Ramy cyberbezpieczeństwa wg NIST (CSF) 2.0

Narodowy Instytut Norm i Technologii (National Institute of Standards and Technology)
Niniejsza publikacja jest dostępna bezpłatnie na stronie: https://doi.org/10.6028/NIST.CSWP.29.pol

26 lutego 2024 r.

Krótki opis

Dokument pt. „Ramy cyberbezpieczeństwa wg NIST (NIST Cybersecurity Framework, CSF) 2.0” przedstawia wytyczne dla przemysłu, agencji rządowych i innych organizacji w zakresie zarządzania ryzykiem związanym z cyberbezpieczeństwem. Oferuje taksonomię wyników w zakresie cyberbezpieczeństwa na wysokim poziomie, które mogą być wykorzystywane przez każdą organizację – niezależnie od jej wielkości, sektora czy dojrzałości – w celu lepszego zrozumienia, oceny, ustalenia priorytetów i komunikowania działań w zakresie cyberbezpieczeństwa. CSF nie określa, w jaki sposób wyniki powinny zostać osiągnięte. Zawiera raczej odniesienia do zasobów internetowych, które zapewniają dodatkowe wytyczne dotyczące praktyk i mechanizmów kontrolnych, jakie można wykorzystać do osiągnięcia tych wyników. W niniejszym dokumencie opisano założenia CSF 2.0, elementy ram oraz kilka sposobów ich wykorzystania.

Słowa kluczowe

cyberbezpieczeństwo; ramy cyberbezpieczeństwa (CSF); nadzór nad ryzykiem w zakresie cyberbezpieczeństwa; zarządzanie ryzykiem w przedsiębiorstwie; profile; poziomy zabezpieczeń.

Odbiorcy

Głównymi odbiorcami CSF są osoby odpowiedzialne za opracowywanie i realizację programów związanych z cyberbezpieczeństwem. Ramy CSF mogą być również wykorzystywane przez inne osoby zaangażowane w zarządzanie ryzykiem – w tym kierownictwo wyższego szczebla, zarząd, specjalistów ds. przejęć, specjalistów ds. technologii, kierowników ds. ryzyka, prawników, specjalistów ds. zasobów ludzkich oraz audytorów ds. cyberbezpieczeństwa i zarządzania ryzykiem – w celu wspierania ich decyzji związanych z cyberbezpieczeństwem. Ponadto ramy CSF mogą być przydatne dla osób tworzących i wpływających na politykę (takich jak stowarzyszenia, organizacje zawodowe, organy regulacyjne), które ustalają i komunikują priorytety w zakresie zarządzania ryzykiem cyberbezpieczeństwa.

Materiały uzupełniające

Instytut NIST nadal będzie tworzyć i udostępniać dodatkowe zasoby, które pomogą organizacjom wdrożyć CSF, w tym przewodniki po szybkim wdrażaniu i profile społeczności. Wszystkie zasoby są dostępne do wiadomości publicznej na stronie internetowej NIST CSF. Sugestie dotyczące dodatkowych zasobów, do których można się odwołać na stronie CSF wg NIST (dalej „NIST CSF”), mogą być zawsze udostępniane NIST pod adresem cyberframework@nist.gov.

Uwaga dla czytelników

O ile nie zaznaczono inaczej, cytowane lub przytaczanee dokumenty bądź fragmenty niniejszej publikacji nie są w całości włączone do niniejszej publikacji.

Przed wydaniem wersji 2.0 ramy cyberbezpieczeństwa nosiły nazwę „Ramy na rzecz poprawy cyberbezpieczeństwa infrastruktury krytycznej” (Framework for Improving Critical Infrastructure Cybersecurity). Tytuł ten nie ma zastosowania w przypadku CSF 2.0.

Podziękowania

Ramy CSF stanowią wynik wieloletniej współpracy przemysłu, środowisk akademickich i rządowych w Stanach Zjednoczonych i na całym świecie. Instytut NIST wyraża uznanie i składa podziękowania wszystkim tym, którzy przyczynili się do powstania niniejszych poprawionych ram CSF. Informacje na temat procesu opracowywania ram CSF można znaleźć na stronie internetowej NIST CSF. Wnioski, jakie wyciągnięto, korzystając z CSF, można zawsze przekazać instytutowi NIST pod adresem cyberframework@nist.gov.

Spis treści

Lista rysunków

Przedmowa

Ramy cyberbezpieczeństwa (Cybersecurity Framework, CSF) 2.0 opracowano z myślą o pomocy organizacjom różnej wielkości i z różnych sektorów – w tym przemysłu, administracji, środowisk akademickich oraz organizacji non-profit – w zarządzaniu ryzykiem związanym z cyberbezpieczeństwem i ograniczaniu tego rodzaju zagrożeń. Ramy CSF są przydatne niezależnie od poziomu dojrzałości i zaawansowania technicznego programów cyberbezpieczeństwa danej organizacji. Nie stanowią jednak podejścia uniwersalnego dla wszystkich. W każdej organizacji występują zarówno wspólne, jak i unikalne rodzaje ryzyka, a także różne poziomy ryzyka tolerowanego, konkretne misje i cele służące ich realizacji. Z tego względu sposoby, w jakie organizacje wdrażają CSF, będą zróżnicowane.

W idealnej sytuacji ramy CSF będą wykorzystywane do przeciwdziałania ryzyku w zakresie cyberbezpieczeństwa wraz z innymi rodzajami zagrożeń dla przedsiębiorstwa, w tym takich jak zagrożenia finansowe, związane z ochroną prywatności, łańcuchem dostaw, reputacją, a także o charakterze technologicznym lub fizycznym.

Ramy CSF *opisują* pożądane wyniki, które powinny być zrozumiałe dla szerokiego grona odbiorców, w tym kadry zarządzającej, kierowników i specjalistów, niezależnie od ich wiedzy fachowej w zakresie cyberbezpieczeństwa. Jako że wyniki te są neutralne z punktu widzenia sektora, kraju i technologii, zapewniają organizacji elastyczność niezbędną do uwzględnienia jej konkretnych zagrożeń, technologii i misji. Wyniki są mapowane bezpośrednio na listę potencjalnych kontroli bezpieczeństwa do natychmiastowego rozważenia w celu złagodzenia ryzyka związanego z cyberbezpieczeństwem.

Chociaż ramy CSF nie mają charakteru nakazowego, pomagają użytkownikom w poznaniu i wyborze konkretnych wyników. Sugestie dotyczące tego, w jaki sposób można osiągnąć poszczególne wyniki, znajdują się w rozszerzającym się zestawie zasobów internetowych, które uzupełniają ramy CSF, w tym w serii przewodników po szybkim wdrażaniu (Quick Start Guides, QSG). Ponadto różne narzędzia oferują dostępne do pobrania formaty, aby pomóc organizacjom, które zdecydują się na zautomatyzowanie niektórych ze swoich procesów. Poradniki QSG sugerują wstępne sposoby wykorzystania ram CSF i zachęcają czytelnika do głębszego zapoznania się z nimi i powiązanymi zasobami. Dostępne na stronie internetowej NIST CSF ramy CSF oraz wspomniane dodatkowe zasoby NIST i innych podmiotów powinny być postrzegane jako „portfel CSF", który pomaga w zarządzaniu ryzykiem i jego ograniczaniu. Niezależnie od sposobu ich zastosowania, ramy CSF zachęcają użytkowników do analizy swojego stanu cyberbezpieczeństwa w danym kontekście, a następnie dostosowania ich do konkretnych potrzeb.

Oparte na poprzednich wersjach ramy CSF 2.0 zawierają nowe funkcje, które podkreślają znaczenie *nadzoru* i *łańcuchów dostaw*. Szczególną uwagę zwrócono na przewodniki po szybkim wdrażaniu(QSG), by zapewnić, że ramy CSF stanowią istotne i łatwo dostępne rozwiązanie zarówno dla mniejszych, jak i większych organizacji. NIST zapewnia obecnie *Przykłady wdrożeń* oraz *Odniesienia informacyjne*, które są dostępne online i regularnie aktualizowane. Tworzenie aktualnych i docelowych *profili organizacyjnych* pomaga organizacjom w porównywaniu ich obecnego stanu z tym, który chcą lub muszą osiągnąć, a także umożliwia im szybsze wdrażanie i ocenę mechanizmów kontroli bezpieczeństwa.

Zagrożenia dla cyberbezpieczeństwa nieustannie rosną, a zarządzanie nimi musi być procesem ciągłym. Jest to prawdą niezależnie od tego, czy organizacja dopiero zaczyna stawiać czoła wyzwaniom związanym z cyberbezpieczeństwem, czy też działa od wielu lat i dysponuje zaawansowanym, dobrze wyposażonym zespołem ds. cyberbezpieczeństwa. Ramy CSF opracowano z myślą o każdym rodzaju organizacji, w związku z czym oczekuje się, że zapewnią one odpowiednie wytyczne na dłuższy czas.

1. Przegląd ram cyberbezpieczeństwa (CSF)

Niniejszy dokument stanowi wersję 2.0 dokumentu pt. „Ramy cyberbezpieczeństwa wg NIST" (dalej „Ramy CSF"). Ramy te składają się on z następujących elementów:

- ***Podstawa CSF*** (ang. CDF Core) – centralny element ram CSF stanowiącytaksonomię wyników w zakresie cyberbezpieczeństwa na wysokim poziomie, które mogą pomóc każdej organizacji w zarządzaniu ryzykiem związanym z cyberbezpieczeństwem. Elementy wchodzące w skład podstawy ram CSF to hierarchia funkcji, kategorii i podkategorii, w których opisano szczegółowo każdy wynik. Wyniki te są zrozumiałe dla szerokiego grona odbiorców, w tym kadry kierowniczej wyższego szczebla, kierowników i specjalistów, niezależnie od ich wiedzy fachowej w zakresie cyberbezpieczeństwa. Jako że wyniki są niezależne od sektora, kraju i technologii, zapewniają organizacji elastyczność niezbędną do uwzględnienia jej wyjątkowych zagrożeń, technologii i misji.
- ***Profile organizacyjne CSF***, które są mechanizmem opisującym obecny i/lub docelowy stan cyberbezpieczeństwa organizacji pod kątem wyników określonych w podstawie ram CSF.
- ***Poziomy CSF***, które można zastosować do profili organizacyjnych CSF w celu scharakteryzowania rygoru zarządzania ryzykiem w zakresie cyberbezpieczeństwa oraz praktyk nadzoru nad ryzykiem w danej organizacji. Poziomy mogą również zapewnić kontekst dla sposobu, w jaki organizacja postrzega ryzyko w zakresie cyberbezpieczeństwa, a także procesy zarządzania tym ryzykiem.

W niniejszym dokumencie opisano pożądane wyniki, *do osiągnięcia których* może dążyć dana organizacja. *Nie narzucono w nim* jednak wyników ani *sposobu* ich osiągnięcia. Opisy tego, w jaki sposób organizacja może osiągnąć te wyniki, znajdują się w pakiecie zasobów internetowych, które uzupełniają ramy CSF i są dostępne na stronie internetowej NIST CSF. Zasoby te oferują dodatkowe wskazówki dotyczące praktyk i kontroli, które można wykorzystać do osiągnięcia wyników i które mają pomóc organizacji w zrozumieniu, przyjęciu i stosowaniu ram CSF. Obejmują one:

- *Odniesienia informacyjne*, które wskazują źródła wytycznych dla każdego wyniku w istniejących normach globalnych, instrukcjach, ramach, regulacjach, politykach itp.
- *Przykłady wdrożeń*, które ilustrują potencjalne sposoby osiągnięcia każdego wyniku.
- *Przewodniki po szybkim wdrażaniu*, które zawierają praktyczne wskazówki dotyczące korzystania z ram CSF i ich zasobów online, w tym przejścia z wcześniejszych wersji ram CSF do wersji 2.0.
- *Profile społeczności* oraz *szablony profili organizacyjnych*, które pomagają danej organizacji wdrożyć w życie ramy CSF i określić priorytety w zakresie zarządzania ryzykiem związanym z cyberbezpieczeństwem.

Organizacja może korzystać z podstawy ram CSF, profili i poziomów wraz z zasobami uzupełniającymi, aby zrozumieć, ocenić, ustalić priorytety i komunikować zagrożenia dla cyberbezpieczeństwa.

- **Zrozumienie i ocena:** opisanie aktualnego lub docelowego stanu cyberbezpieczeństwa części lub całości organizacji, określenie luk oraz ocena postępów mających na celu ich wyeliminowanie.
- **Ustalanie priorytetów: i**dentyfikacja, organizacja i ustalanie priorytetów działań w zakresie zarządzania ryzykiem cyberbezpieczeństwa, które są zgodne z misją organizacji, wymogami prawnymi i regulacyjnymi oraz oczekiwaniami w zakresie zarządzania ryzykiem i nadzoru.
- **Komunikacja: z**apewnienie wspólnego języka komunikacji wewnątrz organizacji i poza nią na temat zagrożeń, możliwości, potrzeb i oczekiwań w zakresie cyberbezpieczeństwa.

Ramy CSF opracowano z myślą o organizacjach różnej wielkości i z różnych sektorów, w tym przemysłu, administracji, środowisk akademickich i organizacji non-profit, niezależnie od poziomu dojrzałości ich programów cyberbezpieczeństwa. Ramy CSF stanowią fundamentalny zasób, który można przyjąć dobrowolnie oraz poprzez politykę i mandaty rządowe. Taksonomia ram CSF i przytoczone standardy, wytyczne i praktyki nie są ukierunkowane na konkretny kraj, a poprzednie wersje CSF były z powodzeniem wykorzystywane przez wiele rządów i innych organizacji zarówno w Stanach Zjednoczonych, jak i w innych krajach.

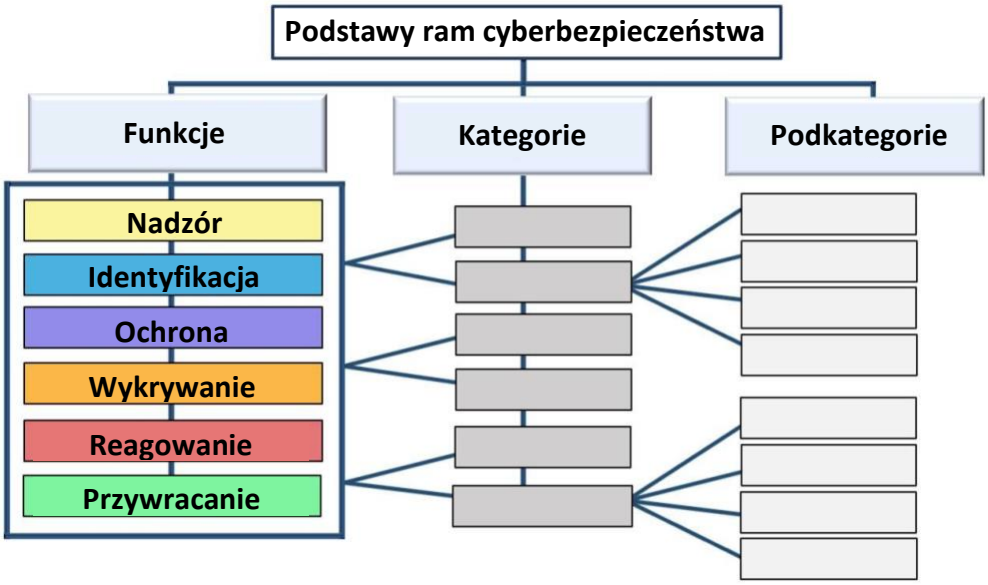
Z ram CSF należy korzystać w połączeniu z innymi zasobami (np. ramami, normami, wytycznymi, wiodącymi praktykami) w celu lepszego zarządzania ryzykiem związanym z cyberbezpieczeństwem oraz informowania o ogólnym zarządzaniu ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (ICT) na poziomie przedsiębiorstwa. CSF to elastyczne ramy, które z założenia mogą być wykorzystywane przez wszystkie organizacje, niezależnie od ich wielkości. W organizacjach nadal będą występować specyficzne rodzaje ryzyka – w tym różne zagrożenia i słabe punkty – oraz tolerancja ryzyka, jak również szczególne cele i kryteria misji. W związku z tym metody stosowane przez organizacje do zarządzania ryzykiem i wdrażania ram CSF będą się różnić.

Pozostała część niniejszego dokumentu ma następującą strukturę:

- W Części 2 wyjaśniono podstawy ram CSF: funkcje, kategorie i podkategorie.
- W Części 3 zdefiniowano koncepcje profili i poziomów CSF.
- Część 4 stanowi przegląd wybranych elementów pakietu zasobów internetowych CSF: odniesienia informacyjne, przykłady wdrożeń i przewodniki po szybkim wdrażaniu.
- W Części 5 omawiono sposób, w jaki organizacja może zintegrować CSF z innymi programami zarządzania ryzykiem.
- Załącznik A to podstawa ram CSF.
- Załącznik B zawiera hipotetyczną ilustrację poziomów CSF.
- Załącznik C to słownik terminologii CSF.

2. Wprowadzenie do podstawy ram CSF (CSF Core)

Załącznik A to podstawa ram CSF – zestaw wyników w zakresie cyberbezpieczeństwa uporządkowanych według funkcji, następnie kategorii, a na końcu podkategorii – jak przedstawiono na Rys. 1. Wyniki te nie stanowią listy kontrolnej działań do wykonania; konkretne działania podjęte w celu osiągnięcia wyniku będą się różnić w zależności od organizacji i przypadku zastosowania, podobnie jak osoba odpowiedzialna za te działania. Co więcej, kolejność i rozmiar funkcji, kategorii i podkategorii przedstawionych w podstawie nie wskazuje na kolejność ani ważność ich osiągnięcia. Struktura podstawy ma na celu w jak największym stopniu współgranie z osobami odpowiedzialnymi za operacjonalizację zarządzania ryzykiem w danej organizacji.



Rys. 1. Struktura podstawy ram CSF

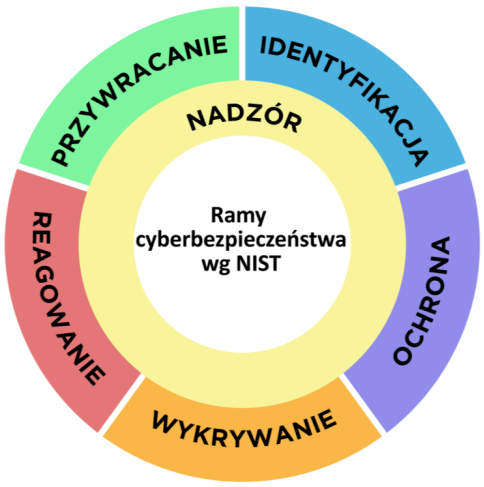
Funkcje podstawy ram CSF – nadzór, identyfikacja, ochrona, wykrywanie, reagowanie i przywracanie – organizują wyniki w zakresie cyberbezpieczeństwa na najwyższym poziomie.

- **Nadzór (Govern = GV)** – *strategia, oczekiwania i polityka organizacji w zakresie zarządzania ryzykiem związanym z cyberbezpieczeństwem są ustanawiane, komunikowane i monitorowane.* Funkcja Nadzoru zapewnia wyniki informujące o tym, co organizacja może zrobić, aby osiągnąć i nadać priorytet wynikom pozostałych pięciu funkcji w kontekście swojej misji oraz oczekiwań interesariuszy. Działania związane z Nadzorem mają kluczowe znaczenie dla włączenia cyberbezpieczeństwa do szerszej strategii zarządzania ryzykiem przedsiębiorstwa (ERM). Nadzór uwzględnia zrozumienie kontekstu organizacyjnego; ustanowienie strategii cyberbezpieczeństwa i zarządzanie ryzykiem cyberbezpieczeństwa w łańcuchu dostaw; role, obowiązki i uprawnienia; politykę; oraz nadzór nad strategią cyberbezpieczeństwa.
- **Identyfikacja (Identify = ID)** – *bieżące zagrożenia organizacji w zakresie cyberbezpieczeństwa organizacji stają się zrozumiałe.* Zrozumienie aktywów organizacji (np. danych, sprzętu, oprogramowania, systemów, obiektów, usług, ludzi), dostawców i powiązanych zagrożeń dla cyberbezpieczeństwa umożliwia organizacji ustalenie priorytetów zgodnie ze strategią zarządzania ryzykiem i potrzebami misji określonymi w ramach funkcji Nadzoru. Funkcja ta obejmuje również identyfikację możliwości poprawy polityki, planów, procesów, procedur i praktyk organizacji wspierających zarządzanie ryzykiem cyberbezpieczeństwa w celu informowania o wysiłkach podejmowanych w ramach wszystkich sześciu funkcji.

- **Ochrona (Protect = PR)** – *stosuje się zabezpieczenia do zarządzania ryzykiem w zakresie cyberbezpieczeństwa organizacji.* Po zidentyfikowaniu i ustaleniu priorytetów pod względem zasobów i zagrożeń funkcji Ochrony wspiera możliwości zabezpieczenia tych zasobów w celu zapobiegania lub zmniejszenia prawdopodobieństwa i wpływu niekorzystnych zdarzeń związanych z cyberbezpieczeństwem, a także w celu zwiększenia prawdopodobieństwa i wpływu wykorzystania możliwości. Wyniki objęte tą funkcją obejmują zarządzanie tożsamością, uwierzytelnianie i kontrolę dostępu; świadomość i szkolenia; bezpieczeństwo danych; bezpieczeństwo platformy (tj. zabezpieczenie sprzętu, oprogramowania i usług platform fizycznych i wirtualnych); oraz odporność infrastruktury technologicznej.
- **Wykrywanie (Detect = DE)** – *możliwe ataki i naruszenia cyberbezpieczeństwa są wykrywane i analizowane.* Funkcja ta umożliwia terminowe wykrywanie i analizowanie anomalii, wskaźników naruszenia bezpieczeństwa i innych potencjalnie niekorzystnych zdarzeń, które mogą wskazywać na występowanie ataków i incydentów cyberbezpieczeństwa. Funkcja wykrywania wspiera skuteczne działania związane z reagowaniem na incydenty i odzyskiwaniem danych.
- **Reagowanie (Respond = RS)** – *podejmowane są działania dotyczące wykrytego incydentu cyberbezpieczeństwa*. Funkcja ta wspiera zdolność do powstrzymywania skutków incydentów cyberbezpieczeństwa. Wyniki w ramach funkcji Reagowania obejmują zarządzanie incydentami, analizę, łagodzenie skutków, raportowanie i komunikację.
- **Przywracanie (Recover = RC)** – *przywrócone zostają aktywa i operacje dotknięte incydentem cyberbezpieczeństwa.* Funkcja ta wspiera terminowe przywracanie normalnych operacji w celu zmniejszenia skutków incydentów cyberbezpieczeństwa i umożliwienia odpowiedniej komunikacji w trakcie działań związanych z przywracaniem funkcjonowania organizacji.

Choć wiele działań z zakresu zarządzania ryzykiem cyberbezpieczeństwa koncentruje się na zapobieganiu negatywnym zdarzeniom, mogą one również wspierać wykorzystywanie pozytywnych możliwości. Działania mające na celu zmniejszenie ryzyka cyberbezpieczeństwa przyniosą organizacji korzyści również w inny sposób, choćby poprzez zwiększenie przychodów (np. najpierw oferując nadwyżkę powierzchni obiektowej komercyjnemu dostawcy usług hostingowych na potrzeby hostingu centrów danych własnych i innych organizacji, a następnie przenosząc główny system finansowy z wewnętrznego centrum danych organizacji do dostawcy usług hostingowych w celu zmniejszenia ryzyka w zakresie cyberbezpieczeństwa).

Na Rys. 2 przedstawiono funkcje ram CSF w formie koła, ponieważ wszystkie funkcje wiążą się ze sobą. Na przykład organizacja skategoryzuje zasoby w ramach funkcji Identyfikacji i podejmie kroki w celu zabezpieczenia tych zasobów w ramach funkcji Ochrony. Inwestycje w planowanie i testowanie w ramach funkcji Nadzoru i Identyfikacji będą wspierać terminowe wykrywanie nieoczekiwanych zdarzeń w ramach funkcji Wykrywania, a ponadto umożliwią reagowanie na incydenty i wdrożenie działań naprawczych w przypadku incydentów związanych z cyberbezpieczeństwem w ramach funkcji Reagowania i Przywracania. Nadzór znajduje się w centrum koła, ponieważ informuje, w jaki sposób organizacja wdroży pozostałe pięć funkcji.



Rys. 2. Funkcje ram CSF

Funkcje powinny być realizowane jednocześnie. Działania wspierające Nadzór, Identyfikację, Ochronę i Wykrywanie powinny odbywać się w sposób ciągły, zaś działania wspierające Reagowanie i Przywracanie powinny pozostawać w gotowości przez cały czas i mieć miejsce, gdy tylko wystąpią incydenty związane z cyberbezpieczeństwem. Wszystkie funkcje pełnią istotne role związane z incydentami w zakresie cyberbezpieczeństwa. Wyniki funkcji Nadzoru, Identyfikacji i Ochrony pomagają zapobiegać incydentom i przygotowywać się na nie, podczas gdy wyniki funkcji Nadzoru, Wykrywania, Reagowania i Przywracania pomagają wykrywać incydenty i zarządzać nimi.

Nazwa każdej funkcji pochodzi od czynności, która opisuje jej znaczenie. Każda funkcja dzieli się na kategorie, które są powiązanymi wynikami w zakresie cyberbezpieczeństwa i które wspólnie składają się na daną funkcję. Podkategorie dzielą każdą kategorię na bardziej szczegółowe wyniki działań o charakterze technicznym i zarządczym. Podkategorie nie są wyczerpujące, lecz opisują szczegółowe wyniki, które wspierają każdą kategorię.

Funkcje, kategorie i podkategorie mają zastosowanie do wszystkich technologii informacyjno-komunikacyjnych wykorzystywanych przez daną organizację, w tym technologii informacyjnej (IT), Internetu rzeczy (IoT) i technologii operacyjnej (OT). Mają one również zastosowanie do wszystkich rodzajów środowisk technologicznych, w tym systemów chmurowych, mobilnych i sztucznej inteligencji. Podstawa ram CSF jest zorientowana na przyszłość i została opracowana z myślą o przyszłych zmianach w technologiach i środowiskach.

3. Wprowadzenie do profili i poziomów ram CSF

W tej sekcji zdefiniowano koncepcje profili i poziomów ram CSF.

3.1. Profile ram CSF

Profil organizacyjny CSF opisuje aktualny i/lub docelowy stan cyberbezpieczeństwa danej organizacji w kontekście wyników określonych w Podstawie ram. Profile organizacyjne wykorzystuje się do zrozumienia, dostosowania, oceny, ustalania priorytetów i komunikowania wyników Podstawy poprzez uwzględnienie celów misji organizacji, oczekiwań interesariuszy, środowiska zagrożeń oraz wymagań. Organizacja może wówczas ustalić priorytety swoich działań w celu osiągnięcia określonych wyników, a następnie przekazać te informacje interesariuszom.

Każdy profil organizacyjny zawiera jeden lub oba z poniższych elementów:

1. *Profil bieżący* (Current Profile) określa wyniki w zakresie podstawy, które organizacja obecnie osiąga (lub próbuje osiągnąć) i charakteryzuje, w jaki sposób lub w jakim stopniu osiągany jest każdy wynik.
2. *Profil docelowy* (Target Profile) określa pożądane wyniki, które organizacja wybrała i uszeregowała pod względem ważności, aby osiągnąć swoje cele w zakresie zarządzania ryzykiem cyberbezpieczeństwa. Profil docelowy uwzględnia przewidywane zmiany w stanie cyberbezpieczeństwa danej organizacji, takie jak nowe wymagania, wdrażanie nowych technologii oraz trendy związane z informacjami o zagrożeniach.

Profil społeczności (Community Profile) jest bazą wyników CSF, którą się tworzy i publikuje w celu uwzględnienia wspólnych interesów i celów wielu organizacji. Profil społeczności jest zazwyczaj opracowywany dla określonego sektora, podsektora, technologii, typu zagrożenia lub innego przypadku użycia. Organizacja może użyć profilu społeczności jako podstawy do stworzenia własnego profilu docelowego. Przykłady profili społeczności można znaleźć na stronie internetowej NIST CSF.

Kroki przedstawione i podsumowane na Rys. 3 ilustrują jeden ze sposobów, w jaki organizacja może wykorzystać profil organizacyjny, aby zapewnić nieustanne udoskonalanie swojego cyberbezpieczeństwa.

Rys. 3. Kroki tworzenia i korzystania z profilu organizacyjnego CSF

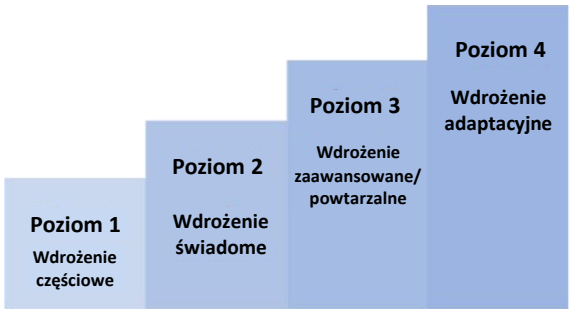
1. **Zakres profilu organizacyjnego.** Należy udokumentować ogólne fakty i założenia, na których profil będzie się opierał, by zdefiniować jego zakres. Organizacja może mieć dowolną liczbę profili organizacyjnych – każdy o innym zakresie. Profil może na przykład dotyczyć całej organizacji lub być ograniczony do systemów finansowych organizacji bądź też do przeciwdziałania zagrożeniom typu ransomware i obsługi incydentów związanych z ransomware dotyczących wspomnianych systemów finansowych.
2. **Zebranie informacji potrzebnych do przygotowania profilu organizacyjnego.** Przykładowe informacje mogą obejmować politykę organizacji, priorytety i zasoby zarządzania ryzykiem, profile ryzyka przedsiębiorstwa, rejestry analizy wpływu na działalność (BIA), wymagania i standardy cyberbezpieczeństwa obowiązujące w organizacji, praktyki i narzędzia (np. procedury i zabezpieczenia) oraz role zawodowe.
3. **Utworzenie profilu organizacyjnego.** Określenie, jakie rodzaje informacji powinien zawierać profil dla wybranych wyników CSF i udokumentowanie potrzebnych informacji. Rozważenie implikacji ryzyka bieżącego profilu w celu poinformowania o planowaniu profilu docelowego i ustalaniu priorytetów. Należy również rozważyć wykorzystanie profilu społeczności jako podstawy do stworzenia profilu docelowego.
4. **Przeanalizowanie luk między profilem bieżącym i docelowym oraz stworzenie planu działania.** Przeprowadzenie analizy luk w celu zidentyfikowania i przeanalizowania różnic między profilem bieżącym i docelowym oraz opracowanie planu działania o ustalonym priorytecie (np. rejestr ryzyka, szczegółowy raport dotyczący ryzyka, plan działania i kamienie milowe [POA&M]) w celu wyeliminowania tych luk.
5. **Wdrożenie planu działania i aktualizacja profilu organizacyjnego.** Należy postępować zgodnie z planem działania, aby wyeliminować luki i przesunąć organizację w kierunku profilu docelowego. Plan działania może mieć określony ogólny termin lub może być realizowany na bieżąco.

Biorąc pod uwagę znaczenie nieustannego udoskonalania, organizacja może powtarzać te kroki tak często, jak jest to konieczne.

Istnieją dodatkowe zastosowania profili organizacyjnych. Profil bieżący może na przykład służyć do dokumentowania i komunikowania możliwości organizacji w zakresie cyberbezpieczeństwa oraz istniejących możliwości udoskonaleń na rzecz interesariuszy zewnętrznych, takich jak partnerzy biznesowi lub potencjalni klienci. Profil docelowy może również pomóc w przedstawieniu wymagań i oczekiwań danej organizacji w zakresie zarządzania ryzykiem cyberbezpieczeństwa dostawcom, partnerom i innym stronom trzecim jako celu do osiągnięcia przez te podmioty.

3.2. Poziomy CSF

Organizacja może zdecydować się na zastosowanie poziomów na potrzeby informowania o swoich profilach bieżących i docelowych. Poziomy charakteryzują rygor praktyk w zakresie nadzoru nad ryzykiem cyberbezpieczeństwa w danej organizacji i zapewniają kontekst dla sposobu, w jaki organizacja postrzega ryzyko cyberbezpieczeństwa i procesy zarządzania tym ryzykiem. Poziomy, jak przedstawiono na Rys. 4 i zilustrowano w Załączniku B, odzwierciedlają praktyki organizacji w zakresie zarządzania ryzykiem cyberbezpieczeństwa jako wdrożenie częściowe (poziom 1), wdrożenie świadome ryzyka (poziom 2), wdrożenie zaawansowane/powtarzalne (poziom 3) oraz wdrożenie adaptacyjne (poziom 4). Poziomy opisują progresję od nieformalnych, doraźnych reakcji do podejść, które są sprawne, świadome ryzyka i nieustannie udoskonalane. Wybór poziomów pomaga nadać ogólny ton sposobowi, w jaki organizacja będzie zarządzać ryzykiem cyberbezpieczeństwa.



Rys. 4. Poziomy CSF na potrzeby nadzoru nad ryzykiem związanym z cyberbezpieczeństwem

Poziomy wdrożeń powinny uzupełniać metodologię zarządzania ryzykiem cyberbezpieczeństwa organizacji, a nie ją zastępować. Organizacja może na przykład wykorzystać poziomy wdrożeń do komunikacji wewnętrznej jako punkt odniesienia dla ogólnego podejścia do zarządzania ryzykiem cyberbezpieczeństwa przyjętego w całej organizacji[1]. Przejście do wyższych poziomów jest wskazane w przypadku, gdy ryzyko lub obowiązki są większe lub gdy analiza kosztów i korzyści wskazuje na wykonalne i opłacalne zmniejszenie negatywnych zagrożeń dla cyberbezpieczeństwa.

Strona internetowa NIST CSF zawiera dodatkowe informacje na temat korzystania z profili i poziomów wdrożeń. Obejmują one wskaźniki do szablonów profili organizacyjnych hostowanych przez NIST oraz repozytorium Profili społeczności w różnych formatach przystosowanych do odczytu maszynowego i obsługi przez człowieka.

[1] Na potrzeby niniejszego dokumentu terminy „cała organizacja” i „przedsiębiorstwo” mają to samo znaczenie.

4. Wprowadzenie do internetowych materiałów uzupełniających CSF

NIST i inne organizacje opracowały zestaw zasobów internetowych, które pomagają organizacjom zrozumieć, przyjąć i stosować ramy CSF. Jako że wspomniane zasoby uzupełniające są hostowane online, mogą być aktualizowane częściej niż niniejszy dokument – który jest aktualizowany dość rzadko – w celu zapewnienia użytkownikom stabilności. Są one również dostępne w formatach przystosowanych do odczytu maszynowego. Ta część zawiera przegląd trzech rodzajów zasobów online: odniesienia informacyjne, przykłady wdrożeń i przewodniki po szybkim wdrażaniu. Odniesienia informacyjne, przykłady wdrożeń i przewodniki po szybkim wdrażaniu.

Odniesienia informacyjne to mapowania, które wskazują relacje między podstawą a różnymi standardami, wytycznymi, przepisami i innymi treściami. Dostarczają one informacji o tym, w jaki sposób organizacja może osiągnąć wyniki zawarte w podstawie ram. Odniesienia informacyjne mogą być powiązane z określonym sektorem lub technologią. Mogą być opracowane przez instytut NIST lub inną organizację. Niektóre Odniesienia informacyjne mają węższy zakres niż podkategoria. Na przykład, konkretna kontrola na podstawie publikacji specjalnej SP 800-53 – *Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji (Security and Privacy Controls for Information Systems and Organizations)*, *Security and Privacy Controls for Information Systems and Organizations*) może być jednym z wielu odniesień potrzebnych do osiągnięcia rezultatu opisanego w jednej z podkategorii. Inne Odniesienia informacyjne mogą znajdować się na wyższym poziomie, np. wymóg wynikający z polityki, która częściowo odnosi się do wielu podkategorii. Korzystając z ram CSF, organizacja może zidentyfikować najistotniejsze Odniesienia informacyjne.

Przykłady wdrożeń dostarczają hipotetycznych przykładów zwięzłych, zorientowanych na działanie kroków, które pomogą osiągnąć wyniki w danych podkategoriach. Działania określone w Przykładach obejmują udostępnianie, dokumentowanie, rozwijanie, wykonywanie, monitorowanie, analizowanie, ocenianie i realizowanie. Przykłady nie stanowią wyczerpującej listy wszystkich działań, które mogą zostać podjęte przez organizację w celu osiągnięcia rezultatu, nie reprezentują podstawy wymaganych działań w celu przeciwdziałania zagrożeniom związanym z cyberbezpieczeństwem.

Przewodniki po szybkim wdrażaniu (Quick-Start Guides, QSG) to krótkie dokumenty dotyczące konkretnych tematów związanych z ramami CSF, często dostosowane do określonych odbiorców. Poradniki QSG mogą pomóc organizacji wdrożyć ramy CSF, ponieważ przekształcają określone części ram CSF w wykonalne „pierwsze kroki", które organizacja może rozważyć na drodze do poprawy swojej sytuacji w zakresie cyberbezpieczeństwa i zarządzania powiązanymi zagrożeniami. Poradniki są aktualizowane według własnych ram czasowych, a nowe poradniki dodaje się w miarę potrzeb.

Sugestie dotyczące nowych Odniesień informacyjnych dla ram CSF 2.0 można zawsze przekazać do instytutu NIST, pisząc na adres olir@nist.gov. Sugestie dotyczące innych zasobów, do których można się odnieść na stronie NIST CSF, w tym dodatkowych tematów ujętych w formie poradnika QSG, należy kierować na adres cyberframework@nist.gov.

5. Poprawa komunikacji i integracji w zakresie ryzyka związanego z cyberbezpieczeństwem

Wykorzystanie ram CSF będzie się różnić w zależności od indywidualnej misji organizacji oraz występujących w niej zagrożeń. Rozumiejąc oczekiwania interesariuszy oraz ryzyko tolerowane (jak określono w funkcji Nadzoru), organizacja może ustalić priorytety działań dotyczących cyberbezpieczeństwa w celu podejmowania świadomych decyzji dotyczących wydatków i działań w zakresie cyberbezpieczeństwa. Organizacja może zdecydować się na obsługę ryzyka na jeden lub na kilka sposobów – w tym poprzez łagodzenie, przenoszenie, unikanie lub akceptowanie ryzyka negatywnego oraz realizowanie, dzielenie się, wzmacnianie lub przyjmowanie ryzyka pozytywnego – w zależności od potencjalnego wpływu i prawdopodobieństwa. Co ważne, organizacja jest w stanie wykorzystywać ramy CSF zarówno wewnętrznie do zarządzania swoimi możliwościami w zakresie cyberbezpieczeństwa, jak i zewnętrznie do nadzorowania lub komunikowania się ze stronami trzecimi.

Niezależnie od sposobu wykorzystania ram CSF organizacja zapewne odniesie korzyści z zastosowania ich jako wytycznych, które pomogą jej zrozumieć, ocenić, ustalić priorytety i zakomunikować zagrożenia związane z cyberbezpieczeństwem, jak również działania, które posłużą do zarządzania tymi zagrożeniami. Wybrane wyniki można wykorzystać do skoncentrowania się na strategicznych decyzjach i ich wdrożenia w celu poprawy cyberbezpieczeństwa i utrzymania ciągłości funkcji niezbędnych do realizacji misji, przy jednoczesnym uwzględnieniu priorytetów i dostępnych zasobów.

5.1. Poprawa komunikacji w zakresie zarządzania ryzykiem

Ramy CSF stanowią podstawę dla lepszej komunikacji w zakresie oczekiwań, planowania i zasobów związanych z cyberbezpieczeństwem. Wspierają dwukierunkowy przepływ informacji (jak pokazano w górnej połowie Rys. 5) między kadrą zarządzającą wyższego szczebla, która koncentruje się na priorytetach organizacji i kierunku strategicznym, a kierownikami, którzy zarządzają określonymi zagrożeniami w zakresie cyberbezpieczeństwa mogącymi mieć wpływ na osiągnięcie tych priorytetów. Ramy CSF wspierają również podobny przepływ komunikacji (jak pokazano w dolnej połowie Rys. 5) między kierownikami a specjalistami, którzy wdrażają i obsługują technologie. Lewa strona rysunku przedstawia znaczenie dzielenia się przez specjalistów aktualizacjami, spostrzeżeniami i obawami z kierownikami oraz kadrą zarządzającą.

Rys. 5. Wykorzystanie ram CSF do poprawy komunikacji w zakresie zarządzania ryzykiem

Przygotowanie do tworzenia i korzystania z profili organizacyjnych obejmuje gromadzenie informacji o priorytetach danej organizacji, jej zasobach i kierunku ryzyka począwszy od kadry zarządzającej. Następnie kierownicy współpracują ze specjalistami w celu komunikowania potrzeb biznesowych i tworzenia świadomych ryzyka profili organizacyjnych. Działania mające na celu usunięcie wszelkich luk zidentyfikowanych między profilem bieżącym a profilem docelowym zostaną wdrożone przez kierowników i specjalistów i zapewnią kluczowe dane wejściowe do planów na poziomie systemu. W miarę osiągania przez organizację stanu określonego w profilu docelowym – w tym poprzez kontrole i monitorowanie stosowane na poziomie systemu – zaktualizowane wyniki mogą być udostępniane za pośrednictwem rejestrów ryzyka i raportów z postępów. W ramach ciągłej oceny kierownicy uzyskują wgląd w celu wprowadzania korekt, które jeszcze bardziej ograniczą potencjalne szkody i zwiększą potencjalne korzyści.

Funkcja Nadzoru wspiera komunikację w zakresie ryzyka dla organizacji z **kadrą zarządzającą**. Dyskusje kadry kierowniczej dotyczą strategii, a w szczególności tego, w jaki sposób niepewność związana z cyberbezpieczeństwem może wpłynąć na osiągnięcie celów organizacyjnych. Dyskusje te wspierają dialog i porozumienie w zakresie strategii nadzoru nad ryzykiem (w tym ryzykiem łańcucha dostaw pod kątem cyberbezpieczeństwa); ról, obowiązków i uprawnień; poszczególnych polityk oraz nadzoru. Gdy kadra zarządzająca ustala priorytety i cele w zakresie cyberbezpieczeństwa w oparciu o te potrzeby, komunikuje oczekiwania dotyczące ryzyka tolerowanego, odpowiedzialności i zasobów. Kadra zarządzająca jest również odpowiedzialna za integrację zarządzania ryzykiem cyberbezpieczeństwa z programami ERM oraz programami zarządzania ryzykiem niższego szczebla (zob. część 5.2). Komunikacja odzwierciedlona w górnej połowie Rys. 5 może obejmować kwestie dotyczące ERM i programów niższego poziomu, a tym samym stanowić źródło informacji dla kierowników i specjalistów.

Ogólne cele cyberbezpieczeństwa ustalone przez kadrę zarządzającą są przekazywane kaskadowo do **kierowników**. W podmiotach komercyjnych mogą one dotyczyć linii biznesowej lub działu operacyjnego. W przypadku podmiotów rządowych mogą to być kwestie na poziomie działu lub oddziału. Podczas wdrażania ram CSF kierownicy skupią się na tym, jak osiągnąć docelowe poziomy ryzyka poprzez wspólne usługi, kontrole i współpracę określone w profilu docelowym i udoskonalane poprzez monitorowanie działań zawartych w planie działania (np. rejestr ryzyka, szczegółowy raport dotyczący ryzyka, plan działań i kamienie milowe (POA&M)).

Specjaliści koncentrują się na wdrażaniu stanu docelowego i mierzeniu zmian w ryzyku operacyjnym, aby ułatwić planowanie, przeprowadzanie i monitorowanie określonych działań w zakresie cyberbezpieczeństwa. W miarę wdrażania mechanizmów kontrolnych w celu zarządzania ryzykiem na akceptowalnym poziomie specjaliści dostarczają kierownikom i kadrze zarządzającej niezbędnych informacji (np. kluczowych wskaźników wydajności, kluczowych wskaźników ryzyka) pozwalających zrozumieć stan cyberbezpieczeństwa organizacji, podejmować świadome decyzje i utrzymywać lub odpowiednio dostosowywać strategię ryzyka. Kadra zarządzająca może również łączyć te dane dotyczące ryzyka cyberbezpieczeństwa z informacjami o innych rodzajach zagrożeń z całej organizacji. Aktualizacje oczekiwań i priorytetów są uwzględniane w zaktualizowanych profilach organizacyjnych w miarę powtarzania się cyklu.

5.2. Poprawa integracji z innymi programami zarządzania ryzykiem

Każda organizacja stoi w obliczu wielu rodzajów ryzyka ICT (np. w zakresie ochrony prywatności, łańcucha dostaw, sztucznej inteligencji) i może korzystać z ram oraz narzędzi zarządzania, dostosowanych do każdego rodzaju ryzyka. Niektóre organizacje integrują ICT i wszystkie inne wysiłki związane z zarządzaniem ryzykiem na wysokim poziomie za pomocą systemu ERM, podczas gdy inne

utrzymują je oddzielnie, by zapewnić należytą uwagę każdemu z nich. Małe organizacje ze względu na swój charakter mogą monitorować ryzyko na poziomie przedsiębiorstwa, podczas gdy większe firmy mogą utrzymywać oddzielne działania w zakresie zarządzania ryzykiem zintegrowane z systemem ERM.

Organizacje mogą stosować metody ERM w celu zrównoważenia portfela czynników ryzyka – w tym cyberbezpieczeństwa – i podejmowania świadomych decyzji. Kadra zarządzająca otrzymuje istotne informacje na temat bieżących i planowanych działań związanych z ryzykiem, ponieważ integruje strategie zarządzania i ryzyka z wynikami poprzednich zastosowań ram CSF. Ramy CSF pomagają organizacjom przełożyć terminologię dotyczącą cyberbezpieczeństwa i zarządzania ryzykiem w zakresie cyberbezpieczeństwa na ogólny język zarządzania ryzykiem, który będzie zrozumiały dla kadry zarządzającej.

Zasoby NIST, które opisują wzajemne relacje między zarządzaniem ryzykiem cyberbezpieczeństwa a systemem EMR, obejmują następujące elementy:

- *Ramy cyberbezpieczeństwa wg NIST 2.0 – Przewodnik po szybkim wdrażaniu zarządzania ryzykiem w przedsiębiorstwie*
- Raport międzyagencyjny NIST (IR) 8286, *Integracja cyberbezpieczeństwa i zarządzanie ryzykiem w przedsiębiorstwie (ERM)*
- IR 8286A, *Identyfikacja i szacowanie ryzyka cyberbezpieczeństwa na potrzeby zarządzania ryzykiem w przedsiębiorstwie*
- IR 8286A, *Priorytetyzacja ryzyka cyberbezpieczeństwa na potrzeby zarządzania ryzykiem w przedsiębiorstwie*
- IR 8286C, *Określenie ryzyka cyberbezpieczeństwa na potrzeby zarządzania ryzykiem w przedsiębiorstwie i nadzoru nad ładem korporacyjnym*
- IR 8286D, *Wykorzystywanie analizy wpływu biznesowego (BIA) do priorytetyzacji ryzyka i reagowania na nie*
- SP 800-221, *Wpływ ryzyka związanego z technologiami informacyjno-komunikacyjnymi na przedsiębiorstwo: zarządzanie programami ryzyka związanego z technologią informacyjno-komunikacyjną (ICT) w ramach portfela ryzyka przedsiębiorstwa*
- SP 800-221A, *Wyniki ryzyka związanego z technologią informacyjno-komunikacyjną (ICT): Integracja programów zarządzania ryzykiem ICT z portfelem ryzyka przedsiębiorstwa*

Organizacja może również uznać ramy CSF za korzystne dla integracji zarządzania ryzykiem cyberbezpieczeństwa z indywidualnymi programami zarządzania ryzykiem ICT, takimi jak:

- **Zarządzanie ryzykiem cyberbezpieczeństwa i jego ocena:** ramy CSF można zintegrować z istniejącymi programami zarządzania i oceny ryzyka cyberbezpieczeństwa, takimi jak SP 800-37 – Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych oraz SP 800-30 – *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka* na podstawie ram zarządzania ryzykiem wg NIST (RMF). W przypadku organizacji korzystającej z ram RMF wg NIST i pakietu publikacji instytutu ramy CSF można wykorzystać do uzupełnienia koncepcji RMF w zakresie wyboru i priorytetyzacji mechanizmów kontrolnych zawartych w publikacji SP 800-53 – *Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji*.
- **Zagrożenia dla prywatności:** chociaż cyberbezpieczeństwo i ochrona prywatności stanowią niezależne dyscypliny, ich cele pokrywają się w pewnych okolicznościach, jak pokazano na Rys. 6.

Rys. 6. Związek ryzyka w zakresie cyberbezpieczeństwa i ochrony prywatności

Zarządzanie ryzykiem cyberbezpieczeństwa jest niezbędne do przeciwdziałania zagrożeniom dla ochrony prywatności związanym z utratą poufności, integralności i dostępności danych osób fizycznych. Na przykład naruszenie danych może prowadzić do kradzieży tożsamości. Zagrożenia związane z ochroną prywatności mogą jednak powstać również w sposób niezwiązany z incydentami cyberbezpieczeństwa.

Organizacja przetwarza dane w celu realizacji misji lub celów biznesowych, co może czasami prowadzić do *zdarzeń związanych z ochroną prywatności*, w wyniku których osoby fizyczne doświadczają problemów wynikających z przetwarzania danych. Problemy te można wyrażać na różne sposoby, ale w NIST opisano je jako obejmujące zarówno skutki związane z godnością (np. zażenowanie lub stygmatyzacja), jak i bardziej namacalne szkody (np. dyskryminacja, straty ekonomiczne lub szkody fizyczne). Ramy ochrony prywatności NIST oraz ramy cyberbezpieczeństwa NIST mogą być wykorzystywane razem w celu uwzględnienia różnych aspektów cyberbezpieczeństwa i zagrożeń dla prywatności. Ponadto metodyka zarządzania ryzykiem w zakresie ochrony prywatności (Privacy Risk Assessment Methodology, PRAM) wg NIST zawiera katalog przykładowych problemów do wykorzystania w ocenach tego typu ryzyka.

- **Ryzyko w łańcuchu dostaw:** organizacja może wykorzystać ramy CSF do wspierania nadzoru nad ryzykiem cyberbezpieczeństwa i komunikacji z interesariuszami w łańcuchach dostaw. Wszystkie rodzaje technologii opierają się na złożonym, rozproszonym globalnie, rozległym i wzajemnie połączonym ekosystemie łańcucha dostaw z geograficznie zróżnicowanymi trasami i wieloma poziomami outsourcingu. Ekosystem ten składa się z podmiotów z sektora publicznego i prywatnego (np. nabywców, dostawców, programistów, integratorów systemów, zewnętrznych dostawców usług systemowych i innych dostawców usług związanych z technologią), które współdziałają w celu prowadzenia badań, opracowywania, projektowania, produkcji, nabywania, dostarczania, integracji, obsługi, utrzymywania, usuwania i wykorzystywania w inny sposób produktów oraz usług technologicznych lub zarządzania nimi. Interakcje te są kształtowane i podlegają wpływom technologii, przepisów prawa, obowiązujących polityk, procedur i praktyk.

  Biorąc pod uwagę złożone i wzajemnie powiązane relacje w tym ekosystemie, zarządzanie ryzykiem w łańcuchu dostaw (Supply Chain Risk Management, SCRM) ma kluczowe znaczenie dla każdej organizacji. Zarządzanie ryzykiem cyberbezpieczeństwa w łańcuchu dostaw (C-SCRM) to systematyczny proces służący do zarządzania narażenia na ryzyko cyberbezpieczeństwa w całym łańcuchu dostaw i opracowywania odpowiednich strategii reagowania, polityk, procesów i procedur. Podkategorie w ramach kategorii C-SCRM ram CSF [GV.SC] zapewniają połączenie

między wynikami, które koncentrują się wyłącznie na cyberbezpieczeństwie, a tymi, które koncentrują się na procesie C-SCRM. Publikacja specjalna SP 800-161r1 (wersja 1) – *Praktyki zarządzania ryzykiem cyberbezpieczeństwa w łańcuchu dostaw dla systemów i organizacji* zawiera szczegółowe informacje na temat C-SCRM.

- **Ryzyko związane z nowymi technologiami:** w miarę udostępniania nowych technologii oraz nowych zastosowań tych technologii, pojawiają się oczywiście nowe zagrożenia. Współczesnym przykładem jest sztuczna inteligencja (AI), która niesie ze sobą zagrożenia dla cyberbezpieczeństwa i prywatności, a także wiele innych rodzajów ryzyka. Opracowano ramy zarządzania ryzykiem sztucznej inteligencji wg NIST (NIST Artificial Intelligence Risk Management Framework, AI RMF), aby pomóc w radzeniu sobie z tymi zagrożeniami. Traktowanie ryzyka związanego ze sztuczną inteligencją wraz z innymi rodzajami ryzyka występującymi w przedsiębiorstwie (np. finansowym, związanym z cyberbezpieczeństwem, reputacją i ochroną prywatności) zapewni bardziej zintegrowane wyniki i efektywność organizacyjną. Zagadnienia i podejścia w ramach zarządzania ryzykiem związanym z cyberbezpieczeństwem i ochroną prywatności mają zastosowanie do projektowania, opracowywania, wdrażania, oceny i użytkowania systemów sztucznej inteligencji. Rdzeń AI RMF wykorzystuje funkcje, kategorie i podkategorie do opisania wyników sztucznej inteligencji i pomaga zarządzać ryzykiem związanym z AI.

Appendix A. Podstawa CSF

W niniejszym dodatku opisano funkcje, kategorie i podkategorie podstawy CSF. Tabela 1 zawiera listę nazw funkcji i kategorii podstawy ram CSF 2.0 oraz unikalne identyfikatory alfabetyczne. Każda nazwa funkcji w tabeli jest powiązana z odpowiednią częścią dodatku. Kolejność funkcji, kategorii i podkategorii podstawy nie jest alfabetyczna, gdyż ma najbardziej odpowiadać osobom odpowiedzialnym za wdrażanie zarządzania ryzykiem w organizacji. Numeracja podkategorii celowo nie jest sekwencyjna – luki w numeracji wskazują na podkategorie ram CSF 1.1, które zostały przeniesione do CSF 2.0.

Tabela 1. Nazwy i identyfikatory funkcji i kategorii podstawy ram CSF 2.0

Funkcja	Kategoria	Identyfikator kategorii
Nadzór (GV)	Kontekst organizacyjny	GV.OC
	Strategia zarządzania ryzykiem	GV.RM
	Role, obowiązki i uprawnienia	GV.RR
	Polityka	GV.PO
	Nadzór	GV.OV
	Zarządzanie ryzykiem cyberbezpieczeństwa w łańcuchu dostaw	GV.SC
Identyfikacja (ID)	Zarządzanie aktywami	ID.AM
	Ocena ryzyka	ID.RA
	Udoskonalanie	ID.IM
Ochrona (PR)	Zarządzanie identyfikacją, uwierzytelnianie i kontrola dostępu	PR.AA
	Świadomość i szkolenia	PR.AT
	Bezpieczeństwo danych	PR.DS
	Bezpieczeństwo platformy	PR.PS
	Odporność infrastruktury technologicznej	PR.IR
Wykrywanie (DE)	Ciągłe monitorowanie	DE.CM
	Analiza zdarzeń niepożądanych	DE.AE
Reagowanie (RS)	Zarządzanie incydentami	RS.MA
	Analiza incydentów	RS.AN
	Raportowanie i komunikacja w zakresie reagowania na incydenty	RS.CO
	Łagodzenie skutków incydentów	RS.MI
Przywracanie (RC)	Wykonanie planu przywracania operacji po incydencie	RC.RP
	Komunikacja w zakresie przywracania operacji po incydencie	RC.CO

Podstawa ram CSF, odniesienia informacyjne i przykłady wdrożeń są dostępne na stronie internetowej CSF 2.0 oraz za pośrednictwem narzędzia odniesienia CSF 2.0, które umożliwia użytkownikom ich eksplorację i eksportowanie w formatach nadających się do odczytu maszynowego i przez człowieka. Podstawa ram CSF 2.0 jest również dostępna w starszym formacie podobnym do CSF 1.1.

NADZÓR (GV): strategia, oczekiwania i polityka organizacji w zakresie zarządzania ryzykiem związanym z cyberbezpieczeństwem są ustanowione, komunikowane i monitorowane

- **Kontekst organizacyjny (GV.OC):** okoliczności – misja, oczekiwania interesariuszy, zależności oraz wymogi prawne, regulacyjne i umowne – otaczające decyzje organizacji dotyczące zarządzania ryzykiem cyberbezpieczeństwa są zrozumiałe.
  - **GV.OC-01:** misja organizacji jest zrozumiała i wpływa znacząco na zarządzanie ryzykiem cyberbezpieczeństwa.
  - **GV.OC-02:** interesariusze wewnętrzni i zewnętrzni są rozumiani, a ich potrzeby i oczekiwania dotyczące zarządzania ryzykiem cyberbezpieczeństwa są zrozumiałe i brane pod uwagę.
  - **GV.OC-03:** w ymogi prawne, regulacyjne i umowne w zakresie cyberbezpieczeństwa – w tym obowiązki dotyczące ochrony prywatności i swobód obywatelskich – są rozumiane i odpowiednio zarządzane.
  - **GV.OC-04:** krytyczne cele, możliwości i usługi, od których uzależnieni są interesariusze zewnętrzni lub których oczekują od organizacji, są zrozumiałe i odpowiednio komunikowane.
  - **GV.OC-05:** w yniki, możliwości i usługi, od których uzależnoiona jest organizacja, są zrozumiałe i odpowiednio komunikowane

- **Strategia zarządzania ryzykiem (GV.RM):** priorytety, ograniczenia, ryzyko tolerowane oraz założenia organizacji są ustalone, odpowiednio komunikowane i wykorzystywane do wspierania decyzji dotyczących ryzyka operacyjnego.
  - **GV.RM-01:** cele zarządzania ryzykiem są ustalone i uzgodnione przez interesariuszy organizacji.
  - **GV.RM-02:** deklaracje dotyczące ryzyka tolerowanego są opracowywane, odpowiednio komunikowane i utrzymywane.
  - **GV.RM-03:** działania i wyniki w zakresie zarządzania ryzykiem cyberbezpieczeństwa są uwzględnione w procesach zarządzania ryzykiem w przedsiębiorstwie.
  - **GV.RM-04:** ustanowiono i zakomunikowano kierunek strategiczny opisujący odpowiednie opcje reagowania na ryzyko.
  - **GV.RM-05:** w całej organizacji są ustanowiono linie komunikacji w zakresie ryzyka cyberbezpieczeństwa, w tym ryzyka ze strony dostawców i innych stron trzecich.
  - **GV.RM-06:** ustanowiono i zakomunikowano znormalizowaną metodę obliczania, dokumentowania, kategoryzowania i ustalania priorytetów w odniesieniu do zagrożeń dla cyberbezpieczeństwa.
  - **GV.RM-07:** worganizacyjnych dyskusjach na temat ryzyka cyberbezpieczeństwa określono i uwzględniono możliwości strategiczne (tj. ryzyko pozytywne).

- **Role, obowiązki i uprawnienia (GV.RR):** ustanowiono i zakomunikowano role, obowiązki i uprawnienia w zakresie cyberbezpieczeństwa w celu wspierania odpowiedzialności, oceny wyników i nieustannego udoskonalania.
  - **GV.RR-01**: przywództwo organizacji jest odpowiedzialne za ryzyko związane z cyberbezpieczeństwem i wspiera kulturę, która jest świadoma ryzyka, etyczna i stale się rozwija.
  - **GV.RR-02:** role, obowiązki i uprawnienia związane z zarządzaniem ryzykiem cyberbezpieczeństwa są ustanowione, odpowiednio komunikowane, zrozumiałe i egzekwowane.
  - **GV.RR-03:** przydzielane są odpowiednie zasoby współmierne do strategii ryzyka cyberbezpieczeństwa, ról, obowiązków i obowiązujących polityk.
  - **GV.RR-04:** cyberbezpieczeństwo jest uwzględnione w praktykach dotyczących zasobów ludzkich
- **Polityka (GV.PO):** w organizacji ustanowiono i zakomunikowano politykę cyberbezpieczeństwa, która jest egzekwowana.
  - **GV.PO-01:** w oparciu o kontekst organizacyjny, strategię cyberbezpieczeństwa i priorytety ustanowiono i zakomunikowano politykę zarządzania ryzykiem cyberbezpieczeństwa, która jest egzekwowana.
  - **GV.PO-02:** polityka zarządzania ryzykiem cyberbezpieczeństwa jest weryfikowana, aktualizowana, komunikowana i egzekwowana w celu odzwierciedlenia zmian w wymaganiach, zagrożeniach, technologii i misji organizacji.
- **Nadzór (GV.OV):** w yniki działań w zakresie zarządzania ryzykiem cyberbezpieczeństwa w całej organizacji są wykorzystywane do informowania, udoskonalania i dostosowywania strategii zarządzania ryzykiem.
  - **GV.OV-01:** w yniki strategii zarządzania ryzykiem cyberbezpieczeństwa są poddawane przeglądowi w celu informowania i dostosowywania strategii i kierunku.
  - **GV.OV-02:** strategia zarządzania ryzykiem cyberbezpieczeństwa jest poddawana przeglądom i dostosowywana w celu zapewnienia pokrycia wymagań organizacyjnych i ryzyka.
  - **GV.OV-03:** w yniki zarządzania ryzykiem cyberbezpieczeństwa w organizacji są oceniane i poddawane przeglądowi pod kątem koniecznych korekt.
- **Zarządzanie ryzykiem cyberbezpieczeństwa w łańcuchu dostaw (GV.SC):** procesy zarządzania ryzykiem cyberbezpieczeństwa w łańcuchu dostaw są identyfikowane, ustalane, zarządzane, monitorowane i udoskonalane przez interesariuszy organizacji.
  - **GV.SC-01:** program zarządzania ryzykiem cyberbezpieczeństwa w łańcuchu dostaw, strategia, cele, zasady i procesy są ustanawiane i uzgadniane przez interesariuszy organizacji.
  - **GV.SC-02:** role i obowiązki dostawców, klientów i partnerów w zakresie cyberbezpieczeństwa są ustalone, zakomunikowane i skoordynowane wewnątrz organizacji i poza nią.
  - **GV.SC-03:** zarządzanie ryzykiem cyberbezpieczeństwa w łańcuchu dostaw jest zintegrowane z zarządzaniem ryzykiem cyberbezpieczeństwa i przedsiębiorstwa, oceną ryzyka i procesami usprawnień.
  - **GV.SC-04:** dostawcy są znani i uszeregowani priorytetowo według poziomu ważności.

- **GV.SC-05:** w ymogi dotyczące ryzyka cyberbezpieczeństwa w łańcuchach dostaw są ustalane, uszeregowane priorytetowo i zintegrowane z kontraktami i innymi rodzajami umów z dostawcami oraz innymi odpowiednimi stronami trzecimi.
- **GV.SC-06:** przed nawiązaniem formalnych relacji z dostawcami lub innymi stronami trzecimi przeprowadza się planowanie i analizę należytej staranności (due diligence) w celu ograniczenia ryzyka.
- **GV.SC-07:** ryzyko stwarzane przez dostawcę, jego produkty i usługi oraz inne strony trzecie jest zrozumiałe, rejestrowane, uszeregowane priorytetowo, oceniane, uwzględniane i monitorowane w trakcie trwania relacji.
- **GV.SC-08:** odpowiedni dostawcy i inne strony trzecie są uwzględniani w planowaniu incydentów, reagowaniu na nie i działaniach naprawczych.
- **GV.SC-09:** praktyki w zakresie bezpieczeństwa łańcucha dostaw są zintegrowane z programami zarządzania ryzykiem cyberbezpieczeństwa i przedsiębiorstwa, a ich wydajność jest monitorowana przez cały cykl życia produktu technologicznego i usługi.
- **GV.SC-10:** plany zarządzania ryzykiem cyberbezpieczeństwa w łańcuchu dostaw obejmują postanowienia dotyczące działań podejmowanych po zawarciu umowy partnerskiej lub umowy o świadczenie usług.

IDENTYFIKACJA (ID): bieżące zagrożenia organizacji w zakresie cyberbezpieczeństwa organizacji są zrozumiałe.

- **Zarządzanie aktywami (ID.AM):** aktywa (np. dane, sprzęt, oprogramowanie, systemy, obiekty, usługi, ludzie), które umożliwiają organizacji osiąganie celów biznesowych, są identyfikowane i zarządzane zgodnie z ich względnym znaczeniem dla celów organizacyjnych i strategii ryzyka organizacji.
  - **ID.AM-01:** prowadzone są inwentaryzacje sprzętu zarządzanego przez organizację.
  - **ID.AM-02:** prowadzone są inwentaryzacje oprogramowania, usług i systemów zarządzanych przez organizację.
  - **ID.AM-03:** utrzymywane są reprezentacje uprawnionej komunikacji sieciowej w organizacji oraz wewnętrznych i zewnętrznych przepływów danych sieciowych.
  - **ID.AM-04:** utrzymywane są wykazy usług świadczonych przez dostawców.
  - **ID.AM-05:** aktywa są uszeregowane priorytetowo w oparciu o klasyfikację, poziom ważności, zasoby i wpływ na misję.
  - **ID.AM-07:** prowadzone są wykazy danych i odpowiadających im metadanych dla wyznaczonych typów danych.
  - **ID.AM-08:** systemy, sprzęt, oprogramowanie, usługi i dane są zarządzane przez cały ich cykl życia.
- **Ocena ryzyka (ID.RA):** ryzyko cyberbezpieczeństwa dla organizacji, aktywów i osób jest zrozumiałe dla organizacji.
  - **ID.RA-01:** słabe punkty w zasobach są identyfikowane, weryfikowane i rejestrowane.

- **ID.RA-02:** informacje o zagrożeniach cybernetycznych są uzyskiwane z forów i źródeł wymiany informacji.
- **ID.RA-03:** w ewnętrzne i zewnętrzne zagrożenia dla organizacji są identyfikowane i rejestrowane.
- **ID.RA-04:** sotencjalne skutki i prawdopodobieństwo wystąpienia zagrożeń wykorzystujących podatności są identyfikowane i rejestrowane.
- **ID.RA-05:** zagrożenia, słabe punkty, prawdopodobieństwa i skutki są wykorzystywane do zrozumienia nieodłącznego ryzyka oraz do informowania o priorytetyzacji w zakresie reagowania na ryzyko.
- **ID.RA-06:** reakcje na ryzyko są wybierane, uszeregowane priorytetowo, planowane, śledzone i komunikowane.
- **ID.RA-07:** zmiany i wyjątki są zarządzane, oceniane pod kątem wpływu na ryzyko, rejestrowane i śledzone.
- **ID.RA-08:** ustanowiono procesy otrzymywania, analizowania i reagowania na ujawnione luki w zabezpieczeniach.
- **ID.RA-09:** autentyczność i integralność sprzętu i oprogramowania są oceniane przed nabyciem i użyciem.
- **ID.RA-10:** krytyczni dostawcy są oceniani przed ich pozyskaniem.

- **Udoskonalenia (ID.IM):** udoskonalenia procesów, procedur i działań związanych z zarządzaniem ryzykiem cyberbezpieczeństwa są identyfikowane we wszystkich funkcjach ram CSF.
  - **ID.IM-01:** udoskonalenia są identyfikowane na podstawie ocen.
  - **ID.IM-02:** udoskonalenia są identyfikowane na podstawie testów bezpieczeństwa i ćwiczeń, w tym tych przeprowadzanych we współpracy z dostawcami i odpowiednimi stronami trzecimi.
  - **ID.IM-03:** udoskonalenia są identyfikowane na podstawie realizacji procesów operacyjnych, procedur i działań.
  - **ID.IM-04:** plany reagowania na incydenty oraz inne plany w zakresie cyberbezpieczeństwa, które mają wpływ na operacje, są ustanawiane, komunikowane, utrzymywane i udoskonalane.

OCHRONA (PR): stosowane są zabezpieczenia do zarządzania ryzykiem w zakresie cyberbezpieczeństwa organizacji.

- **Zarządzanie identyfikacją, uwierzytelnianie i kontrola dostępu (PR.AA):** dostęp do zasobów fizycznych i logicznych jest ograniczony do upoważnionych użytkowników, usług i sprzętu oraz zarządzany współmiernie do oszacowanego ryzyka uzyskania nieuprawnionego dostępu.
  - **PR.AA-01:** tożsamości i dane uwierzytelniające upoważnionych użytkowników, usług i sprzętu są zarządzane przez organizację.
  - **PR.AA-02:** tożsamości są potwierdzane i wiązane z poświadczeniami w oparciu o kontekst interakcji.
  - **PR.AA-03:** użytkownicy, usługi i sprzęt podlegają procesowi uwierzytelniania.

- **PR.AA-04:** potwierdzenia tożsamości są chronione, przekazywane i weryfikowane.
- **PR.AA-05:** uprawnienia dostępu, upoważnienia i autoryzacje są zdefiniowane w polityce, zarządzane, egzekwowane i weryfikowane; obejmują one zasady najmniejszych przywilejów i rozdziału obowiązków.
- **PR.AA-06:** dostęp fizyczny do zasobów jest zarządzany, monitorowany i egzekwowany proporcjonalnie do ryzyka.

- **Świadomość i szkolenia (PR.AT):** personel organizacji jest uświadamiany i szkolony w zakresie cyberbezpieczeństwa, aby móc wykonywać swoje zadania związane z cyberbezpieczeństwem.
  - **PR.AT-01:** personel jest uświadamiany i szkolony w taki sposób, by posiadać wiedzę i umiejętności umożliwiające wykonywanie ogólnych zadań z uwzględnieniem zagrożeń dla cyberbezpieczeństwa.
  - **PR.AT-02:** osoby pełniące specjalistyczne funkcje są uświadamiane i szkolone, w taki sposób, by zdobyły wiedzę i umiejętności umożliwiające wykonywanie odpowiednich zadań z uwzględnieniem zagrożeń dla cyberbezpieczeństwa.

- **Bezpieczeństwo danych (PR.DS):** dane są zarządzane zgodnie ze strategią ryzyka organizacji w celu ochrony poufności, integralności i dostępności informacji.
  - **PR.DS-01:** chroniona jest poufność, integralność i dostępność danych w stanie spoczynku.
  - **PR.DS-02:** chroniona jest poufność, integralność i dostępność danych w tranzycie.
  - **PR.DS-10:** chroniona jest poufność, integralność i dostępność danych w użyciu.
  - **PR.DS-11:** Kopie zapasowe danych są tworzone, chronione, utrzymywane i testowane.

- **Bezpieczeństwo platformy (PR.PS):** sprzęt, oprogramowanie (np. oprogramowanie układowe, systemy operacyjne, aplikacje) i usługi platform fizycznych i wirtualnych są zarządzane zgodnie ze strategią ryzyka organizacji w celu ochrony ich poufności, integralności i dostępności.
  - **PR.PS-01:** praktyki zarządzania konfiguracją są ustanowione i stosowane.
  - **PR.PS-02:** oprogramowanie jest utrzymywane, wymieniane i usuwane współmiernie do ryzyka.
  - **PR.PS-03:** sprzęt jest utrzymywany, wymieniany i usuwany współmiernie do ryzyka.
  - **PR.PS-04:** zapisy dziennika są generowane i udostępniane do ciągłego monitorowania.
  - **PR.PS-05:** uniemożliwiono instalację i uruchamianie nieautoryzowanego oprogramowania.
  - **PR.PS-06:** bezpieczne praktyki tworzenia oprogramowania są zintegrowane, a ich wydajność jest monitorowana przez cały cykl życia oprogramowania.

- **Odporność infrastruktury technologicznej (PR.IR):** architektury bezpieczeństwa są zarządzane zgodnie ze strategią ryzyka organizacji w celu ochrony poufności, integralności i dostępności zasobów oraz odporności organizacyjnej.
  - **PR.IR-01:** sieci i środowiska są chronione przed nieupoważnionym dostępem logicznym i użyciem.
  - **PR.IR-02:** zasoby technologiczne organizacji są chronione przed zagrożeniami środowiskowymi.

- **PR.IR-03:** w drażane są mechanizmy w celu osiągnięcia wymagań dotyczących odporności w sytuacjach normalnych i niekorzystnych.
- **PR.IR-04:** utrzymywana jest odpowiednia pojemność zasobów w celu zapewnienia dostępności

Wykrywanie (DE): możliwe ataki i naruszenia cyberbezpieczeństwa są wykrywane i analizowane.

- **Ciągłe monitorowanie (DE.CM):** zasoby są monitorowane w celu wykrycia anomalii, wskaźników naruszenia bezpieczeństwa oraz innych potencjalnie niepożądanych zdarzeń.
  - **DE.CM-01:** sieci i usługi sieciowe są monitorowane w celu wykrycia potencjalnie niepożądanych zdarzeń.
  - **DE.CM-02:** środowisko fizyczne jest monitorowane w celu wykrycia potencjalnie niepożądanych zdarzeń.
  - **DE.CM-03:** aktywność personelu i wykorzystanie technologii są monitorowane w celu wykrycia potencjalnie niepożądanych zdarzeń.
  - **DE.CM-06:** działania i usługi zewnętrznych dostawców usług są monitorowane w celu wykrycia potencjalnie niepożądanych zdarzeń.
  - **DE.CM-09:** sprzęt komputerowy i oprogramowanie, środowiska uruchomieniowe i ich dane są monitorowane w celu wykrycia potencjalnie niepożądanych zdarzeń.
- **Analiza zdarzeń niepożądanych (DE.AE):** anomalie, wskaźniki naruszenia bezpieczeństwa i inne potencjalnie niepożądane zdarzenia są analizowane w celu scharakteryzowania zdarzeń i wykrycia incydentów cyberbezpieczeństwa.
  - **DE.AE-02:** potencjalnie niepożądane zdarzenia są analizowane w celu lepszego zrozumienia powiązanych działań.
  - **DE.AE-03:** informacje są korelowane z wielu źródeł.
  - **DE.AE-04:** szacowany wpływ i zakres zdarzeń niepożądanych są dobrze rozumiane.
  - **DE.AE-06: i**nformacje o zdarzeniach niepożądanych są dostarczane upoważnionemu personelowi i narzędziom.
  - **DE.AE-07:** analiza zagrożeń cybernetycznych i inne informacje kontekstowe są włączone do analizy.
  - **DE.AE-08:** incydenty są zgłaszane, gdy zdarzenia niepożądane spełniają określone kryteria incydentu.

Reagowanie (RS): podejmowane są działania dotyczące wykrytego incydentu cyberbezpieczeństwa.

- **Zarządzanie incydentami (RS.MA):** zarządzane jest reagowanie na wykryte incydenty cyberbezpieczeństwa.
  - **RS.MA-01:** plan reagowania na incydenty jest realizowany w porozumieniu z odpowiednimi stronami trzecimi po zgłoszeniu incydentu.
  - **RS.MA-02:** zgłoszenia incydentów są segregowane i zatwierdzane.
  - **RS.MA-03:** incydenty są kategoryzowane i priorytetyzowane.
  - **RS.MA-04:** incydenty są wzmacniane lub podnoszone w zależności od potrzeb.
  - **RS.MA-05:** stosowane są kryteria inicjowania odzyskiwania incydentów.
- **Analiza incydentu (RS.AN):** prowadzone są dochodzenia w celu zapewnienia skutecznego reagowania i wspierania działań związanych z dochodzeniem i odzyskiwaniem danych.
  - **RS.AN-03:** przeprowadzana jest analiza w celu ustalenia, co miało miejsce podczas incydentu i jaka była jego pierwotna przyczyna.
  - **RS.AN-06:** działania wykonywane podczas dochodzenia są rejestrowane, a integralność i pochodzenie zapisów zostają zachowane.
  - **RS.AN-07:** dane i metadane dotyczące incydentu są gromadzone, a ich integralność i pochodzenie zostają zachowane.
  - **RS.AN-08:** w ielkość incydentu jest szacowana i weryfikowana.
- **Raportowanie i komunikacja w zakresie reagowania na incydenty (RS.CO):** działania w zakresie reagowania są koordynowane z wewnętrznymi i zewnętrznymi interesariuszami zgodnie z wymogami przepisów ustawowych i wykonawczych lub obowiązujących polityk.
  - **RS.CO-02: i**nteresariusze wewnętrzni i zewnętrzni są powiadamiani o incydentach.
  - **RS.CO-03: i**nformacje są udostępniane wyznaczonym interesariuszom wewnętrznym i zewnętrznym.
- **Łagodzenie skutków incydentów (RS.MI):** w ykonywane są działania mające na celu zapobieganie rozszerzaniu się zdarzenia i łagodzenie jego skutków.
  - **RS.MI-01: i**ncydenty są ograniczane.
  - **RS.MI-02: i**ncydenty są eliminowane.

PRZYWRACANIE (RC): przywracane są aktywa i operacje , na które niekorzystnie wpłynął incydent związany z cyberbezpieczeństwem.

- **Wykonanie planu przywracania operacji po incydencie (RC.RP):** działania przywracania są wykonywane w celu zapewnienia dostępności operacyjnej systemów i usług , na które niekorzystnie wpłynął incydent związany z cyberbezpieczeństwem.
  - **RC.RP-01:** część planu reagowania na incydenty dotycząca odzyskiwania danych jest wykonywana po zainicjowaniu procesu reagowania na incydenty.

- **RC.RP-02:** działania naprawcze są wybierane, określane, priorytetyzowane i wykonywane.
- **RC.RP-03:** integralność kopii zapasowych i innych zasobów przywracania jest weryfikowana przed użyciem ich do przywracania operacji.
- **RC.RP-04:** krytyczne funkcje misji i zarządzanie ryzykiem cyberbezpieczeństwa są brane pod uwagę przy ustanawianiu norm operacyjnych po wystąpieniu incydentu.
- **RC.RP-05:** integralność przywróconych zasobów jest weryfikowana, systemy i usługi są przywracane, a normalny stan operacyjny zostaje potwierdzony.
- **RC.RP-06:** koniec usuwania skutków incydentu jest ogłoszony w oparciu o kryteria, a dokumentacja związana z incydentem zostaje uzupełniona.

- **Komunikacja związana z usuwaniem skutków incydentu (RC.CO):** działania naprawcze są koordynowane z podmiotami wewnętrznymi i zewnętrznymi.
  - **RC.CO-03:** działania naprawcze i postępy w przywracaniu zdolności operacyjnych są przekazywane wyznaczonym interesariuszom wewnętrznym i zewnętrznym.
  - **RC.CO-04:** aktualizacje dotyczące usuwania skutków incydentu są udostępniane do wiadomości publicznej przy użyciu zatwierdzonych metod i komunikatów.

Appendix B. Poziomy CSF

Tabela 2 zawiera hipotetyczną ilustrację poziomów CSF omówionych w części 3. Poszczególne poziomy wdrożeń określają rygor praktyk nadzoru nad ryzykiem cyberbezpieczeństwa w organizacji (Nadzór) oraz praktyk zarządzania ryzykiem cyberbezpieczeństwa (Identyfikacja, Ochrona, Wykrywanie, Reagowanie i Przywracanie).

Tabela 2. Przykładowa ilustracja poziomów CSF

Poziom	Nadzór nad ryzykiem cyberbezpieczeństwa	Zarządzanie ryzykiem cyberbezpieczeństwa
Poziom 1: wdrożenie częściowe	Stosowanie organizacyjnej strategii w zakresie cyberbezpieczeństwa jest zarządzane w sposób doraźny. Ustalanie priorytetów ma charakter doraźny i nie jest formalnie oparte na celach ani na środowisku zagrożeń.	Świadomość zagrożeń cyberbezpieczeństwa na poziomie organizacyjnym jest ograniczona. Organizacja wdraża zarządzanie ryzykiem cyberbezpieczeństwa w sposób nieregularny, indywidualnie w każdym przypadku. Organizacja może nie dysponować procesami umożliwiającymi wewnętrzną wymianę informacji dotyczących cyberbezpieczeństwa. Organizacja jest ogólnie nieświadoma zagrożeń w zakresie cyberbezpieczeństwa związanych z jej dostawcami oraz produktami i usługami, które nabywa i z których korzysta.
Poziom 2: wdrożenie świadome ryzyka	Praktyki zarządzania ryzykiem są zatwierdzone przez kierownictwo, ale mogą nie być ustanowione jako polityka całej organizacji. Priorytetyzacja działań w zakresie cyberbezpieczeństwa i potrzeb w zakresie ochrony jest bezpośrednio oparta na celach ryzyka organizacyjnego, środowisku zagrożeń lub wymaganiach biznesowych i misji.	Istnieje świadomość zagrożeń związanych z cyberbezpieczeństwem na poziomie organizacyjnym, ale nie ustalono kompleksowego wewnętrznego podejścia do zarządzania nimi. Uwzględnienie cyberbezpieczeństwa w celach i programach organizacyjnych może mieć miejsce na niektórych, ale nie na wszystkich poziomach organizacji. Ocena ryzyka cyberbezpieczeństwa dla aktywów organizacyjnych i zewnętrznych ma miejsce, ale zazwyczaj nie jest powtarzalna ani cykliczna. Informacje dotyczące cyberbezpieczeństwa są udostępniane w organizacji w sposób nieformalny. Organizacja jest świadoma zagrożeń w zakresie cyberbezpieczeństwa związanych z jej dostawcami oraz produktami i usługami, które nabywa i z których korzysta, ale nie działa konsekwentnie ani formalnie w celu reagowania na te zagrożenia.

Poziom	Nadzór nad ryzykiem cyberbezpieczeństwa	Zarządzanie ryzykiem cyberbezpieczeństwa
Poziom 3: wdrożenie zaawansowane/ powtarzalne	Praktyki zarządzania ryzykiem w organizacji są formalnie zatwierdzone i przedstawione w formie polityki. Polityki, procesy i procedury uwzględniające ryzyko są definiowane, wdrażane zgodnie z założeniami i poddawane przeglądom. Praktyki organizacji w zakresie cyberbezpieczeństwa są regularnie aktualizowane w oparciu o zastosowanie procesów zarządzania ryzykiem w kontekście zmian w wymaganiach biznesowych/misji, zagrożeniach i środowisku technologicznym.	W organizacji istnieje kompleksowe wewnętrzne podejście do zarządzania ryzykiem cyberbezpieczeństwa. Informacje dotyczące cyberbezpieczeństwa są rutynowo udostępniane w całej organizacji. Istnieją spójne metody skutecznego reagowania ze względu na zmiany ryzyka. Personel dysponuje wiedzą i umiejętnościami niezbędnymi do pełnienia wyznaczonych ról i obowiązków. Organizacja konsekwentnie i dokładnie monitoruje ryzyko związane z cyberbezpieczeństwem aktywów. Kadra zarządzająca odpowiedzialna za cyberbezpieczeństwo oraz kadra zarządzająca niezwiązana z cyberbezpieczeństwem regularnie komunikują się w sprawie zagrożeń dla cyberbezpieczeństwa. Kadra zarządzająca zapewnia, że cyberbezpieczeństwo jest brane pod uwagę na wszystkich liniach operacyjnych w organizacji. Strategia ryzyka organizacji uwzględnia ryzyko cyberbezpieczeństwa związane z jej dostawcami oraz produktami i usługami, które nabywa i z których korzysta. Personel formalnie działa w oparciu o te zagrożenia poprzez określone mechanizmy, takie jak pisemne umowy służące przekazywaniu podstawowych wymagań, struktury zarządzania (np. rady ds. ryzyka) oraz wdrażanie i monitorowanie polityki. Działania te są wdrażane konsekwentnie i zgodnie z zamierzeniami, są też na bieżąco monitorowane i poddawane przeglądom.

Poziom	Nadzór nad ryzykiem cyberbezpieczeństwa	Zarządzanie ryzykiem cyberbezpieczeństwa
Poziom 4: Wdrożenie adaptacyjne	W całej organizacji istnieje kompleksowe podejście do zarządzania ryzykiem związanym z cyberbezpieczeństwem, które wykorzystuje polityki, procesy i procedury oparte na analizie ryzyka w celu reagowania na potencjalne zdarzenia w zakresie cyberbezpieczeństwa. Związek między zagrożeniami dla cyberbezpieczeństwa a celami organizacyjnymi jest zrozumiały i brany pod uwagę przy podejmowaniu decyzji. Kadra zarządzająca monitoruje zagrożenia w zakresie cyberbezpieczeństwa w tym samym kontekście, co zagrożenia finansowe i inne zagrożenia w danej organizacji. Budżet organizacji opiera się na zrozumieniu obecnego i przewidywanego środowiska ryzyka oraz na tolerancji ryzyka. Jednostki biznesowe wdrażają wizję zarządu i analizują ryzyko na poziomie systemu w kontekście tolerancji ryzyka organizacyjnego. Zarządzanie ryzykiem cyberbezpieczeństwa stanowi część kultury korporacyjnej. Ewoluuje ze świadomości poprzednich działań i ciągłej świadomości działań w systemach i sieciach organizacyjnych. Organizacja może szybko i skutecznie uwzględniać zmiany w celach biznesowych / misji w sposobie podejścia do ryzyka i informowania o nim.	Organizacja dostosowuje swoje praktyki w zakresie cyberbezpieczeństwa w oparciu o poprzednie i bieżące działania w tym zakresie, w tym o wyciągnięte wnioski i wskaźniki prognostyczne. Poprzez proces nieustannego udoskonalania, który obejmuje zaawansowane technologie i praktyki w zakresie cyberbezpieczeństwa, organizacja aktywnie dostosowuje się do zmieniającego się środowiska technologicznego oraz reaguje szybko i skutecznie na ewoluujące, zaawansowane zagrożenia. Organizacja wykorzystuje informacje w czasie rzeczywistym lub zbliżonym do rzeczywistego, aby zrozumieć i konsekwentnie reagować na zagrożenia dla cyberbezpieczeństwa związane z jej dostawcami oraz produktami i usługami, które nabywa i z których korzysta. Informacje dotyczące cyberbezpieczeństwa są na bieżąco dostępniane w całej organizacji oraz upoważnionym stronom trzecim.

Appendix C. Słownik pojęć

Kategoria CSF
Grupa powiązanych wyników związanych z cyberbezpieczeństwem, które wspólnie składają się na funkcję ram CSF.

Profil społeczności CSF
Baza wyników CSF, którą się tworzy i publikuje w celu uwzględnienia wspólnych interesów i celów wielu organizacji. Profil społeczności jest zazwyczaj opracowywany dla określonego sektora, podsektora, technologii, typu zagrożenia lub innego przypadku użycia. Organizacja może użyć profilu społeczności jako podstawy do stworzenia własnego profilu docelowego.

Podstawa CSF
Taksonomia wyników w zakresie cyberbezpieczeństwa na wysokim poziomie, które mogą pomóc każdej organizacji w zarządzaniu ryzykiem związanym z cyberbezpieczeństwem. Elementy y wchodzące w skład podstawy ram CSF to hierarchia funkcji, kategorii i podkategorii, które opisują szczegółowo każdy wynik.

Profil bieżący CSF
Część profilu organizacyjnego określająca wyniki w zakresie podstawy, które organizacja obecnie osiąga (lub próbuje osiągnąć), i charakteryzujący, w jaki sposób lub w jakim stopniu osiągany jest każdy wynik.

Funkcja ram CSF
Najwyższy poziom organizacji pod względem wyników w zakresie cyberbezpieczeństwa. Istnieje sześć funkcji CSF: Nadzór, Identyfikacja, Ochrona, Wykrywanie, Reagowanie i Przywracanie.

Przykład wdrożenia ram CSF
Zwięzła, zorientowana na działanie, hipotetyczna ilustracja sposobu, w jaki można pomóc w osiągnięciu wyniku podstawy CSF.

Odniesienie informacyjne CSF
Mapowanie wskazujące na związek między wynikiem podstawy CSF a istniejącą normą, wytyczną, regulacją lub inną treścią.

Profil organizacyjny CSF
Mechanizm, który opisuje aktualny i/lub docelowy stan cyberbezpieczeństwa danej organizacji w kontekście wyników określonych w Podstawie ram CSF.

Przewodnik po szybkim wdrażaniu CSF
Dodatkowy zasób, który zawiera krótkie, praktyczne wskazówki dotyczące konkretnych tematów związanych z ramami CSF.

Podkategoria CSF
Grupa bardziej szczegółowych wyników działań technicznych i zarządczych w zakresie cyberbezpieczeństwa, które składają się na kategorię CSF.

Profil docelowy CSF
Część profilu organizacyjnego, która określa pożądane wyniki podstawy, które organizacja wybrała i uszeregowała pod względem ważności, aby osiągnąć swoje cele w zakresie zarządzania ryzykiem cyberbezpieczeństwa.

Poziomy CSF
Charakterystyka rygoru praktyk w zakresie nadzoru nad ryzykiem cyberbezpieczeństwa i zarządzania ryzykiem cyberbezpieczeństwa w danej organizacji. Istnieją cztery poziomy wdrożenia: wdrożenie częściowe (poziom 1), wdrożenie świadome ryzyka (poziom 2), wdrożenie zaawansowane/powtarzalne (poziom 3) oraz wdrożenie adaptacyjne (poziom 4).

Niektóre komercyjne urządzenia, instrumenty, oprogramowanie lub materiały – komercyjne lub niekomercyjne – zostały zidentyfikowane w tym dokumencie w celu właściwego określenia procedury eksperymentalnej. Taka identyfikacja nie oznacza rekomendacji ani poparcia instytutu NIST dla jakiegokolwiek produktu lub usługi, nie oznacza też, że zidentyfikowane materiały lub sprzęt są z założenia najlepszymi dostępnymi rozwiązaniami do danego celu.

Zasady NIST dotyczące serii technicznych
Prawa autorskie, użytkowanie i oświadczenia licencyjne
Składnia identyfikatora publikacji NIST z serii technicznych

Jak cytować tę publikację NIST z serii technicznych:
Ramy cyberbezpieczeństwa wg NIST (CSF) 2.0 (2024 r.)(ang. National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0.) (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 pol. https://doi.org/10.6028/NIST.CSWP.29.pol

Dane do kontaktu
cyberframework@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899–2000

Wszystkie komentarze są udostępniane zgodnie z ustawą o wolności informacji (Freedom of Information Act, FOIAFOIA).