczeń systemu i środowiska pracy w planach bezpieczeństwa i ochrony prywatności.	• BO • CCP	• AO lub AODR • IO/S • SSE • PA • SSO • SPO
ZADANIE S-5 **Strategia ciągłego monitorowania systemu** Opracowanie i wdrożenie na poziomie systemowym strategii monitorowania skuteczności zabezpieczeń, która jest spójna z organizacyjną strategią ciągłego monitorowania i stanowi jej uzupełnienie.	• SO • CCP	• SAORM / RE • CIO • SAISO • SAOP • AO lub AODR • IO/S • SA • PA • SSE • PA • SSO • SPO

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE S-6 **Przegląd i zatwierdzenie planu** Przegląd i zatwierdzenie planów bezpieczeństwa i ochrony prywatności systemu i środowiska pracy.	• AO LUB AODR	• SAORM / RE • CIO • SAISO • SAOP • CAO

WDROŻENIE ZADAŃ, PODSTAWOWA ODPOWIEDZIALNOŚĆ I ROLE POMOCNICZE

TABELA E-4:

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE I-1 **Wdrożenie zabezpieczeń** Wdrożenie zabezpieczeń w ramach planów bezpieczeństwa i ochrony prywatności.	• BO • CCP	• IO/S • SA • PA • SSE • PA • SSO • SPO • EA • SA
ZADANIE I-2 **Aktualizacja informacji o realizacji zabezpieczeń** Dokumentowanie zmian w planowanych wdrożeniach zabezpieczeń w stosunku do zaimplementowanych dotychczas zabezpieczeń..	• BO • CCP	• IO/S • SA • PA • SSE • PA • SSO • SPO • EA • SA

OCENA ZADAŃ, PODSTAWOWA ODPOWIEDZIALNOŚĆ I ROLE POMOCNICZE

TABELA E-5

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE A-1 **Wybór podmiot oceniający** Wybór odpowiedniego podmiot oceniający lub zespołu podmiot oceniający do przeprowadzenia danego rodzaju oceny zabezpieczeń, która ma zostać przeprowadzona.	• AO LUB AODR	• CIO • SAISO • SAOP
ZADANIE A-2 **Plan oceny** Opracowanie, przegląd i zatwierdzenie planów oceny wdrożonych zabezpieczeń.	• AO LUB AODR • CA	• SAISO • SAOP • BO • CCP • IO/S • SSO • SPO

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE A-3 **Ocena zabezpieczeń** Ocena zabezpieczeń zgodnie z procedurami oceny opisanymi w planach oceny.	• CA	• AO LUB AODR • BO • CCP • IO/S • SAISO • SAOP • SSO • SPO
ZADANIE A-4 **Sprawozdania z oceny** Przygotowanie sprawozdań z oceny dokumentujących ustalenia i zalecenia wynikające z oceny zabezpieczeń.	• CA	• BO • CCP • SSO • SPO
ZADANIE A-5 **Działania naprawcze** Przeprowadzenie wstępnych działań korygujących w zakresie środków bezpieczeństwa i ponownej oceny skorygowanych zabezpieczeń.	• BO • CCP • CA	• AO LUB AODR • SAISO • SAOP • SAORM / RE • IO/S • SSE • PA • SSO • SPO

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE A-6 **Plan i etapy działania** Przygotowanie planu działania i głównych etapów w oparciu o ustalenia i zalecenia zawarte w sprawozdaniach z oceny.	• BO • CCP	• IO/S • SSO • SPO • SAISO • SAOP • CAO • CA

AUTORYZACJA ZADAŃ, PODSTAWOWA ODPOWIEDZIALNOŚĆ I ROLE POMOCNICZE

TABELA E-6

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE R-1 **Pakiet autoryzacyjny** Skompletowanie pakietu autoryzacyjnego i przedłożenie go osobie autoryzującej w celu podjęcia decyzji o autoryzacji.	• BO • CCP	• SSO • SPO • SAISO • SAOP • CA
ZADANIE R-2 **Analiza i określenie ryzyka** Analiza i określenie ryzyka związanego z działaniem lub użytkowaniem systemu lub zapewnieniem zabezpieczeń wspólnych.	• AO LUB AODR	• SAORM / RE • SAISO • SAOP
ZADANIE R-3 **Reakcja na ryzyko** Określenie i wdrożenie preferowanego sposobu postępowania w odpowiedzi na określone ryzyko.	• AO LUB AODR	• SAORM / RE • SAISO • SAOP • BO lub CCP • IO/S • SSE • PA • SSO • SPO

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE R-4 **Decyzja autoryzująca** Ustalenie, czy ryzyko wynikające z działania lub stosowania systemu informatycznego, albo zapewnienia lub stosowania zabezpieczeń wspólnych, jest dopuszczalne.	• AO	• SAORM / RE • CIO • SAISO • SAOP • AODR
ZADANIE R-5 **Sprawozdania z autoryzacji** Zgłoszenie decyzji o zezwoleniu oraz wszelkich niedoskonałościach zabezpieczeń, które stanowią znaczące zagrożenie dla bezpieczeństwa lub prywatności.	• AO LUB AODR	• SO lub CCP • IO/S • SSO • SPO • SAISO • SAOP

MONITOROWANE ZADAŃ, PODSTAWOWA ODPOWIEDZIALNOŚĆ I ROLE POMOCNICZE

TABELA E-7

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE M-1 **Zmiany systemowe i środowiskowe** Monitorowanie systemu informatycznego i jego środowisko pracy pod kątem zmian, które mają wpływ na bezpieczeństwo i prywatność systemu.	• SO lub CCP • SAISO • SAOP	• SAORM / RE • AO LUB AODR • IO/S • SSO • SPO
ZADANIE M-2 **Oceny bieżące** Ocena zabezpieczeń zaimplementowanych w ramach systemu i dziedziczonych przez system zgodnie ze strategią ciągłego monitorowania.	• CA	• AO LUB AODR • SO lub CCP • IO/S • SSO • SPO • SAISO • SAOP

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE M-3 **Bieżąca reakcja na ryzyko** Reakcja na ryzyko na podstawie wyników trwających działań monitorujących, szacowania ryzyka i zaległych pozycji w planach i etapach działania.	• AO • BO • CCP	• SAORM / RE • SAISO • SAOP / AODR • IO/S • SSO / SPO • SSE • PA • SA • PA
ZADANIE M-4 **Aktualizacje pakietów autoryzacyjnych** Aktualizacja planów, sprawozdań z oceny oraz planów i etapów działań na podstawie wyników procesu ciągłego monitorowania.	• BO • CCP	• IO/S • SSO • SPO • SAOP • SAISO

ZADANIA RMF	PODSTAWOWA ODPOWIEDZIALNOŚĆ	ROLE POMOCNICZE
ZADANIE M-5 **Sprawozdawczość w zakresie bezpieczeństwa i ochrony prywatności** Informuje na bieżąco uprawniony personel i innych przedstawicieli organizacji o stanie bezpieczeństwa i prywatności systemu, zgodnie z organizacyjną strategią ciągłego monitorowania.	• BO • CCP • SAISO • SAOP	• SSO • SSO
ZADANIE M-6 **Bieżąca autoryzacja** Bieżący przegląd pozycji systemu w zakresie bezpieczeństwa i ochrony prywatności w celu ustalenia, czy ryzyko jest nadal dopuszczalne.	• AO	• SAORM / RE • CIO • SAISO • SAOP • AODR
ZADANIE M-7 **Utylizacja systemu** Wdrożenie strategii utylizacji systemu i przeprowadzenie wymaganych czynności w przypadku usunięcia systemu z eksploatacji.	• BO	• AO LUB AODR • IO/S • SSO / SPO • SAORM / RE • SAISO • SAOP

ZAŁĄCZNIK F AUTORYZACJA SYSTEMU I ZABEZPIECZEŃ WSPÓLNYCH

Decyzje autoryzacyjne i ewidencja uzupełniająca

Niniejszy załącznik zawiera informacje na temat autoryzacji systemu i zabezpieczeń wspólnych, które obejmują: rodzaje autoryzacji; zawartość pakietów autoryzacyjnych; decyzje autoryzacyjne; dokumenty decyzji autoryzacyjnych; autoryzację bieżącą; autoryzację powtórną; sterowane zdarzenia wyzwalające i znaczące zmiany; autoryzację typu i obiektu; oraz podejścia do autoryzacji.

RODZAJE AUTORYZACJI

Autoryzacja jest procesem, w ramach którego personel wyższego szczebla, osoba autoryzująca, dokonuje przeglądu informacji dotyczących bezpieczeństwa i ochrony prywatności, opisując aktualny stan w zakresie bezpieczeństwa i ochrony prywatności systemów informatycznych lub zabezpieczeń wspólnych, które są dziedziczone przez systemy. Osoba autoryzująca wykorzystuje te informacje w celu określenia, czy ryzyko związane z obsługą systemu lub zapewnieniem zabezpieczeń wspólnych jest akceptowalne – i jeśli jest, jednoznacznie akceptuje to ryzyko. Informacje dotyczące bezpieczeństwa i ochrony prywatności są przedstawiane osobie autoryzującej, jako pakiet autoryzacyjny, który może składać się z raportu z narzędzia do automatycznego zarządzania bezpieczeństwem/prywatnością i raportowania. [116] Autoryzacja systemowa i zabezpieczeń wspólnych odbywa się w ramach etapu *Autoryzacji* RMF. Autoryzacja systemowa lub zabezpieczeń wspólnych może być autoryzacją wstępną, bieżącą lub ponowną zdefiniowaną poniżej:

- *Autoryzacja wstępna* jest zdefiniowana, jako wstępne (rozruch) określenie ryzyka i decyzji o akceptacji ryzyka na podstawie pełnego, zerowego przeglądu systemu lub zabezpieczeń wspólnych. Przegląd systemu oparty na podejściu zerowym obejmuje

[116] [SP 800-137] dostarcza informacji na temat zautomatyzowanych narzędzi do zarządzania bezpieczeństwem i sprawozdawczości. Przyszłe publikacje będą dotyczyły narzędzi zarządzania prywatnością i narzędzi sprawozdawczych.

ocenę wszystkich wdrożonych zabezpieczeń na poziomie systemu (w tym części zabezpieczeń hybrydowych na poziomie systemu) oraz przegląd stanu bezpieczeństwa odziedziczonych zabezpieczeń wspólnych określonych w planach bezpieczeństwa i ochrony prywatności.[117] Przegląd zabezpieczeń wspólnych oparty na przeglądzie zerowym (innym niż zabezpieczeń wspólnych opartych na przeglądach systemowych) obejmuje ocenę stosowanych zabezpieczeń (np. polityki, procedur operacyjnych, informacji dotyczących wdrażania), które przyczyniają się do zapewnienia zabezpieczeń wspólnych lub zestawu zabezpieczeń wspólnych.

- *Autoryzacja bieżąca* definiowana jest, jako kolejne (następcze) ustalenia dotyczące ryzyka i decyzje o akceptacji ryzyka podejmowane z uzgodnioną i udokumentowaną częstotliwością, zgodnie z misją/wymogami biznesowymi organizacji i tolerancją ryzyka organizacyjnego. Autoryzacja bieżąca jest procesem autoryzacji czasowej lub zdarzeniowej. Osoba autoryzująca otrzymuje niezbędne informacje dotyczące bezpieczeństwa i prywatności systemu w czasie zbliżonym do rzeczywistego w celu określenia, czy ryzyko związane z misją/przedsiębiorstwem kontynuowania działania systemu lub zapewnienia zabezpieczeń wspólnych jest dopuszczalne. Autoryzacja bieżąca jest zasadniczo związana z ciągłym zrozumieniem i akceptacją ryzyka związanego z bezpieczeństwem i prywatnością i jest uzależniona od solidności programu ciągłego monitorowania.
- *Reautoryzacja* jest definiowana, jako statyczne, jednopunktowe określenie ryzyka i decyzji o akceptacji ryzyka, która następuje po wstępnej autoryzacji. Generalnie, działania związane z ponowną autoryzacją mogą być czasowe lub zdarzeniowe. Jednakże, w ramach bieżącej autoryzacji, w większości przypadków, reautoryzacja jest działaniem

[117] Zerowy przegląd systemu nie wymaga zerowego przeglądu zabezpieczeń wspólnych, które są dostępne podczas dziedziczenia przez ten system. Zabezpieczenia wspólne są autoryzowane w ramach odrębnego procesu autoryzacji, przy czym odrębna osoba autoryzująca przyjmuje ryzyko związane z dostarczeniem tych zabezpieczeń. Przegląd planów bezpieczeństwa i ochrony prywatności zawierających zabezpieczenia wspólne jest konieczny w celu zrozumienia obecnego stanu zabezpieczeń dziedziczonych przez systemy organizacyjne i uwzględnienia tych informacji w decyzjach opartych na ryzyku związanym z systemem.

wywołanym przez zdarzenie, zainicjowanym przez osobę autoryzującą, SAORM lub RE w odpowiedzi na zdarzenie, które skutkuje ryzykiem bezpieczeństwa i prywatności powyżej poziomu ryzyka zaakceptowanego wcześniej przez osobę autoryzującą. Reautoryzacja składa się z przeglądu systemu lub zabezpieczeń wspólnych, wykonywanych podobnie jak w przeglądzie przeprowadzanym podczas autoryzacji wstępnej. Reautoryzacja różni się od autoryzacji wstępnej, ponieważ osoba autoryzująca może zdecydować się na zainicjowanie pełnego przeglądu systemu lub zabezpieczeń wspólnych w oparciu o przegląd zerowy lub na zainicjowanie ukierunkowanego przeglądu w oparciu o rodzaj zdarzenia, które spowodowało reautoryzację. Reautoryzacja jest czynnością odrębną od trwającego procesu autoryzacji. Jednak informacje dotyczące bezpieczeństwa i ochrony prywatności generowane w ramach programu ciągłego monitorowania mogą być wykorzystywane do wsparcia procesu reautoryzacji. Działania związane z ponowną autoryzacją mogą wymagać przeglądu i zmian w strategii ciągłego monitorowania bezpieczeństwa i ochrony prywatności informacji organizacji, co z kolei może mieć wpływ na trwającą autoryzację.

PAKIET AUTORYZACYJNY

Pakiet autoryzacyjny zawiera zapis wyników oceny zabezpieczeń i dostarcza osobie autoryzującej informacje potrzebne do podjęcia decyzji w oparciu o ryzyko, czy zezwolić na działanie systemu lub zabezpieczeń wspólnych.[118] Właściciel systemu lub dostawca zabezpieczeń wspólnych jest odpowiedzialny za opracowanie, kompilację i złożenie pakietu autoryzacyjnego. Obejmuje to informacje dostępne z raportów generowanych przez narzędzie do automatycznego zarządzania bezpieczeństwem/prywatnością i raportowania. Właściciel systemu lub dostawca zabezpieczeń wspólnych otrzymuje informacje z wielu źródeł podczas przygotowywania pakietu autoryzacyjnego (np. SAISO; SAOP, SAORM lub RE; CA; SSO lub SPO; oraz program ciągłego monitorowania).

[118] Pakiety autoryzacyjne dla zabezpieczeń wspólnych, które nie są oparte na systemie, mogą nie zawierać planu bezpieczeństwa lub ochrony prywatności, ale zawierają zapis szczegółów realizacji zabezpieczeń wspólnych.

Pakiet autoryzacyjny[119] zawiera następujące elementy:

- Streszczenie;
- Plany bezpieczeństwa i ochrony prywatności; [120, 121]
- Sprawozdania z oceny bezpieczeństwa i ochrony prywatności;[122] oraz
- Plany i etapy działania.

Streszczenie przedstawia skonsolidowany przegląd informacji dotyczących bezpieczeństwa i ochrony prywatności w pakiecie autoryzacyjnym. Identyfikuje i podkreśla kwestie zarządzania ryzykiem związane z ochroną systemów informatycznych i środowisk, w których systemy te działają. Streszczenie dostarcza istotnych informacji niezbędnych osobie autoryzującej do zrozumienia zagrożeń dla bezpieczeństwa i prywatności operacji i aktywów organizacji, osób, innych organizacji i Państwa. Podsumowanie informacji może być wykorzystane przez osobę autoryzującą do podejmowania świadomych, opartych na ryzyku decyzji dotyczących działania i korzystania z systemu lub zapewnienia zabezpieczeń wspólnych, które mogą być dziedziczone przez systemy organizacyjne.

Plany bezpieczeństwa i ochrony prywatności przedstawiają przegląd wymogów bezpieczeństwa i ochrony prywatności oraz opisują zabezpieczenia, które zostały wprowadzone lub są planowane w celu spełnienia tych wymogów. [123] Plany dostarczają wystarczających informacji, aby zrozumieć zamierzone lub rzeczywiste wdrożenie zabezpieczeń zaimplementowanych w ramach systemu i wskazują zabezpieczenia, które są

[119] Osoba autoryzująca określa, jakie dodatkowe informacje pomocnicze, artefakty lub referencje mogą być wymagane w pakiecie autoryzacyjnym. Dodatkowa dokumentacja może zawierać np. Szacowanie ryzyka, plany awaryjne lub plany SCRM.

[120] [NSC 800-18] zawiera wskazówki dotyczące planów bezpieczeństwa systemu. Wskazówki dotyczące planów ochrony prywatności zostaną omówione w planowanej publikacji właściwej dla planów ochrony prywatności.

[121] Plan bezpieczeństwa systemu informatycznego i plan ochrony prywatności mogą być zintegrowane w jednym skonsolidowanym dokumencie.

[122] [NSC 800-53A] zawiera wytyczne dotyczące raportów oceny bezpieczeństwa. Wskazówki dotyczące raportów z oceny ochrony prywatności zostaną omówione w przyszłych publikacjach.

[123] Plan bezpieczeństwa systemu informatycznego i plan ochrony prywatności mogą być zintegrowane w jednym skonsolidowanym dokumencie.

wdrażane poprzez odziedziczone zabezpieczenia wspólne. Dodatkowo, plany ochrony prywatności opisują metodologie i wskaźniki, które będą stosowane do oceny zabezpieczeń. Plany bezpieczeństwa i ochrony prywatności mogą również zawierać, jako załączniki pomocnicze lub odniesienia, dodatkowe dokumenty, takie jak ocena wpływu na prywatność, umowy dotyczące bezpieczeństwa połączeń wzajemnych, konfiguracje bezpieczeństwa i prywatności, plan awaryjny, plan zarządzania konfiguracją, plan zarządzania ryzykiem w łańcuchu dostaw, plan reagowania na incydenty oraz strategia ciągłego monitorowania na poziomie systemu. Plany bezpieczeństwa i ochrony prywatności są aktualizowane za każdym razem, gdy zdarzenia dyktują zmiany w zabezpieczeniach wdrożonych w systemie lub odziedziczonych przez system.

Raporty z oceny bezpieczeństwa i ochrony prywatności, przygotowywane przez osobę oceniającą zabezpieczenia lub generowane przez zautomatyzowane narzędzia do zarządzania bezpieczeństwem/prywatnością i sprawozdawczością, zawierają ustalenia i wyniki oceny wdrożenia zabezpieczeń określonych w planach bezpieczeństwa i ochrony prywatności w celu określenia zakresu, w jakim zabezpieczenia są wdrażane prawidłowo, działają zgodnie z założeniami i dają pożądany rezultat w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatności. Sprawozdania z oceny mogą zawierać zalecane działania naprawcze w odniesieniu do niedociągnięć stwierdzonych w stosowanych zabezpieczeniach.[124] Osoba autoryzująca dokonuje przeglądu sprawozdań i określa odpowiednią reakcję na ryzyko [Zadanie R-3].

[124] Streszczenie przedstawia osobie autoryzującej skróconą wersję sprawozdań z oceny bezpieczeństwa i prywatności, koncentrując się na najważniejszych punktach oceny, podsumowaniu ustaleń i zaleceniach dotyczących usunięcia niedociągnięć w środkach bezpieczeństwa i ochrony prywatności.

Zarządzanie ryzykiem na potrzeby procesu autoryzacji w czasie zbliżonym do rzeczywistego, wymaga, aby raporty z szacowania ryzyka były na bieżąco aktualizowane za każdym razem, gdy wprowadzane są zmiany w zabezpieczeniach wdrożonych w systemie lub dziedziczonych przez ten system.[125] Aktualizacje raportów podmiot oceniających zapewniają właścicielom systemu, dostawcom zabezpieczeń wspólnych oraz osobom autoryzującym utrzymanie świadomości skuteczności zabezpieczeń. Skuteczność zabezpieczeń ma bezpośredni wpływ na bezpieczeństwo i prywatność systemu oraz na decyzje dotyczące świadomej akceptacji ryzyka.

Plan i etapy działania opisują planowane środki mające na celu usunięcie niedociągnięć stwierdzonych w zabezpieczeniach w trakcie oceny oraz środki zaradcze odnoszące się do znanych słabości lub zagrożeń dla bezpieczeństwa i prywatności.[126] Treść i struktura planów i etapów działania są oparte na strategii zarządzania ryzykiem opracowanej w ramach funkcji wykonawczej ds. ryzyka i są zgodne z planami i etapami działania ustanowionymi przez organizację, które zawierają wszelkie wymagania określone w przepisach, rozporządzeniach wykonawczych, zasadach, dyrektywach lub standardach. Jeżeli systemy i środowiska, w których funkcjonują, mają więcej podatności niż dostępne zasoby, które można realistycznie uwzględnić, organizacje opracowują i wdrażają plany i etapy działania, które ułatwiają priorytetowe podejście do ograniczania ryzyka i są spójne w całej organizacji. Uszeregowane pod względem ważności i spójności podejście do ograniczania ryzyka gwarantuje, że plany i etapy działania oparte są na:

- Kategoryzacji bezpieczeństwa systemu oraz ocenie ryzyka związanego z bezpieczeństwem, prywatnością i łańcuchem dostaw;

[125] Ze względu na to, że w centrum uwagi (a nie w ramach konkretnego procesu) znajduje się pożądany rezultat bieżącego śledzenia i reagowania na wyniki oceny w celu ułatwienia podejmowania decyzji dotyczących zarządzania ryzykiem, organizacje mogą zarządzać i aktualizować informacje zawarte w raportach z oceny bezpieczeństwa przy użyciu dowolnego formatu lub metody zgodnej z wewnętrznymi procesami organizacyjnymi.

[126] Jeżeli w wyniku działań łagodzących zostaną wprowadzone zmiany w planach i etapach działania, plany bezpieczeństwa systemu są odpowiednio aktualizowane.

- Określaniu luk (niedociągnięć) w stosowanych środkach bezpieczeństwa;
- Krytyczności niedociągnięć w zakresie zabezpieczeń (tj. bezpośredni lub pośredni wpływ, jaki niedociągnięcia mogą mieć na bezpieczeństwo i prywatność systemu oraz narażenie organizacji na ryzyko);[127]
- Podejściu organizacji do ograniczania ryzyka w celu wyeliminowania stwierdzonych niedociągnięć w zakresie stosowanych zabezpieczeń; oraz
- Uzasadnieniu zaakceptowania określonych luk w wprowadzonych zabezpieczeniach.

Strategie organizacyjne w zakresie planów i etapów działania są oparte na kategoryzacji bezpieczeństwa systemów, na które mają wpływ działania ograniczające ryzyko. Organizacje mogą na przykład zdecydować o przeznaczeniu swoich zasobów ograniczających ryzyko początkowo na systemy o największym wpływie lub inne aktywa o dużej wartości, ponieważ nieusunięcie znanych luk w tych systemach lub aktywach mogłoby mieć potencjalnie najbardziej znaczące negatywne skutki dla ich misji lub funkcji biznesowych. Organizacje traktują luki priorytetowo na podstawie informacji pochodzących z szacowania ryzyka i strategii zarządzania ryzykiem opracowanej w ramach funkcji wykonawczej ds. ryzyka. W związku z tym, system o dużym wpływie miałby uszeregowany pod względem ważności wykaz luk tego systemu, podobnie jak systemy o umiarkowanym wpływie i niewielkim wpływie.

DECYZJE AUTORYZACYJNE

Decyzje autoryzacyjne są podejmowane w oparciu o zawartość pakietu autoryzacyjnego. Istnieją cztery rodzaje decyzji autoryzacyjnych, które mogą być wydane przez osoby autoryzujące:

- Upoważnienie do działania;
- Autoryzacja zabezpieczeń wspólnych;

[127] Ogólnie rzecz biorąc, narażenie na ryzyko jest to stopień, w jakim organizacja jest zagrożona potencjalnym negatywnym wpływem na jej działalność i aktywa, osoby fizyczne, inne organizacje lub Państwo.

- Zezwolenie na użytkowanie; oraz
- Odmowa autoryzacji.

UPOWAŻNIENIE DO DZIAŁANIA

Jeżeli po zapoznaniu się z pakietem autoryzacyjnym, osoba autoryzująca stwierdzi, że ryzyko dla działalności organizacji, majątku organizacyjnego, osób, innych organizacji i Państwa jest dopuszczalne, wydawane jest *upoważnienie do działania (ang. Authorization to operate)* systemu informatycznego. System jest upoważniony do działania na czas określony, zgodnie z warunkami określonymi przez osobę autoryzującą. *Data wygaśnięcia* upoważnienia jest ustalana przez osobę autoryzującą, jako warunek upoważnienia. Data wygaśnięcia autoryzacji może być w każdej chwili zmieniona przez osobę autoryzującą w celu uwzględnienia zwiększonego poziomu obaw dotyczących bezpieczeństwa i ochrony prywatności systemu. Na przykład, osoba autoryzująca może zdecydować się na upoważnienie systemu do działania tylko na krótki okres czasu, jeżeli konieczne jest przetestowanie systemu w środowisku operacyjnym, zanim wszystkie zabezpieczenia zostaną w pełni wprowadzone (tzn. upoważnienie do działania jest ograniczone do czasu potrzebnego do ukończenia testowania obiektu).[128] Osoba autoryzująca może zdecydować się na uwzględnienie ograniczeń eksploatacyjnych, takich jak ograniczenie logicznego i fizycznego dostępu do minimalnej liczby użytkowników; ograniczenie okresów użytkowania systemu; zastosowanie rozszerzonego lub zwiększonego rejestru audytów, skanowania i monitorowania; lub ograniczenie funkcjonalności systemu do funkcji, które wymagają bieżącego testowania. Osoba autoryzująca bierze pod uwagę wyniki oceny zabezpieczeń, które są w pełni lub częściowo wdrożone, ponieważ jeżeli system jest gotowy do przetestowania w warunkach rzeczywistych, wiele z tych zabezpieczeń powinno już być wdrożonych. Jeśli system jest w trakcie autoryzacji, określona jest częstotliwość autoryzacji

[128] Dawniej określany, jako tymczasowe upoważnienie do przeprowadzania testów.

w czasie. Dodatkowo, może wystąpić niekorzystne zdarzenie, które spowoduje konieczność przeglądu upoważnienie na prowadzenie działania.[129]

AUTORYZACJA ZABEZPIECZEŃ WSPÓLNYCH

Autoryzacja zabezpieczeń wspólnych jest podobna do upoważnienia do działania systemu. Jeśli osoba autoryzująca, po zapoznaniu się z pakietem autoryzacyjnym przedłożonym przez dostawcę zabezpieczeń wspólnych, stwierdzi, że ryzyko dla operacji organizacyjnych i aktywów, osób, innych organizacji i Państwa jest akceptowalne, wydawana jest autoryzacja dotycząca zabezpieczeń wspólnych. Obowiązkiem dostawców zabezpieczeń wspólnych jest wskazanie, że zabezpieczenia wspólne wybrane przez organizację zostały wdrożone, ocenione i autoryzowane oraz są dostępne do dziedziczenia przez systemy organizacyjne. Dostawcy zabezpieczeń wspólnych są również odpowiedzialni za zapewnienie, że właściciele systemów dziedziczących zabezpieczenia mają dostęp do odpowiedniej dokumentacji i narzędzi.

Zabezpieczenia wspólne są autoryzowane na określony okres czasu zgodnie z warunkami ustanowionymi przez osobę autoryzującą i organizację. *Data wygaśnięcia autoryzacji* jest ustalana przez osobę autoryzującą, jako warunek wstępnej autoryzacji zabezpieczeń wspólnych. Data wygaśnięcia autoryzacji może być zmieniona w dowolnym momencie w celu odzwierciedlenia poziomu obaw osoby autoryzującej dotyczących bezpieczeństwa i prywatności zabezpieczeń wspólnych, które są dostępne do dziedziczenia. Jeśli te zabezpieczenia są przeprowadzane w ramach autoryzacji bieżącej, określa się częstotliwość autoryzacji w zależności od czasu.

W ramach każdego rodzaju autoryzacji, niekorzystne zdarzenie może spowodować konieczność przeglądu autoryzacji zabezpieczeń wspólnych. Zabezpieczenia wspólne, które są zaimplementowane w systemie, nie wymagają oddzielnej autoryzacji, ponieważ

[129] Dodatkowe informacje na temat wyzwalaczy sterowanych zdarzeniami znajdują się poniżej.

zabezpieczenia te uzyskują upoważnienie (autoryzację) do działania jako część upoważnienia do działania systemu.[130]

ZEZWOLENIE NA UŻYTKOWANIE

Zezwolenie na użytkowanie (ang. Authorization to use) jest stosowane, gdy organizacja (zwana dalej "organizacją konsumencką") zdecyduje się zaakceptować informacje zawarte w istniejącym pakiecie autoryzacyjnym, opracowanym przez inną organizację, odnoszącym się do systemu informatycznego, który jest upoważniony do działania przez uprawnioną jednostkę (zwaną dalej "dostawcą usług").[131] Zezwolenie na użytkowanie systemu jest mechanizmem promującym wzajemność dla systemów podlegających różnym osobom autoryzującym. Zezwolenie na użytkowanie jest wydawane przez osobę autoryzującą z organizacji klienta w miejsce upoważnienia do działania. Osoba wydająca zezwolenie na użytkowanie systemu ma taki sam poziom odpowiedzialności i uprawnień w zakresie zarządzania ryzykiem jak osoba autoryzująca wydająca upoważnienie do działania lub dokonująca autoryzacji zabezpieczeń wspólnych.[132]

Akceptacja informacji zawartych w pakiecie autoryzacyjnym dostawcy usług jest formą wzajemności i opiera się na potrzebie korzystania ze wspólnych systemów, usług lub aplikacji. Organizacja konsumencka może wydać zezwolenie na użytkowanie tylko wtedy,

[130] W pewnych sytuacjach właściciele systemów mogą zdecydować się na dziedziczenie zabezpieczeń po innych systemach organizacyjnych, które mogą nie być oficjalnie wyznaczone, jako zabezpieczenia wspólne. Właściciele systemów, którzy dziedziczą zabezpieczenia od dostawców nieautoryzowanych zabezpieczeń wspólnych, zapewniają, że systemy stosujące takie zabezpieczenia posiadają ważne uprawnienia do działania. Osoba autoryzująca system dziedziczący zabezpieczenia, jest również powiadamiana o dziedziczonych zabezpieczeniach.

[131] Termin "dostawca usług" odnosi się do podmiotu, która dostarcza współdzielony system, usługę lub aplikację i/lub posiada i utrzymuje pakiet autoryzacyjny (tzn. Udzieliła upoważnienia do działania współdzielonego systemu, usługi lub aplikacji). Współdzielony system, usługa lub aplikacja nie może być własnością organizacji, która jest właścicielem pakietu autoryzacyjnego, na przykład w sytuacji, gdy współdzielony system, usługa lub aplikacja jest dostarczana przez zewnętrznego dostawcę.

[132] Decyzje oparte na ryzyku związane z wyborem zabezpieczeń i dostosowaniem zabezpieczeń bazowych przez organizacje dostarczające chmurę lub współdzielone systemy, usługi lub aplikacje, powinny uwzględniać potrzeby ochrony organizacji klientów, które mogą korzystać z tej chmury lub systemów, usług lub aplikacji współdzielonych. W związku z tym organizacje udostępniające chmurę lub współdzielone systemy, usługi lub aplikacje powinny rozważyć wspólne ryzyko związane z działaniem w tego rodzaju środowiskach.

gdy ważne upoważnienie do działania zostało wydane przez dostawcę usług). Upoważnienie do działania wydane przez dostawcę usług jest oświadczeniem o akceptacji ryzyka dla systemu, usługi lub aplikacji, która jest dostarczana. Zezwolenie na użytkowanie wydane przez organizację konsumencką jest oświadczeniem o akceptacji ryzyka przy korzystaniu z systemu, usługi lub aplikacji w odniesieniu do informacji klienta. Zezwolenie na użytkowanie systemu daje możliwość znacznych oszczędności kosztów i pozwala uniknąć potencjalnie kosztownego i czasochłonnego procesu autoryzacji przez organizację konsumencką.

Zezwolenie na użytkowanie wymaga od organizacji konsumenckiej przejrzenia pakietu autoryzacyjnego dostarczonego przez dostawcę usług, jako fundamentalnej podstawy do określenia ryzyka.[133] Dokonując przeglądu pakietu autoryzacyjnego, organizacja konsumencka bierze pod uwagę różne czynniki ryzyka, takie jak czas, jaki upłynął od momentu uzyskania wyników autoryzacji; środowisko działania (jeśli różni się od środowiska odzwierciedlonego w pakiecie autoryzacyjnym); poziom wpływu informacji, które mają być przetwarzane, przechowywane lub przekazywane; oraz ogólną tolerancję na ryzyko organizacji klienta. Jeżeli organizacja konsumencka planuje zintegrować współdzielony system, aplikacje lub usługi z jednym lub większą liczbą swoich systemów, organizacja konsumencka bierze pod uwagę związane z tym ryzyko.

Jeżeli organizacja konsumencka stwierdzi, że w pakiecie autoryzacyjnym usługodawcy nie ma wystarczającej ilości informacji lub istnieją niewystarczające środki bezpieczeństwa w celu ustalenia dopuszczalnego poziomu ryzyka, organizacja może negocjować z dostawcą usług i zażądać dodatkowych zabezpieczeń i przedstawienia informacji dotyczących środków bezpieczeństwa, prywatności lub łańcucha dostaw. Prośby o dodatkowe zabezpieczenia mogą obejmować na przykład uzupełnienie zabezpieczeń w celu zmniejszenia ryzyka,

[133] Udostępnienie pakietu autoryzacyjnego (łącznie z planami bezpieczeństwa i ochrony prywatności, raportami z oceny bezpieczeństwa i ochrony prywatności, planami i etapami działań oraz dokumentem decyzji autoryzacyjnej) odbywa się na warunkach uzgodnionych przez wszystkie strony (tj. Organizację konsumencką i organizację dostawcy usług).

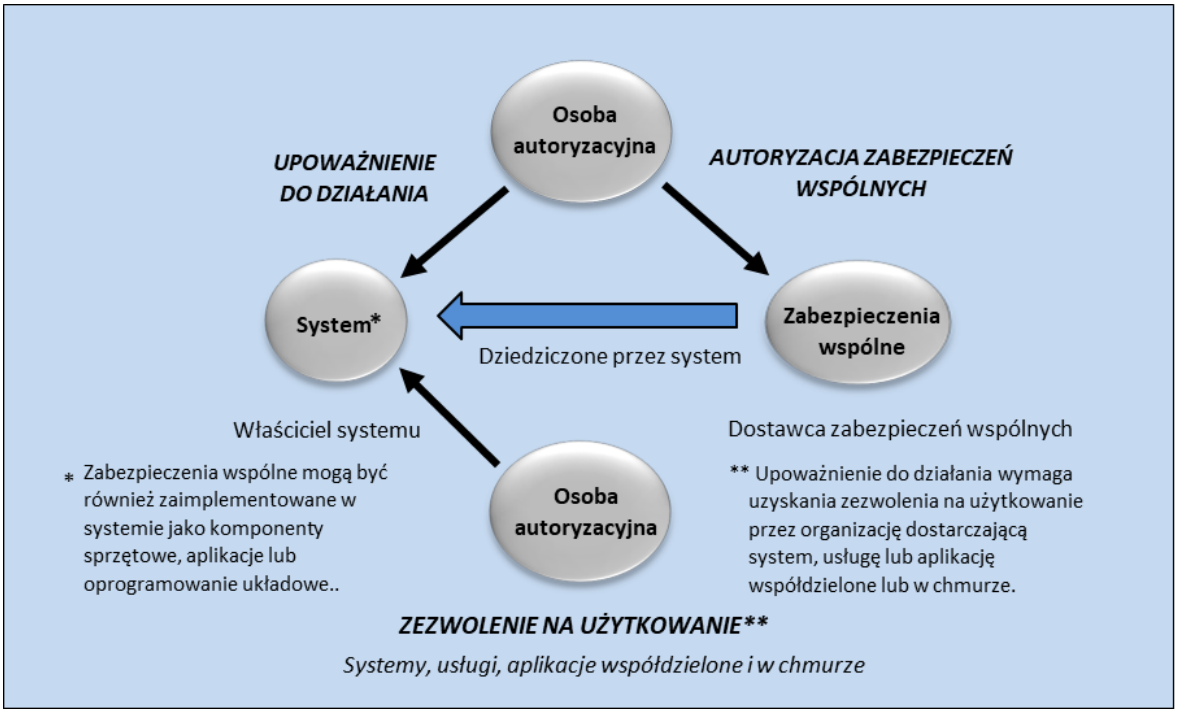
wdrożenie zabezpieczeń kompensacyjnych, przeprowadzenie dodatkowych lub bardziej rygorystycznych ocen lub ustanowienie ograniczeń w korzystaniu z systemu, aplikacji lub świadczonych usług. Żądania dotyczące dodatkowych informacji mogą obejmować na przykład informacje, które dostawca usług opracował lub uzyskał w trakcie użytkowania systemu, a które nie są odzwierciedlone w pakiecie autoryzacyjnym. Jeżeli dostawca usług nie zapewnia wymaganych zabezpieczeń, organizacja konsumencka może zdecydować się na wdrożenie dodatkowych zabezpieczeń w celu zmniejszenia ryzyka do akceptowalnego poziomu. Dodatkowe zabezpieczenia, wraz z wszelkimi innymi środkami bezpieczeństwa, za które organizacja konsumencka jest odpowiedzialna, są dokumentowane, wdrażane, oceniane, autoryzowane i monitorowane.

Z chwilą, gdy organizacja konsumencka akceptuje poziom bezpieczeństwa i ochrony prywatności współdzielonych lub w chmurze systemów, aplikacji lub usług (co odzwierciedla obecny pakiet autoryzacyjny), a ryzyko korzystania ze współdzielonego lub w chmurze systemu, aplikacji lub usługi zostało wystarczająco zmniejszone, organizacja konsumencka wydaje zezwolenie na użytkowanie, w którym jednoznacznie pojmuje i akceptuje ryzyko związane z bezpieczeństwem lub ochroną prywatności wynikające z korzystania ze współdzielonego systemu, aplikacji lub usługi. Ostatecznie, organizacja konsumencka jest odpowiedzialna za ryzyko, które może mieć wpływ na działalność i aktywa organizacji konsumenckiej, osoby fizyczne, inne organizacje lub Państwo.

Zezwolenie na użytkowanie nie wymaga daty wygaśnięcia, ale pozostaje w mocy, jeżeli organizacja konsumencka nadal akceptuje ryzyko związane z bezpieczeństwem i prywatnością podczas korzystania z udostępnionego lub w chmurze systemu, aplikacji lub usługi, a upoważnienie do działania wydane przez dostawcę usługi spełnia wymagania określone w przepisach i zasadach organizacyjnych. Obowiązkiem organizacji konsumenckiej jest zapewnienie, aby informacje z działań monitorujących prowadzonych przez dostawcę usług były udostępniane na bieżąco i aby dostawca usług powiadamiał organizację konsumencką o istotnych zmianach w systemie, aplikacji lub usłudze, które mogą wpływać na bezpieczeństwo i prywatność dostawcy. Jeśli jest to wymagane, zezwolenie na

użytkowanie może określać czasowe lub nawet uwarunkowane czasowo bodźce do przeglądu bezpieczeństwa i prywatności systemu, usługi lub aplikacji używanej przez organizację konsumencką. Dostawca usług powiadamia organizację konsumencką o zaistnieniu istotnego zdarzenia, które zagraża lub negatywnie wpływa na informacje organizacji konsumenckiej.[134]

Rysunek F-1 ilustruje rodzaje decyzji autoryzacyjnych, które mogą być stosowane do systemów organizacyjnych i zabezpieczeń wspólnych oraz ról zarządzania ryzykiem w procesie autoryzacji.



Rysunek F-1: Rodzaje decyzji autoryzacyjnych

ODMOWA AUTORYZACJI

Jeżeli osoba autoryzująca, po zapoznaniu się z pakietem autoryzacyjnym, w tym z wszelkimi danymi dostarczonymi personel wyższego szczebla odpowiedzialny za zarządzanie ryzykiem

[134] Organizacja konsumencka może opracowywać protokoły ustaleń/porozumień, umowy lub inne rodzaje umów z dostawcą usług, aby pomóc w zapewnieniu, że informacje o pozycji bezpieczeństwa w dostarczonym systemie są odpowiednio udostępniane.

lub funkcja wykonawcza ds. ryzyka, stwierdzi, że ryzyko dla działań organizacyjnych, majątku organizacji, osób, innych organizacji i Państwa jest nie do przyjęcia i nie można podjąć natychmiastowych kroków w celu zmniejszenia ryzyka do akceptowalnego poziomu, autoryzacja nie jest udzielana. *Odmowa autoryzacji* oznacza, że system informatyczny nie jest upoważniony do działania i nie jest wprowadzany do użytku; zabezpieczenia wspólne nie są autoryzowane do wprowadzania do systemu lub, że dostarczony systemu nie jest autoryzowany do użytku przez organizację konsumencką. Jeśli system jest aktualnie używany, cała działalność zostaje wstrzymana. Nieotrzymanie autoryzacji oznacza, że istnieją znaczące braki w zabezpieczeniach.

Osoba autoryzująca lub wyznaczony pełnomocnik współpracuje z właścicielem systemu lub dostawcą zabezpieczeń wspólnych w celu dokonania przeglądu planu i etapów działania, aby zapewnić podjęcie kroków w celu usunięcia niedociągnięć. Szczególnym przypadkiem odmowy autoryzacji jest *unieważnienie autoryzacji*. Osoby autoryzujące mogą unieważnić wcześniejszą decyzję o autoryzacji w przypadku naruszenia prawa lub zasad organizacyjnych, dyrektyw, regulacji, standardów lub wytycznych; lub naruszenia warunków autoryzacji. Na przykład, podstawą do unieważnienia autoryzacji może być nieutrzymanie skutecznego programu ciągłego monitorowania.

INFORMACJE ZAWARTE W DECYZJI AUTORYZACYJNEJ

Decyzja o autoryzacji jest przekazywana przez osobę autoryzującą właścicielom systemu, dostawcom zabezpieczeń wspólnych i innym kluczowym osobom w organizacji. Decyzja autoryzacyjna zawiera następujące informacje:

- Decyzja o autoryzacji;
- Zasady i warunki autoryzacji;
- Częstotliwość czasowej autoryzacji lub data zakończenia autoryzacji;
- Zdarzenia, które mogą spowodować weryfikację decyzji o autoryzacji (jeśli taka istnieje); oraz

- W przypadku zabezpieczeń wspólnych, poziom wpływu obsługiwany przez te zabezpieczenia (określany zgodnie z [NSC 199]).

Decyzja o autoryzacji wskazuje, czy system jest upoważniony do działania, czy posiada upoważnienie do działania; lub czy zabezpieczenia wspólne są autoryzowane do przekazania właścicielom systemu i do dziedziczenia przez systemy organizacyjne. Zasady i warunki autoryzacji określają wszelkie ograniczenia lub restrykcje nałożone na działanie systemu, które muszą być przestrzegane przez właściciela systemu lub alternatywnie, ograniczenia lub restrykcje nałożone na wdrożenie zabezpieczeń wspólnych, które muszą być przestrzegane przez dostawcę zabezpieczeń wspólnych. Jeżeli system lub zabezpieczenia wspólne nie są objęte bieżącą autoryzacją, data ważności autoryzacji ustalona przez osobę autoryzującą wskazuje, kiedy autoryzacja wygasa i wymagana jest reautoryzacja. Dokument autoryzacyjny jest przekazywany wraz z oryginalnym pakietem autoryzacyjnym do właściciela systemu lub dostawcy zabezpieczeń wspólnych.[135]

Po otrzymaniu decyzji o autoryzacji i pakietu autoryzacyjnego, właściciel systemu i dostawca zabezpieczeń wspólnych potwierdzają, wdrażają i przestrzegają warunki autoryzacji. Właściciel systemu i dostawca zabezpieczeń wspólnych zachowują decyzję o autoryzacji i pakiet autoryzacyjny.[136] Organizacja zapewnia, że dokumenty autoryzacyjne są dostępne dla personelu organizacji na żądanie. Zawartość pakietów autoryzacyjnych, w tym wrażliwe informacje dotyczące podatności systemu, zagrożeń prywatności i niedociągnięć w zabezpieczeniach, są oznaczone i chronione zgodnie z przepisami i zasadami organizacyjnymi. Informacje o decyzjach dotyczących autoryzacji są przechowywane zgodnie z polityką przechowywania dokumentacji organizacji. Osoba autoryzująca weryfikuje na bieżąco, czy warunki ustanowione, jako część autoryzacji są przestrzegane przez właściciela systemu i dostawcę zabezpieczeń wspólnych.

[135] W celu zapewnienia autentyczności dokumenty decyzji autoryzacyjnej mogą być podpisane cyfrowo.
[136] Organizacje mogą zdecydować się na zastosowanie zautomatyzowanych narzędzi wspomagających opracowywanie, dystrybucję i archiwizację informacji dotyczących zarządzania ryzykiem w celu uwzględnienia artefaktów związanych z procesem autoryzacji.

DECYZJA ZEZWALAJĄCA NA UŻYTKOWANIE

Zezwolenie na użytkowanie jest uproszczoną wersją upoważnienia do działania i zawiera:

- Oświadczenie o akceptacji ryzyka; oraz
- Wyzwalacze czasowe lub zdarzeniowe powodujące przegląd pozycji w zakresie bezpieczeństwa i ochrony prywatności współdzielonej chmury lub systemu, aplikacji lub usługi (jeśli istnieją) dostawcy usług.

Zezwolenie na użytkowanie jest wydawane przez osobę autoryzującą z organizacji konsumenckiej w miejsce upoważnienia do działania. Osoba autoryzująca wydająca zezwolenie na użytkowanie ma taki sam poziom odpowiedzialności i uprawnień w zakresie zarządzania ryzykiem, jak osoba autoryzująca wydająca upoważnienie do działania lub autoryzację zabezpieczeń wspólnych.

Oświadczenie o akceptacji ryzyka wskazuje na jednoznaczną akceptację ryzyka związanego z bezpieczeństwem i prywatnością wynikającą z korzystania ze współdzielonego systemu, usługi lub aplikacji w odniesieniu do informacji organizacji konsumenckiej przetwarzanych, przechowywanych lub przekazywanych przez lub za pośrednictwem współdzielonego systemu, usługi lub aplikacji w chmurze.

AUTORYZACJA BIEŻĄCA

Strategie ciągłego monitorowania [137] promują skuteczne i wydajne zarządzanie ryzykiem prowadzone na bieżąco. Zarządzanie ryzykiem może odbywać się w *czasie zbliżonym do rzeczywistego* dzięki zastosowaniu narzędzi, technik i procedur automatyzacji bieżącego monitorowania zabezpieczeń i zmian w systemach i środowiskach, w których systemy te działają. Ciągły monitoring oparty na wymaganiach osoby autoryzującej, dostarcza informacji niezbędnych do określenia pozycji systemu w zakresie bezpieczeństwa i ochrony

[137] [SP 800-137] zawiera dodatkowe wskazówki dotyczące ciągłego monitorowania bezpieczeństwa i informacji. Wskazówki dotyczące stałego monitorowania prywatności zostaną przedstawione w przyszłych publikacjach.

prywatności[138] oraz podkreśla zagrożenia dla operacji organizacyjnych i majątku, osób, innych organizacji i Państwa. Docelowo należy prowadzić stały monitoring i informować osobę autoryzującą o decyzji, czy zezwolić na dalsze funkcjonowanie systemu, czy też na dalsze stosowanie zabezpieczeń wspólnych odziedziczonych po systemach organizacyjnych.

Ciągłe monitorowanie pomaga osiągnąć stan *autoryzacji bieżącej, w* którym osoba autoryzująca posiada wystarczającą wiedzę na temat aktualnej pozycji systemu w zakresie bezpieczeństwa i ochrony prywatności, aby określić, czy dalsze działania są dopuszczalne na podstawie bieżących ustaleń dotyczących ryzyka, a jeśli nie, to jakie kroki w zakresie RMF należy ponownie przeanalizować, aby skutecznie zareagować na dodatkowe ryzyko. Ponowne autoryzacje są zbędne w sytuacjach, w których program stałego monitorowania dostarcza osobom autoryzującym informacje niezbędne do zarządzania ryzykiem wynikającym ze zmian w systemie lub środowisku, w którym system działa. W przypadku, gdy wymagana jest reautoryzacja, organizacje maksymalizują wykorzystanie raportów o statusie oraz istotnych informacji o bezpieczeństwie i prywatności systemu, które są tworzone podczas procesu ciągłego monitorowania w celu poprawy jego efektywności.

Kiedy system lub zabezpieczenia wspólne są w trakcie autoryzacji, system lub zabezpieczenia wspólne mogą być autoryzowane w oparciu o czas i/lub zdarzenia, wykorzystując informacje dotyczące bezpieczeństwa i ochrony prywatności generowane przez program ciągłego monitorowania. System i zabezpieczenia wspólne są autoryzowane na podstawie czasowej autoryzacji, zgodnie z częstotliwością określoną, jako część strategii ciągłego monitorowania na poziomie organizacji i systemu. System i zabezpieczenia wspólne są autoryzowane na podstawie zdarzeń do czasu wystąpienia zdefiniowanych przez organizację zdarzeń wyzwalających. Niezależnie od tego, czy autoryzacja jest czasowa czy zdarzeniowa, osoba

[138] W celu zwiększenia wydajności, strategie ciągłego monitorowania bezpieczeństwa informacji (ang. Information security continuous monitoring - ISCM) i ciągłego monitorowania prywatności (ang. Privacy continuous monitoring - PCM) mogą być skonsolidowane w jedną ujednoliconą strategię ciągłego monitorowania. Podobnie, programy ISCM i PCM mogą być również skonsolidowane w jeden jednolity program ciągłego monitorowania.

autoryzująca potwierdza bieżącą akceptację zidentyfikowanego ryzyka. Organizacja określa poziom formalności wymagany do takiego potwierdzenia przez osobę autoryzującą.

WARUNKI REALIZACJI AUTORYZACJI BIEŻĄCEJ

Kiedy RMF został skutecznie zastosowany w całej organizacji, a organizacja wdrożyła stosowny program ciągłego monitorowania, systemy mogą przejść od statycznego, okresowego procesu autoryzacji do dynamicznego, niemalże bieżącego procesu autoryzacji w czasie rzeczywistym. Warunkiem przeprowadzenia tego jest spełnienie następujących warunków:

- System lub zabezpieczenia wspólne rozpatrywane do celów autoryzacji bieżącej uzyskały wstępne zezwolenie w oparciu o pełny zerowy przegląd systemu lub zabezpieczeń wspólnych.[139]
- W organizacji funkcjonuje program ciągłego monitorowania, który monitoruje wdrożone zabezpieczenia z odpowiednim stopniem rygoru i z wymaganą częstotliwością określoną przez organizację zgodnie ze strategią ciągłego monitorowania oraz standardami i wytycznymi.[140]

Organizacja ustanawia i wdraża proces mający na celu określenie, czy oba te warunki są spełnione, a system lub zabezpieczenia wspólne przechodzą do bieżącej autoryzacji. Proces ten obejmuje potwierdzenie przez osobę autoryzującą, że system lub zabezpieczenie wspólne są obecnie zarządzane przez bieżący proces autoryzacji i przyjęcie odpowiedzialności za wykonanie wszystkich czynności związanych z tym procesem.

[139] Właściciele systemów i osoby autoryzujące korzystają z informacji dotyczących bezpieczeństwa i ochrony prywatności odziedziczonych po ocenach przeprowadzonych przez dostawców zabezpieczeń wspólnych.
[140] [NSC 800-53] i [NSC 800-53A] zawierają wytyczne dotyczące odpowiedniego stopnia rygoru w zakresie oceny i monitorowania bezpieczeństwa. Przyszłe publikacje będą dotyczyły oceny ochrony prywatności.

Przejście do bieżącej autoryzacji jest dokumentowane przez osobę autoryzującą poprzez wydanie nowej decyzji autoryzacyjnej.[141] Informacje dotyczące bezpieczeństwa i ochrony prywatności generowane w ramach procesu ciągłego monitorowania są przekazywane terminowo osobom autoryzującym i innym przedstawicielom organizacji za pomocą narzędzi zarządzania bezpieczeństwem i prywatnością oraz narzędzi sprawozdawczych. Narzędzia te ułatwiają podejmowanie decyzji opartych na analizie ryzyka w odniesieniu do bieżącej autoryzacji systemów i zabezpieczeń wspólnych.

WYMAGANIA DOTYCZĄCE GENEROWANIA, GROMADZENIA I NIEZALEŻNOŚCI INFORMACJI

W celu wsparcia bieżącej autoryzacji, informacje dotyczące środków bezpieczeństwa i ochrony prywatności są generowane i gromadzone z częstotliwością określoną w strategii ciągłego monitorowania organizacji. Informacje dotyczące bezpieczeństwa i prywatności mogą być gromadzone przy użyciu zautomatyzowanych narzędzi lub innych metod oceny, w zależności od rodzaju i celu zabezpieczeń oraz pożądanego rygoru oceny. Zautomatyzowane narzędzia mogą nie generować informacji dotyczących bezpieczeństwa i prywatności, które są wystarczające, aby pomóc osobie autoryzującej w określeniu ryzyka. Narzędzia zautomatyzowane mogą nie zapewniać wystarczającego wsparcia z różnych powodów (np. narzędzia nie generują informacji dla każdego zabezpieczenia lub każdej części zabezpieczenia; konieczne jest dodatkowe poświadczenie; lub narzędzia nie generują informacji na temat konkretnych technologii lub platform). W takich przypadkach ręczna ocena zabezpieczeń jest przeprowadzana z częstotliwością określoną przez organizację w celu uzupełnienia wszelkich luk w zautomatyzowanym generowaniu informacji dotyczących bezpieczeństwa i ochrony prywatności. Ręcznie wygenerowane wyniki oceny są przekazywane jednostce autoryzacyjnej w sposób uznany przez organizację za właściwy.

[141] Przed przejściem do autoryzacji bieżącej, organizacje posiadają decyzje autoryzacyjne, które zawierają datę zakończenia autoryzacji. Wymagając nowej decyzji autoryzacyjnej, wyraźnie stwierdza się, że system lub zabezpieczenia wspólne nie obowiązują od daty zakończenia okresu ważności określonej w pierwotnym dokumencie autoryzacyjnym, ponieważ system i zabezpieczenia wspólne są obecnie w trakcie autoryzacji.

W celu wsparcia bieżących autoryzacji systemów o umiarkowanym i dużym wpływie, informacje dotyczące bezpieczeństwa i ochrony prywatności przekazywane jednostce autoryzacyjnej, generowane ręcznie lub w sposób zautomatyzowany, są wytwarzane i analizowane przez podmiot, który spełnia wymogi niezależności ustanowione przez organizację. SAOP jest odpowiedzialny za ocenę zabezpieczeń prywatności i dostarczanie informacji o prywatności osobie autoryzującej. Według uznania organizacji, zabezpieczenia prywatności mogą być oceniane przez niezależną osobę oceniającą. Niezależny podmiot oceniający jest bezstronny i wolny od wszelkich postrzeganych lub rzeczywistych konfliktów interesów dotyczących rozwoju, wdrażania, oceny, działania lub zarządzania systemami organizacyjnymi i zabezpieczeniami wspólnymi, które są monitorowane.

CZĘSTOTLIWOŚĆ PRZEPROWADZANIA AUTORYZACJI BIEŻĄCEJ

[NSC 800-53] - kategoria CA-6, Autoryzacja bezpieczeństwa, część C - określa, że autoryzacja systemu i wszelkich zabezpieczeń wspólnych dziedziczonych przez system są aktualizowane z częstotliwością ustaloną przez organizację. Ta część zabezpieczeń wzmacnia koncepcję ciągłej autoryzacji. Zgodnie z kategorią CA-6 (wraz z oceną bezpieczeństwa i prywatności oraz ustaleniami dotyczącymi częstotliwości monitorowania ustanowionymi w ramach strategii ciągłego monitorowania), organizacje określają częstotliwość, z jaką osoby autoryzujące dokonują przeglądu informacji dotyczących bezpieczeństwa i ochrony prywatności za pomocą narzędzi zarządzania bezpieczeństwem i prywatnością oraz raportowania lub procesów ręcznych.[142] Informacje pochodzące z narzędzi sprawozdawczych lub procesów ręcznych, przekazywane w czasie zbliżonym do rzeczywistego, są wykorzystywane do określenia, czy misja lub ryzyko biznesowe związane

[142] Bieżąca autoryzacja i bieżąca ocena to różne pojęcia, ale ściśle ze sobą powiązane. Aby zastosować podejście polegające na stałym upoważnieniu (co oznacza stałe rozumienie i akceptację ryzyka), organizacje muszą posiadać proces stałego monitorowania na poziomie organizacji i systemu, aby na bieżąco oceniać wdrożone mechanizmy kontrolne. Ustalenia lub wyniki procesu ciągłego monitorowania dostarczają informacji osobom autoryzującym do wspierania podejmowania decyzji w oparciu o ryzyko w czasie zbliżonym do rzeczywistego.

z obsługą systemu lub zapewnieniem zabezpieczeń wspólnych są nadal dopuszczalne. [SP 800-137] zawiera kryteria określania częstotliwości oceny i monitorowania.

W ramach autoryzacji bieżącej, autoryzacyjna uwarunkowana czasem odnosi się do częstotliwości, z jaką organizacja określa, że osoby autoryzujące mają przeglądać informacje dotyczące bezpieczeństwa i ochrony prywatności oraz autoryzować system (lub zabezpieczenia wspólne) do dalszego działania w sposób opisany powyżej. Czasowe uruchamianie autoryzacji może być oparte na różnych zdefiniowanych przez organizację czynnikach, w tym na poziomie wpływu systemu. W przypadku wystąpienia wyzwolenia czasowego, osoby autoryzujące dokonują przeglądu informacji dotyczących bezpieczeństwa i ochrony prywatności systemów, za które są odpowiedzialni i rozliczani, w celu określenia bieżącej misji organizacji lub ryzyka biznesowego, akceptowalności takiego ryzyka zgodnie z tolerancją ryzyka organizacyjnego oraz tego, czy zgoda na kontynuację działania jest uzasadniona. Proces ciągłego monitorowania organizacji, wspierany przez narzędzia zarządzania bezpieczeństwem i prywatnością oraz narzędzia raportowania, zapewnia odpowiednią funkcjonalność do powiadomienia osoby autoryzującej o zbliżającym się czasie przeglądu informacji dotyczących bezpieczeństwa i ochrony prywatności w celu wsparcia bieżącej autoryzacji.

W przeciwieństwie do wyzwalaczy czasowych, *wyzwalacze zdarzeniowe* wymagają natychmiastowego przeglądu informacji dotyczących bezpieczeństwa i ochrony prywatności przez osobę autoryzującą. Organizacje mogą definiować *wyzwalacze wywołane zdarzeniami* (tj. wskaźniki lub podpowiedzi, które powodują, że organizacja reaguje w określony sposób) w celu autoryzacji bieżącej i reautoryzacji. W przypadku wystąpienia wyzwolenia wywołanego przez zdarzenie w ramach autoryzacji bieżącej, osoba autoryzująca jest powiadamiana przez personel organizacji (np. SAISO, SAOP, właściciela systemu, dostawcę zabezpieczeń wspólnych lub SSPO) lub za pomocą zautomatyzowanych narzędzi, które zdefiniowały zdarzenia wyzwalające wymagające natychmiastowego przeglądu systemu lub zabezpieczeń wspólnych. Osoba autoryzująca może również niezależnie stwierdzić, że konieczny jest natychmiastowy przegląd. Autoryzacja wywołana zdarzeniem jest

przeprowadzana oprócz weryfikacji czasowej zdefiniowanej w organizacyjnej strategii ciągłego monitorowania i ma miejsce podczas bieżącej autoryzacji, gdy ryzyko szczątkowe pozostaje w dopuszczalnych granicach tolerancji ryzyka organizacyjnego.[143]

PRZEJŚCIE Z AUTORYZACJI STATYCZNEJ DO AUTORYZACJI BIEŻĄCEJ

Celem ciągłego monitorowania jest monitorowanie zabezpieczeń z częstotliwością wystarczającą do zapewnienia osobom autoryzującym informacji niezbędnych do podejmowania skutecznych, opartych na ryzyku decyzji, zarówno w sposób automatyczny, jak i ręczny.[144] Jeżeli jednak znaczna część monitorowania nie jest realizowana w sposób zautomatyzowany, przejście od obecnego statycznego podejścia do autoryzacji do efektywnego i skutecznego podejścia do autoryzacji bieżącej nie będzie wykonalne ani praktyczne. Etapowe podejście do generowania informacji dotyczących bezpieczeństwa i ochrony prywatności może być konieczne w okresie przejściowym, w miarę jak narzędzia zautomatyzowane stają się dostępne, a większa liczba zabezpieczeń jest monitorowana za pomocą technik zautomatyzowanych. Organizacje mogą zacząć od generowania informacji o bezpieczeństwie i prywatności z wykorzystaniem zautomatyzowanych narzędzi i uzupełnić luki poprzez wygenerowanie dodatkowych informacji z ręcznych ocen. W miarę dodawania dodatkowych zautomatyzowanych funkcji monitorowania, procesy mogą być dostosowywane.

Przejście od statycznego procesu autoryzacji do dynamicznego, ciągłego procesu autoryzacji wymaga znacznego przemyślenia i planowania. Jedną z metodologii, którą organizacje mogą rozważyć, jest stopniowe podejście do migracji w oparciu o kategoryzację bezpieczeństwa

[143] Natychmiastowe przeglądy zainicjowane przez określone zdarzenia wyzwalające mogą mieć miejsce jednocześnie (tj. W połączeniu) z działaniami monitorującymi sterowanymi w czasie, w oparciu o częstotliwość monitorowania ustaloną przez organizację i sposób, w jaki przeglądy są zorganizowane w organizacji. Ta sama struktura sprawozdawczości może być stosowana w przypadku przeglądów inicjowanych zdarzeniami i przeglądów inicjowanych w czasie w celu osiągnięcia efektywności.

[144] Ciągłe monitorowanie ochrony prywatności oznacza utrzymywanie stałej świadomości zagrożeń dla prywatności oraz ocenę zabezpieczeń prywatności z częstotliwością wystarczającą do zapewnienia zgodności z obowiązującymi wymogami w zakresie ochrony prywatności oraz do zarządzania zagrożeniami dla prywatności.

systemu. Ponieważ poziomy tolerancji ryzyka dla systemów o niskim poziomie wpływu mogą być większe niż dla systemów o umiarkowanym lub dużym wpływie, wdrożenie stałego monitorowania i bieżącej autoryzacji dla systemów o niskim poziomie wpływu może ułatwić przejście ze statycznego do dynamicznego procesu autoryzacji. Etapowe podejście rozpoczynające się od systemów o niskim poziomie wpływu pozwala organizacjom na wykorzystanie zdobytych doświadczeń, ponieważ w przypadku systemów o umiarkowanym i wysokim wpływie wdrażane są procesy ciągłego monitorowania i bieżącej autoryzacji. Wykorzystanie zdobytych doświadczeń ułatwia konsekwentne przechodzenie od najniższego do najwyższego poziomu wpływu na systemy w organizacji, w ramach ciągłego monitorowania i bieżącego procesu autoryzacji. Organizacje mogą również rozważyć zastosowanie podejścia stopniowego wdrażania poprzez podział systemów na podsystemy lub elementy systemu, a następnie przechodzenie tych podsystemów lub elementów systemu do autoryzacji bieżącej jednego segmentu po kolei, aż do momentu, gdy cały system będzie gotowy do pełnego przejścia (w tym czasie osoba autoryzująca uznaje, że system jest obecnie zarządzany przez trwający proces autoryzacji).

REAUTORYZACJA

Reautoryzacja odbywa się według uznania osoby autoryzującej zgodnie z przepisami i zasadami organizacyjnymi.[145] W przypadku konieczności przeprowadzenia reautoryzacji, organizacje maksymalizują wykorzystanie informacji o ryzyku związanym z bezpieczeństwem i prywatnością, które powstają w ramach aktualnie prowadzonych procesów ciągłego monitorowania. Działania reautoryzacji, jeśli są inicjowane, mogą być czasowe lub zdarzeniowe. Reautoryzację czasową przeprowadza się po osiągnięciu daty zakończenia autoryzacji (jeśli została ona określona). Jeżeli system jest w trakcie autoryzacji bieżącej,[146] to czasowa autoryzacja może nie być konieczna. Jeśli jednak program ciągłego

[145] Decyzje o formalnym rozpoczęciu ponownej autoryzacji obejmują wkład SAISO, SAOP, oraz SAORM lub RM.
[146] Podejście oparte na autoryzacji bieżącej wymaga wprowadzenia programu stałego monitorowania wszystkich wdrożonych środków bezpieczeństwa z częstotliwością określoną w strategii stałego monitorowania.

monitorowania nie jest wystarczająco wszechstronny, aby w pełni wspierać autoryzację bieżącą, to maksymalny okres autoryzacji może być określony przez osobę autoryzującą. Daty zakończenia autoryzacji zależą od polityki organizacyjnej oraz od wymagań osób autoryzujących.

W przypadku wystąpienia zdarzenia powodującego ryzyko przekraczające dopuszczalną tolerancję ryzyka organizacyjnego, może być konieczne przeprowadzenie reautoryzacji w ramach autoryzacji bieżącej. Reautoryzacja może być zagwarantowana, na przykład w przypadku naruszenia/zdarzenia, awarii lub istotnych problemów z programem stałego monitorowania. Reautoryzacja może wymagać przeglądu i zmian w strategii ciągłego monitorowania, co z kolei może mieć wpływ na autoryzację bieżącą.

W celu oceny bezpieczeństwa i prywatności związanej z ponowną autoryzacją, organizacje wykorzystują informacje dotyczące bezpieczeństwa i ochrony prywatności generowane przez program ciągłego monitorowania i wypełniają luki wykorzystując ocenę ręczną. Organizacje mogą uzupełniać informacje o ocenach generowanych automatycznie o informacje generowane ręcznie w sytuacjach, w których wymagany jest zwiększony poziom pewności. Jeżeli oceny środków bezpieczeństwa przeprowadzane są przez wykwalifikowany personel podmiot oceniający o niezbędnej niezależności, wykorzystują odpowiednie standardy i wytyczne w zakresie bezpieczeństwa i są oparte na potrzebach osób autoryzujących, wyniki oceny mogą być zastosowane do reautoryzacji.[147]

Za ocenę zabezpieczeń prywatności odpowiedzialny jest SAOP, a wyniki tej oceny mogą być stosowane łącznie do reautoryzacji. Niezależne podmioty oceniające zabezpieczenia mogą oceniać zabezpieczenia prywatności według uznania organizacji SAOP zatwierdza pakiety autoryzacyjne dla systemów informatycznych, które przetwarzają dane osobowe przed podjęciem decyzji o reautoryzacji. Działania związane z ponowną autoryzacją mogą być tak nieskomplikowane, jak aktualizacja planów bezpieczeństwa i ochrony prywatności, raportów

[147] [NSC 800-53A] opisuje specyficzne warunki, w których informacje z zakresu bezpieczeństwa mogą być ponownie wykorzystane do obsługi działań autoryzacyjnych.

z oceny bezpieczeństwa i ochrony prywatności oraz planów i etapów działania koncentrujących się wyłącznie na konkretnych problemach lub bieżących kwestiach, lub tak kompleksowe, jak autoryzacja wstępna.

Osoba autoryzująca podpisuje zaktualizowany dokument decyzji autoryzacyjnej w oparciu o aktualne określenie ryzyka i akceptację ryzyka dla działalności i majątku organizacji, osób fizycznych, innych organizacji i Państwa. We wszystkich sytuacjach, w których istnieje decyzja o reautoryzacji systemu lub zabezpieczeń wspólnych dziedziczonych po systemach organizacyjnych, zachęca się do maksymalnego ponownego wykorzystania informacji o autoryzacji w celu zminimalizowania czasu i kosztów związanych z ponowną autoryzacją (zgodnie z polityką ponownego wykorzystania w organizacji).

WYZWALACZE WYWOŁYWANE PRZEZ ZDARZENIA I ZNACZĄCE ZMIANY

Organizacje definiują *wyzwalacze wywoływane zdarzeniami* (tj. wskaźniki lub podpowiedzi, które wywołują predefiniowaną reakcję organizacji) zarówno dla autoryzacji bieżącej, jak i autoryzacji ponownej. Zmiana wywołana przez zdarzenie to np.:

- Nowe zagrożenia, podatność na zagrożenia, ryzyko utraty prywatności lub wpływ na informację;
- Zwiększona liczba zarejestrowanych ustaleń lub niedoskonałości w programie ciągłego monitorowania;
- Nowe misje/wymagania biznesowe;
- Zmiana osoby autoryzującej;
- Znacząca zmiana w wynikach szacowania ryzyka;
- Istotne zmiany w systemie, zabezpieczeniach wspólnych lub środowisku pracy;
- Zmiany w łańcuchu dostaw wpływające na zagrożenia dla bezpieczeństwa lub ochrony prywatności systemów operacyjnych; lub
- Przekroczenie progów organizacyjnych.

W przypadku zmiany osoby autoryzującej, nowa osoba autoryzująca dokonuje przeglądu aktualnej decyzji autoryzacyjnej, pakietu autoryzacyjnego, wszelkich uaktualnionych dokumentów z bieżących działań monitorujących lub raportu ze zautomatyzowanych narzędzi zarządzania bezpieczeństwem/prywatnością i raportowania. Jeżeli nowa osoba autoryzująca uzna obecne ryzyko za dopuszczalne, podpisuje nowy lub zaktualizowany dokument decyzji autoryzacyjnej, formalnie przekazując odpowiedzialność za system lub zabezpieczenia wspólne. Czyniąc to, nowa osoba autoryzująca jednoznacznie akceptuje ryzyko dla operacji organizacyjnych i aktywów, osób, innych organizacji i Państwa. Jeżeli nowa osoba autoryzująca uzna, że obecne ryzyko jest nie do zaakceptowania, może zainicjować akcję autoryzacyjną (tj. autoryzację bieżącą lub autoryzację ponowną). Alternatywnie, nowa osoba autoryzująca może zamiast tego ustanowić nowe zasady i warunki kontynuowania pierwotnej autoryzacji, ale nie może przedłużać daty wygaśnięcia pierwotnej autoryzacji (jeśli nie jest to podczas autoryzacji bieżące).

Istotną zmianę definiuje się, jako zmianę, która może w istotny sposób wpłynąć na bezpieczeństwo lub prywatność systemu. Istotne zmiany w systemie, które mogą wywołać działanie autoryzacyjne wywołane zdarzeniem, mogą obejmować, ale nie ograniczają się do nich:

- Instalacja nowego lub zaktualizowanego systemu operacyjnego, komponentu oprogramowania pośredniczącego lub aplikacji;
- Modyfikacje portów systemowych, protokołów lub usług;
- Instalacja nowej lub zmodernizowanej platformy sprzętowej;
- Modyfikacje sposobu przetwarzania informacji, w tym informacji dotyczących ochrony danych osobowych;
- Modyfikacje modułów lub usług kryptograficznych;
- Zmiany w typach informacji przetwarzanych, przechowywanych lub przesyłanych przez system; lub

- Modyfikacje w zakresie środków bezpieczeństwa i ochrony prywatności.

Istotne zmiany w środowisku pracy, które mogą wywołać działanie autoryzacyjne wywołane zdarzeniem, to np.:

- Przeprowadzka do nowej siedziby;
- Dodanie nowych podstawowych misji lub funkcji biznesowych;
- Uzyskanie konkretnej i wiarygodnej informacji o zagrożeniu, że organizacja jest celem ataku ze strony źródła zagrożenia; lub
- Tworzenie nowych/modyfikowanych ustaw, dyrektyw, polityk lub rozporządzeń.

Wymienione powyżej przykłady zmian są istotne tylko wtedy, gdy stanowią one zmianę, która może mieć wpływ na bezpieczeństwo i prywatność systemu. Organizacje ustalają kryteria dotyczące tego, co stanowi istotną zmianę w oparciu o różne czynniki (np. misję i potrzeby biznesowe; informacje o zagrożeniach i podatnościach na zagrożenia; środowisko działania systemów; zagrożenia dla prywatności; oraz kategoryzację bezpieczeństwa).

Wyniki szacowania ryzyka lub wyniki analizy wpływu mogą być wykorzystane do określenia, czy zmiany w systemach lub zabezpieczeniach wspólnych są istotne i czy powodują podjęcie działań związanych z udzieleniem autoryzacji. W przypadku rozpoczęcia akcji autoryzacyjnej, organizacja koncentruje się wyłącznie na konkretnych zabezpieczeniach, których dotyczą zmiany i w miarę możliwości wykorzystuje ponownie wyniki poprzedniej oceny. Efektywny program monitorowania może znacząco zmniejszyć ogólne koszty i poziom wysiłku związanego z działaniami autoryzacyjnymi. Większość zmian w systemie lub jego środowisku pracy może być obsługiwana poprzez program ciągłego monitorowania i autoryzację bieżącą.

AUTORYZACJA TYPU I AUTORYZACJA OBIEKTU

Autoryzacja typu[148] jest oficjalną decyzją autoryzacyjną, która pozwala na opracowanie jednego pakietu autoryzacyjnego (tzn. wspólnego) dla pierwowzoru wersji systemu. Obejmuje to na przykład komponenty sprzętowe, programowe lub firmware, które są rozmieszczone w wielu lokalizacjach w celu wykorzystania w określonych środowiskach działania (np. wymagania dotyczące instalacji i konfiguracji systemu lub potrzeby w zakresie bezpieczeństwa operacyjnego i prywatności zapewniane przez organizację hostującą w danej lokalizacji). Autoryzacja typu jest właściwa, gdy system jest wdrażany w określonym środowisku i jest złożony z identycznych elementów architektury systemu, oprogramowania, identycznych typów informacji, identycznego funkcjonalnie sprzętu, informacji przetwarzanych w ten sam sposób, identycznych implementacji zabezpieczeń lub identycznych konfiguracji. Autoryzacja typu jest stosowana w połączeniu z autoryzacją zabezpieczeń specyficznych dla danej lokalizacji[149] lub z autoryzacją obiektu, jak opisano poniżej. Autoryzacja typu jest wydawana przez osobę autoryzacyjną odpowiedzialną za rozwój systemu[150] i stanowi upoważnienie do działania. W lokalizacji lub obiekcie, w którym system jest wdrażany, osoba autoryzująca, która jest odpowiedzialna za system w lokalizacji lub obiekcie, akceptuje ryzyko związane z wdrożeniem systemu i wydaje upoważnienie do działania. Upoważnienie do działania systemu wykorzystuje informacje zawarte w pakietach autoryzacyjnych dla pierwotnego systemu i zabezpieczeń wspólnych obiektu.

[148] Przykładowe autoryzacje typu obejmują: zezwolenie na użytkowanie sprzętu i oprogramowania dla standardowego systemu finansowego wdrożonego w wielu lokalizacjach; lub zezwolenie na użytkowanie wspólnej stacji roboczej lub środowiska operacyjnego (tj. Sprzętu, systemu operacyjnego i aplikacji) wdrożonych we wszystkich jednostkach operacyjnych w organizacji.

[149] Zabezpieczenia specyficzne dla danej lokalizacji są zazwyczaj wdrażane przez organizację, jako zabezpieczenia wspólne. Przykłady obejmują środki ochrony fizycznej i środowiskowej oraz środki bezpieczeństwa personelu.

[150] Zazwyczaj autoryzacje typu są wydawane przez organizacje, które są odpowiedzialne za rozwój standardowych możliwości sprzętu i oprogramowania dla klientów i dostarczane do organizacji odbiorców, jako rozwiązania "pod klucz". Osoby wydające takie autoryzacje mogą być określani, jako osoby wydający autoryzacje na rozwój.

Autoryzacja obiektu jest oficjalną decyzją o autoryzacji, która koncentruje się na konkretnych zabezpieczeniach wdrożonych w określonym środowisku działania w celu wsparcia jednego lub więcej systemów znajdujących się w tym środowisku. Autoryzacja obiektu odnosi się do zabezpieczeń wspólnych w obiekcie i pozwala systemom znajdującym się w zdefiniowanym środowisku na dziedziczenie zabezpieczeń wspólnych oraz planów bezpieczeństwa i prywatności systemu, które dotyczą pakietu autoryzacji dla obiektu. Zabezpieczenia wspólne są zapewnione na określonym poziomie wpływu w celu ułatwienia podejmowania decyzji o ryzyku związanym z lokalizacją danego systemu w danym obiekcie. [151] Zabezpieczenia fizyczne i środowiskowe są uwzględnione w zezwoleniu dla obiektu, ale mogą być również uwzględnione inne zabezpieczenia, na przykład ochrona granic obiektu, plan awaryjny i plan reagowania na incydenty dla obiektu lub szkolenie i uświadamianie personelu oraz bezpieczeństwo osobowe personelu obiektu. Osoba autoryzująca obiekt wydaje decyzję autoryzacyjną dla zabezpieczeń wspólnych w celu opisania zabezpieczeń wspólnych dostępnych do dziedziczenia przez systemy znajdujące się na terenie obiektu.

AUTORYZACJA TRADYCYJNA I WSPÓLNA

Organizacje mogą wybierać spośród dwóch różnych podejść przy planowaniu i wykonywaniu autoryzacji. Obejmują one autoryzację przez *jedną osobę autoryzującą* lub autoryzację przeprowadzaną przez *wielu autoryzujących*.[152] Pierwsze podejście to tradycyjny proces autoryzacji zdefiniowany w tym załączniku, w którym pojedyncza osoba w organizacji zajmująca wyższe stanowisko kierownicze jest odpowiedzialna za system lub zabezpieczenia wspólne. Osoba ta akceptuje ryzyko związane z bezpieczeństwem i prywatnością, które może mieć negatywny wpływ na działalność organizacji, aktywa organizacyjne, osoby prywatne, inne organizacje lub Państwo.

[151] Na przykład, jeżeli obiekt zostanie sklasyfikowany, jako obiekt o umiarkowanym poziomie wpływu, zlokalizowanie systemów lub elementów systemu o wysokim poziomie wpływu w tym środowisku pracy może nie być właściwe.

[152] Podejścia autoryzacyjne mogą być stosowane do systemów oraz do zabezpieczeń wspólnych dziedziczonych przez systemy organizacyjne.

Drugie podejście, *autoryzacja wspólna*, jest stosowane, gdy wiele osób z tej samej organizacji lub różnych organizacji, ma wspólny interes w autoryzacji systemu. Osoby z organizacji są wspólnie odpowiedzialne za system i łącznie akceptują ryzyko związane z bezpieczeństwem i prywatnością, które może mieć negatywny wpływ na operacje i aktywa organizacji, osoby prywatne, inne organizacje i Państwo. Proces autoryzacji jest realizowany podobnie jak w przypadku wykonywanego przez pojedynczą osobę autoryzującą, z zasadniczą różnicą polegającą na dodaniu do procesu autoryzacji wielu osób autoryzujących. Od organizacji wybierających autoryzację wspólną oczekuje się wspólnej pracy nad planowaniem i realizacją zadań RMF oraz wspólnego dokumentowania swojej zgody i postępów w realizacji zadań.

Współpraca w zakresie kategoryzacji bezpieczeństwa, doboru i dostosowania zabezpieczeń, opracowanie planu oceny zabezpieczeń w celu określenia skuteczności, planu i etapów działania oraz strategii ciągłego monitorowania na poziomie systemu, są niezbędne do skutecznego wspólnego udzielania autoryzacji wspólnej. Zasady i warunki autoryzacji wspólnej są ustalane przez strony uczestniczące we wspólnej autoryzacji, łącznie z procesem bieżącego określania i akceptacji ryzyka. Autoryzacja wspólna obowiązuje tylko wtedy, gdy istnieje zgoda między osobami autoryzującymi, a autoryzacja spełnia specyficzne wymagania ustanowione przez politykę krajową i organizacyjną. [NSC 800-53 wer. 2], zabezpieczenie rozszerzone CA-6(1) *Autoryzacja wspólna - wewnątrzorganizacyjna,* oraz zabezpieczenie rozszerzone CA-6(2) *Autoryzacja wspólna - międzyorganizacyjna*, opisują wymagania dotyczące autoryzacji wspólnych.

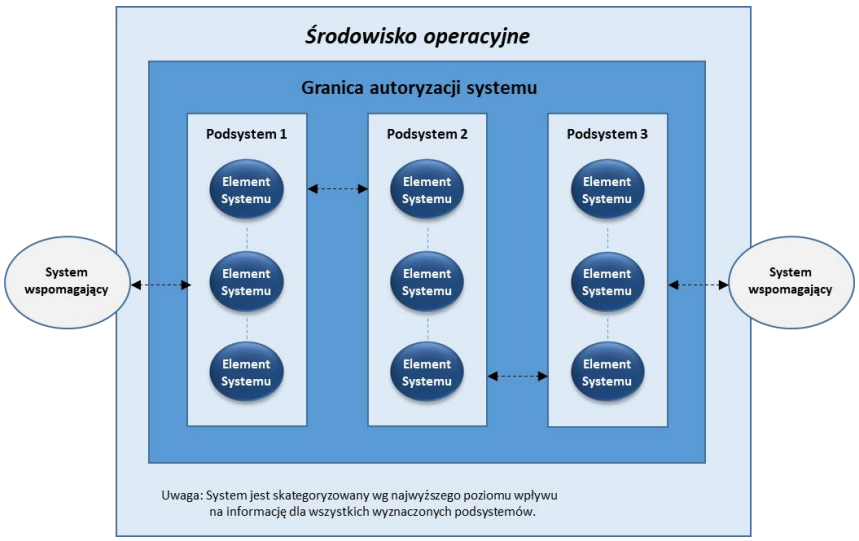
ZAŁĄCZNIK G GRANICE AUTORYZACJI

SYSTEMY ZŁOŻONE, ZASTOSOWANIA I SKUTKI ZMIENIAJĄCYCH SIĘ TECHNOLOGII

Niniejszy załącznik zawiera dodatkowe informacje dotyczące wyznaczania granic autoryzacji dla systemów złożonych i aplikacji programowych. Zawiera on również wskazówki dotyczące granic autoryzacji w przypadku, gdy organizacje korzystają z zewnętrznych dostawców swoich zasobów informatycznych. Podstawowe kroki i zadania RMF opisane w rozdziale trzecim mogą być stosowane we wszystkich trzech scenariuszach, aby pomóc organizacjom w zarządzaniu ryzykiem związanym z bezpieczeństwem i prywatnością oraz w przestrzeganiu przepisów prawa, rozporządzeń wykonawczych i zasad omówionych w rozdziale pierwszym.

GRANICE AUTORYZACJI SYSTEMÓW ZŁOŻONYCH

Ustalenie granic autoryzacji dla systemów złożonych może stanowić istotne wyzwanie dla organizacji. System złożony może być postrzegany, jako zestaw indywidualnych podsystemów. Podsystem jest głównym podzbiorem systemu składającym się z elementów systemu, które realizują jedną lub więcej określonych funkcji. Rysunek G-1 ilustruje koncepcję systemu złożonego.



Rysunek G-1: Koncepcyjne postrzeganie systemu złożonego

Organizacje mogą stosować koncepcję podsystemów w celu podzielenia złożonych systemów na zestaw zarządzanych elementów systemu lub zidentyfikowania tych elementów, które wspierają podobną misję, ale są wystarczająco odrębne, aby mogły być zidentyfikowane oddzielnie. Każdy podsystem posiada własną granicę (odrębną od granicy autoryzacji) i może być określony w ramach kompleksowej granicy autoryzacji, która obejmuje wszystkie podsystemy.

Na przykład, organizacja może uznać za użyteczne połączenie w jeden system kilku systemów, które znajdują się pod tą samą bezpośrednią kontrolą zarządczą lub które mają podobne zadania lub funkcje biznesowe, aby osiągnąć oba cele skutecznego zarządzania ryzykiem i zasobami. Organizacja może również zdecydować się na opracowanie systemu składającego się z wielu niezależnych systemów (rozmieszczonych na rozległym obszarze geograficznym) wspierających zestaw wspólnych misji lub funkcji biznesowych. Podobnie, system może być podzielony na wiele podsystemów, aby ułatwić i wesprzeć zarządzanie systemem i podejmowanie decyzji opartych na ryzyku (np. decyzje kategoryzacyjne, decyzje dostosowawcze i decyzje o alokacji zabezpieczeń).

Podział systemu na podsystemy (tj. dzielenie i kontrola systemu) ułatwia ukierunkowane zastosowanie zabezpieczeń w celu osiągnięcia odpowiedniego bezpieczeństwa, ochrony prywatności osób oraz efektywnego kosztowo procesu zarządzania ryzykiem. Podział złożonych systemów na podsystemy wspiera również ważne koncepcje bezpieczeństwa w zakresie rozdzielania domen i segmentacji sieci, które mogą być istotne w przypadku aktywów o wysokiej wartości. Gdy systemy są podzielone na podsystemy, organizacje mogą zdecydować się na opracowanie indywidualnych planów bezpieczeństwa i ochrony prywatności podsystemów lub ująć system i podsystemy w tych samych planach bezpieczeństwa i ochrony prywatności.

Architektury bezpieczeństwa i prywatności informacji odgrywają kluczową rolę w procesie dzielenia złożonych systemów na podsystemy. Obejmuje to monitorowanie i kontrolowanie komunikacji w wewnętrznych granicach między podsystemami oraz wybór, przydzielanie

i wdrażanie zabezpieczeń, które spełniają lub rozszerzają wymagania dotyczące bezpieczeństwa i ochrony prywatności podsystemów wchodzących w ich skład. Jednym z podejść do wyboru i przydzielania zabezpieczeń jest kategoryzowanie każdego zidentyfikowanego podsystemu oddzielnie (zob. Zadanie C-2). Oddzielna kategoryzacja każdego podsystemu nie zmienia jednak ogólnej kategoryzacji systemu. Oddzielna kategoryzacja każdego podsystemu pozwala na oddzielne i ukierunkowane przydzielanie zabezpieczeń z [NSC 800-53], zamiast wprowadzania zabezpieczeń o większym wpływie na cały system (zob. Zadanie P-17 i Zadanie S- 3). Innym podejściem jest łączenie mniejszych podsystemów w większe podsystemy w ramach systemu, kategoryzowanie każdego z zagregowanych podsystemów i, w razie potrzeby, przydzielanie zabezpieczeń podsystemom. Podczas, gdy podsystemy w ramach złożonych systemów mogą istnieć, jako kompletne systemy, w większości przypadków nie są one traktowane, jako niezależne podmioty, ponieważ są one zazwyczaj współzależne i wzajemnie powiązane.

W przypadku, gdy kategorie bezpieczeństwa dla zidentyfikowanych podsystemów są różne (np. o małym lub dużym wpływie), organizacja bada interfejsy podsystemów,[153] przepływu informacji oraz zależności między podsystemami w zakresie bezpieczeństwa i ochrony prywatności oraz wybiera odpowiednie zabezpieczenia dla wzajemnych połączeń podsystemów w celu wyeliminowania lub zmniejszenia potencjalnych podatności. Pomaga to zapewnić odpowiednią ochronę systemu. Zabezpieczenia wzajemnych połączeń podsystemów są również stosowane, gdy podsystemy realizują różne polityki bezpieczeństwa i ochrony prywatności lub są administrowane przez różne organy. Zakres, w jakim wybrane zabezpieczenia są prawidłowo wdrażane, działają zgodnie z założeniami i dają pożądany rezultat w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony

[153] Rodzaje interfejsów między podsystemami mogą wprowadzać niezamierzone podatności w systemie złożonym. Na przykład, jeżeli duży organizacyjny intranet zostanie podzielony na mniejsze podsystemy (np. Systemy rozdzielne, takie jak segmenty sieci lokalnej), a następnie skategoryzowany indywidualnie, konkretne zabezpieczenia na poziomie systemu mogą narazić wektor ataku na atak z intranetu poprzez błędne wybranie i wprowadzenie środków bezpieczeństwa, które nie są wystarczająco silne w stosunku do reszty systemu. Aby uniknąć takiej sytuacji, organizacje dokładnie badają interfejsy między podsystemami i podejmują odpowiednie działania w celu wyeliminowania potencjalnych podatności w tym obszarze, pomagając w ten sposób zapewnić odpowiednią ochronę systemu informatycznego.

prywatności dla złożonego systemu, można określić poprzez połączenie oceny zabezpieczeń na poziomie systemu i dodanie rozważań dotyczących kwestii związanych z interfejsami. Połączone podejście do oceny ułatwia ukierunkowany i efektywny kosztowo proces zarządzania ryzykiem poprzez skalowanie poziomu wysiłku związanego z oceną zgodnie z kategoryzacją bezpieczeństwa i umożliwienie ponownego wykorzystania wyników oceny na poziomie systemu.

GRANICE AUTORYZACJI APLIKACJI

Granice autoryzacji obejmują wszystkie elementy systemu, w tym sprzęt, oprogramowanie układowe i elementy oprogramowania. Elementy oprogramowania obejmują aplikacje (np. aplikacje bazodanowe, niestandardowe aplikacje biznesowe i aplikacje internetowe), oprogramowanie pośredniczące i systemy operacyjne. Elementy oprogramowania są zawarte w granicach autoryzacji, albo, jako część systemu informatycznego, w którym znajduje się oprogramowanie, albo, jako część systemu lub podsystemu wyłącznie aplikacyjnego, który dziedziczy zabezpieczenia systemu hostingowego. Elementy oprogramowania mogą zależeć od zasobów zapewnianych przez system hostingowy i jako takie mogą wykorzystywać środki bezpieczeństwa zapewniane przez system hostingowy, aby pomóc w zapewnieniu podstawowego poziomu ochrony hostowanych aplikacji. Dodatkowe mechanizmy bezpieczeństwa na poziomie aplikacji są zapewniane przez odpowiednie aplikacje, w zależności od potrzeb. Właściciele aplikacji koordynują swoje działania z właścicielami systemów, aby zapewnić spełnienie wymogów w zakresie bezpieczeństwa i ochrony prywatności w odniesieniu do aplikacji i systemów hostingowych. Koordynacja między właścicielami systemów i aplikacji obejmuje na przykład rozważenie wyboru, wdrożenia, oceny i monitorowania zabezpieczeń aplikacji; wpływu zmian w aplikacjach na bezpieczeństwo i prywatność systemu i organizacji; oraz wpływu zmian w systemie na aplikacje hostingowe.

GRANICE AUTORYZACJI I DOSTAWCY ZEWNĘTRZNI

O ile koncepcje systemów zewnętrznych i zewnętrznych dostawców usług nie są nowe, o tyle obecna powszechność i częstotliwość ich przywoływania może stanowić dla organizacji istotne, nowe wyzwania. Istnieją przypadki, w których elementy systemu, podsystemy, a nawet cały system może znajdować się poza bezpośrednią kontrolą organizacji, która autoryzuje jego działanie. Charakter takich zewnętrznych systemów może być różny w zależności od tego, czy organizacje wykorzystują zewnętrzne usługi chmury obliczeniowej do przetwarzania, przechowywania i przekazywania informacji do organizacji pozwalających platformom będącym pod ich kontrolą na hostowanie aplikacji lub usług opracowanych przez jakiś podmiot zewnętrzny.

Zasady cyberbezpieczeństwa wymagają, aby dostawcy zewnętrzni, którzy przetwarzają informacje lub obsługują systemy informatyczne w imieniu podmiotów publicznych, spełniali te same wymogi bezpieczeństwa i prywatności co podmioty publiczne. Wymogi rządowe w zakresie bezpieczeństwa i ochrony prywatności mają również zastosowanie do zewnętrznych systemów przechowujących, przetwarzających lub przekazujących informacje rządowe oraz do wszelkich usług świadczonych przez system zewnętrzny lub z nim związanych. Ponadto, wiarygodność lub pewność, że ryzyko związane z korzystaniem z usług dostawców zewnętrznych jest na akceptowalnym poziomie, zależy od zaufania, jakie organizacja pokłada w dostawcy. W niektórych przypadkach poziom zaufania opiera się na ilości bezpośrednich kontroli, jakie organizacja może sprawować nad dostawcą w zakresie stosowania zabezpieczeń niezbędnych do ochrony informacji przetwarzanych przez podmioty realizujące zadania publiczne i ochrony prywatności osób fizycznych.

Poziom zaufania może również opierać się na dowodach przedstawionych przez zewnętrznego dostawcę usług lub przez niezależnego podmiot oceniający w zakresie skuteczności tych zabezpieczeń. W innych przypadkach zaufanie może opierać się na innych czynnikach, takich jak wcześniejsze doświadczenia organizacji z usługodawcą zewnętrznym oraz zaufanie, jakim organizacja obdarza usługodawcę w zakresie podejmowania właściwych

działań. Istnieje wiele różnych czynników, które mogą komplikować poziom zaufania do zewnętrznych dostawców:

- Rozgraniczenie pomiędzy tym, co jest własnością dostawcy zewnętrznego, a organizacją może być rozmyte (np. należąca do organizacji platforma realizująca opracowaną przez dostawcę zewnętrznego aplikację, moduł oprogramowania lub firmware);
- Stopień kontroli organizacji nad dostawcą zewnętrznym może być bardzo ograniczony;
- Charakter i zawartość systemu, podsystemu, usługi lub aplikacji może podlegać szybkim zmianom; oraz
- System, podsystem, usługa lub aplikacja mogą mieć tak krytyczny charakter, że muszą być bardzo szybko włączone do systemów organizacyjnych.

Konsekwencją powyższych czynników jest to, że niektóre z tradycyjnych środków wykorzystywanych przez organizacje do weryfikacji i oceny prawidłowego funkcjonowania systemu, podsystemu, usługi lub zastosowania oraz skuteczności wdrożonych zabezpieczeń (np. jasno określone wymagania, analiza projektu, testowanie i ocena przed wdrożeniem, ocena zabezpieczeń i ciągłe monitorowanie) mogą być niewykonalne. W rezultacie organizacje mogą być uzależnione od charakteru relacji zaufania z dostawcą zewnętrznym stanowiącej podstawę do określenia, czy wydać zezwolenie na użytkowanie lub upoważnienie do działania systemu lub podsystemów, przetwarzanie, przechowywanie lub przekazywanie informacji przez podmioty realizujące zadania publiczne. Alternatywnie, organizacje mogą zezwolić na stosowanie systemów lub usług dostarczanych z zewnątrz tylko w tych przypadkach, w których ryzyko wymiany informacji określone przez organizację jest dopuszczalne. Ostatecznie, kiedy poziom zaufania do zewnętrznego dostawcy nie zapewnia wystarczającej pewności, organizacja stosuje zabezpieczenia kompensacyjne; akceptuje większe ryzyko; zawiera umowy z bardziej godnym zaufania zewnętrznym dostawcą; lub nie wykonuje usługi (tzn. realizuje swoje misje i prowadzi działalność biznesową z ograniczonym poziomem funkcjonalności lub ewentualnie nie realizuje jej wcale).

WYKORZYSTANIE ZABEZPIECZEŃ I OCEN DOSTAWCÓW ZEWNĘTRZNYCH

Organizacje powinny zachować ostrożność, podczas korzystania z zabezpieczeń i wyników oceny dostawców zewnętrznych. Zabezpieczenia wprowadzane przez dostawców zewnętrznych mogą różnić się od zabezpieczeń przewidzianych w [NSC 800-53] pod względem możliwości, zakresu stosowania i wydajności. Publikacja [NSC 800-53 MAP] dostarcza mapowanie środków bezpieczeństwa: NSC 800-53 – ISO/IEC 27001; ISO/IEC 27001 – NSC 800-53. Takie mapowania są jednak z natury rzeczy subiektywne i powinny być dokładnie przeanalizowane przez organizacje w celu ustalenia, czy zabezpieczenia i wymagania, do których odnoszą się dostawcy zewnętrzni, spełniają potrzeby organizacji w zakresie ochrony. Mapowanie pomiędzy różnymi normami lub wytycznymi nie uwzględnia również możliwości istnienia różnych zakresów i celów dla każdej publikacji.

Podobną ostrożność należy zachować w przypadku prób użycia lub stosowania wyników oceny bezpieczeństwa i ochrony prywatności uzyskanych od dostawców zewnętrznych. Rodzaj, rygor i zakres oceny może się znacznie różnić w zależności od dostawcy. Ponadto, procedury oceny stosowane przez dostawcę oraz niezależność osób przeprowadzających ocenę są krytycznymi zagadnieniami, które powinny zostać przeanalizowane i rozważone przez organizacje przed wykorzystaniem wyników oceny.

Skuteczność decyzji dotyczących ryzyka podejmowanych przez osoby autoryzujące zależy od przejrzystości zabezpieczeń wybranych i wdrożonych przez dostawców zewnętrznych oraz od jakości i skuteczności dowodów oceny przedstawionych przez tych usługodawców. Przejrzystość jest niezbędna do osiągnięcia pewności niezbędnej do zapewnienia odpowiedniej ochrony aktywów organizacji.

ZAŁĄCZNIK H UWAGI DOTYCZĄCE CYKLU ŻYCIA SYSTEMU

Inne czynniki wpływające na realizację RMF

Wszystkie systemy, w tym systemy operacyjne, systemy w trakcie rozwoju oraz systemy poddawane modyfikacjom lub modernizacji, znajdują się w pewnej fazie SDLC.[154] Definiowanie wymagań jest krytyczną częścią procesu SDLC i rozpoczyna się w fazie początkowej. Wymagania dotyczące bezpieczeństwa i ochrony prywatności są częścią wymagań funkcjonalnych i niefunkcjonalnych[155] przydzielonych do systemu. Wymagania dotyczące bezpieczeństwa i prywatności są włączane do SDLC równocześnie z innymi wymaganiami. Bez wczesnej integracji wymagań dotyczących bezpieczeństwa i ochrony prywatności, organizacja może ponieść znaczne wydatki w późniejszym okresie cyklu życia w celu rozwiązania problemów związanych z bezpieczeństwem i prywatnością, które mogły zostać uwzględnione w początkowym projekcie. Gdy wymagania dotyczące bezpieczeństwa i prywatności zostaną określone na wczesnym etapie SDLC i zintegrowane z innymi wymaganiami systemowymi, wynikowy system ma mniej braków, a co za tym idzie, mniej zagrożeń dla prywatności lub luk w zabezpieczeniach, które mogą być wykorzystane w przyszłości.

Włączenie wymagań dotyczących bezpieczeństwa i ochrony prywatności do SDLC jest najbardziej efektywną, skuteczną i opłacalną metodą zapewnienia, że strategia ochrony organizacji jest wdrażana. Zapewnia również, że procesy bezpieczeństwa i ochrony prywatności nie są odizolowane od innych procesów wykorzystywanych przez organizację do opracowania, wdrożenia, obsługi i utrzymania systemów wspierających bieżące misje i funkcje biznesowe. Poza włączeniem wymagań dotyczących bezpieczeństwa i ochrony prywatności do SDLC, wymagania te są zintegrowane z programem organizacji, planowaniem i budżetowaniem działalności organizacji, aby zapewnić dostępność zasobów w razie

[154] SDLC składa się z pięciu faz, w tym inicjacji, rozwoju i przejęcia, wdrożenia, eksploatacji i utrzymania oraz utylizacji. [SP 800-64] zawiera wytyczne dotyczące SDLC.
[155] Wymagania niefunkcjonalne obejmują, na przykład, wymagania dotyczące jakości i wiarygodności.

potrzeby oraz realizację etapów działania programu i projektu. Architektura korporacyjna zapewnia centralny zapis tej integracji w organizacji.

ZARZĄDZANIE RYZYKIEM W CYKLU ŻYCIA SYSTEMU

Działania w zakresie zarządzania ryzykiem rozpoczynają się we wczesnym etapie SDLC i są kontynuowane przez cały cykl życia produktu. Działania te są ważne w kształtowaniu możliwości systemu w zakresie bezpieczeństwa i ochrony prywatności; zapewnieniu, że wdrożone zostaną niezbędne zabezpieczenia i, że ryzyko związane z bezpieczeństwem i ochroną prywatnością będzie na bieżąco odpowiednio uwzględniane; oraz zapewnieniu, że osoby autoryzujące rozumieją obecną pozycję systemu w zakresie bezpieczeństwa i ochrony prywatności, aby zaakceptować ryzyko dla operacji i aktywów organizacyjnych, osób fizycznych, innych organizacji i Państwa.

Zapewnienie, że wymagania dotyczące bezpieczeństwa i ochrony prywatności są zintegrowane z SDLC pomaga ułatwić rozwój i wdrażanie bardziej odpornych systemów w celu zmniejszenia ryzyka związanego z bezpieczeństwem i prywatnością (w tym ryzyka związanego z łańcuchem dostaw) dla operacji organizacyjnych i aktywów, osób fizycznych, innych organizacji i Państwa. Można to osiągnąć dzięki zastosowaniu koncepcji zintegrowanych zespołów projektowych.[156] Decydenci organizacyjni zapewniają, że specjaliści ds. bezpieczeństwa i prywatności są częścią działań SDLC. Taka integracja zespołów sprzyja zwiększeniu współpracy pomiędzy personelem odpowiedzialnym za projektowanie, opracowywanie, wdrażanie, ocenę, eksploatację, utrzymanie i dysponowanie systemami oraz personelem ds. bezpieczeństwa i ochrony prywatności doradzającym kierownictwu wyższego szczebla w zakresie zabezpieczeń niezbędnych do odpowiedniego

[156] Zintegrowane zespoły projektowe są multidyscyplinarnymi jednostkami składającymi się z osób posiadających szereg umiejętności i pełniących różne role, które pomagają w rozwoju systemów spełniających wymagania organizacji.

ograniczenia ryzyka związanego z bezpieczeństwem i prywatnością oraz ochrony misji organizacji i funkcji biznesowych.

Wreszcie, organizacje maksymalizują wykorzystanie informacji istotnych z punktu widzenia bezpieczeństwa i ochrony prywatności wygenerowanych podczas procesu SDLC w celu spełnienia wymagań dotyczących podobnych informacji potrzebnych do innych celów związanych z bezpieczeństwem i prywatnością. Ponowne wykorzystanie informacji dotyczących bezpieczeństwa i ochrony prywatności jest skuteczną metodą ograniczania powielania wysiłków i dokumentacji; promowania wzajemności; oraz unikania niepotrzebnych kosztów, gdy działania związane z bezpieczeństwem i prywatnością są prowadzone niezależnie od procesów SDLC. Ponowne wykorzystanie promuje spójność informacji w zakresie opracowywania, wdrażania, oceny, obsługi, konserwacji i dysponowania systemami, w tym kwestie bezpieczeństwa i ochrony prywatności.

ISTOTNE ZNACZENIE DZIEDZINY ARCHITEKTURY I INŻYNIERII

Architekci ds. bezpieczeństwa, architekci ds. prywatności, inżynierowie bezpieczeństwa systemów i inżynierowie ds. prywatności mogą odegrać zasadniczą rolę w SDLC i w pomyślnym wykonaniu RMF. Architekci ds. bezpieczeństwa i prywatności oraz inżynierowie ds. bezpieczeństwa i prywatności udzielają właścicielom systemów oraz osobom autoryzującym porad technicznych w zakresie wyboru i wdrażania zabezpieczeń w systemach informatycznych - prowadząc i informując o decyzjach opartych na ryzyku w całym przedsiębiorstwie.

Architekci bezpieczeństwa i ochrony prywatności:

- Zapewniają, że wymagania dotyczące bezpieczeństwa i ochrony prywatności niezbędne do ochrony misji i procesów biznesowych są odpowiednio uwzględniane we wszystkich aspektach architektury korporacyjnej, w tym w modelach referencyjnych, architekturach segmentów i rozwiązań oraz systemach wspierających te misje i procesy biznesowe.
- Służą, jako główny łącznik pomiędzy architektami korporacyjnymi, a inżynierami bezpieczeństwa systemów, ochrony prywatności i danych osobowych.
- Współpracują z właścicielami systemów, dostawcami zabezpieczeń wspólnych oraz SSPO w zakresie przydzielania zabezpieczeń.
- Doradzają AO, CIO, SAORM lub RE, SAISO oraz SAOP w zakresie szeregu kwestii dotyczących bezpieczeństwa i prywatności.

Inżynierowie bezpieczeństwa systemów, ochrony prywatności i danych osobowych:

- Zapewniają, że wymagania dotyczące bezpieczeństwa i ochrony prywatności są zintegrowane z systemami i elementami systemu poprzez celową architekturę bezpieczeństwa lub ochrony prywatności, projektowanie, rozwój oraz konfigurację.

- Wprowadzają najlepsze praktyki podczas wdrażania zabezpieczeń w ramach systemu, w tym stosowania metodologii inżynierii oprogramowania; zasady bezpieczeństwa systemów lub inżynierii prywatności; bezpieczne lub zwiększające prywatność projektowanie, bezpieczną lub zwiększającą prywatność architekturę oraz bezpieczne ·lub zwiększające prywatność techniki kodowania.
- Koordynują działalność w zakresie bezpieczeństwa i ochrony prywatności z SAISO, SAOP, właścicielami systemów, dostawcami zabezpieczeń wspólnych, architektami bezpieczeństwa oraz ochrony prywatności oraz SSPO.