Ramy Usprawniania Cyberbezpieczeństwa Krytycznej Infrastruktury

Wersja 1.0

Narodowy Instytut ds. Norm i Technologii

12 Lutego, 2014

Spis treści

Lista ilustracji

Lista tabel

Podsumowanie Wykonawcze

Bezpieczeństwo krajowe i gospodarcze Stanów Zjednoczonych zależy od niezawodnego funkcjonowania krytycznej infrastruktury. Zagrożenia cyberbezpieczeństwa wykorzystują większą złożoność i łączność krytycznych systemów infrastrukturalnych, stanowiąc ryzyko dla bezpieczeństwa kraju, gospodarki, bezpieczeństwa i zdrowia publicznego. Podobnie jak w przypadku zagrożeń finansowych i wizerunkowych, ryzyko związane z cyberbezpieczeństwem wpływa na podstawy przedsiębiorstwa. Może podnosić koszty i wpływać na przychody. Może narazić możliwości organizacji w zakresie innowacyjności, pozyskiwania i utrzymania klientów.

Aby lepiej odnieść się do tego typu zagrożeń, 12 lutego 2013 roku prezydent wydał Dekret 13636 „Poprawa Cyberbezpieczeństwa Krytycznej Infrastruktury", który stanowi, że „strategią Stanów Zjednoczonych jest poprawa bezpieczeństwa i wytrzymałości krytycznej infrastruktury kraju oraz utrzymanie środowiska cybernetycznego, które zachęcać będzie do wydajności, innowacyjności i dobrobytu ekonomicznego, promując jednocześnie bezpieczeństwo, ochronę, poufność handlową, prywatność i wolności obywatelskie". W odniesieniu do egzekwowania tej strategii Dekret wzywa do opracowania dobrowolnych Ram Cyberbezpieczeństwa na podstawie ryzyka – zbioru norm i najlepszych praktyk przemysłowych, by pomóc organizacjom zarządzać zagrożeniami związanymi z cyberbezpieczeństwem. Wynikające z tego Ramy, utworzone w drodze współpracy pomiędzy rządem, a sektorem prywatnym, stosują wspólną terminologię w zakresie zarządzania ryzykiem związanym z cyberbezpieczeństwem w sposób wydajny pod względem kosztów na podstawie potrzeb handlowych bez nakładania na firmy dodatkowych wymogów ustawowych.

Ramy skupiają się na wykorzystaniu stymulantów działalności, by prowadzić działania związane z cyberbezpieczeństwem, traktując zagrożenia cybernetyczne jako część procesu zarządzania ryzykiem w organizacji. Ramy składają się z trzech części: Rdzenia Ram, Profilu Ram i Poziomu Wdrożeń Ram. Rdzeń Ram jest zbiorem czynności dotyczących cyberbezpieczeństwa, wyników i odniesień informacyjnych obowiązującychwe wszystkich sektorach, w których obecna jest krytyczna infrastruktura, zapewniając szczegółowe wytyczne dla opracowania poszczególnych Profilów organizacyjnych. Dzięki użyciu Profilów, Ramy pomogą organizacji ustawić swoje czynności związane z cyberbezpieczeństwem względem wymogów działalności, tolerancji ryzyka i zasobów. Poziomy zapewniają organizacji mechanizm kontroli i zrozumienia cech swojego podejścia do zarządzania zagrożeniami cybernetycznymi.

Dekret wymaga również tego, aby Ramy zawierały metodologię ochrony prywatności osób i wolności obywatelskich, na wypadek wykonywania przez organizacje wykorzystujące krytyczną infrastrukturę działań związanych z cyberbezpieczeństwem. Ponieważ procesy i istniejące potrzeby będą się różniły, Ramy mogą wspomóc organizacjom we wdrażaniu prywatności i wolności obywatelskich jako część kompleksowego programu cyberbezpieczeństwa.

Ramy umożliwiają organizacjom – bez względu na wielkość, stopień ryzyka cyberbezpieczeństwa lub jego wyrafinowania– stosowanie zasad i najlepszych praktyk zarządzania ryzykiem, by poprawić bezpieczeństwo i wytrzymałość krytycznej infrastruktury. Ramy zapewniają organizację i strukturę wielostronnego podejścia do cyberbezpieczeństwa, opracowując normy, wytyczne i praktyki, które z powodzeniem sprawdzają się w dzisiejszym przemyśle. Ponadto, ponieważ odnoszą się do globalnie uznanych norm w zakresie cyberbezpieczeństwa, Ramy mogą być również

stosowane przez organizacje znajdujące się poza Stanami Zjednoczonymi i mogą służyć jako model międzynarodowej współpracy w zakresie wzmacniania cyberbezpieczeństwa krytycznej infrastruktury.

Ramy nie zapewniają uniwersalnego podejścia do zarządzania zagrożeniami cybernetycznymi krytycznej infrastruktury. Organizacje zawsze będą wystawione na specyficzne ryzyko – różne zagrożenia, słabości, tolerancje ryzyka – a oprócz tego sposób, w jaki będą wdrażać praktyki wynikające z Ram, będzie się różnić. Organizacje mogą wyznaczyć działania, które są istotne podczas zapewnienia krytycznych usług, i mogą priorytetyzować inwestycje, aby zmaksymalizować dochód z każdego wydanego dolara. Ostatecznym celem Ram jest ograniczenie i lepsze zarządzanie zagrożeniami cybernetycznymi.

Ramy to żyjący dokument, który jest przez cały czas aktualizowany i poprawiany w miarę otrzymywania sygnałów zwrotnych wynikających z wdrożeń. W miarę wdrażania Ram, uzyskane doświadczenia zostaną włączone do przyszłych wersji. Zapewni to spełnienie potrzeb właścicieli krytycznej infrastruktury i jej operatorów działających w dynamicznym i wymagającym środowisku nowych zagrożeń, ryzyka i rozwiązań.

Stosowanie niniejszych dobrowolnych Ram stanowi kolejny etap poprawy cyberbezpieczeństwa krytycznej infrastruktury naszego kraju – zapewniając wytyczne dla poszczególnych organizacji, przy zwiększeniu wytrzymałości ogółu cyberbezpieczeństwa krytycznej infrastruktury kraju.

1.0 Wprowadzenie do Ram

Bezpieczeństwo krajowe i gospodarcze Stanów Zjednoczonych jest zależne od niezawodnego funkcjonowania krytycznej infrastruktury. Aby zwiększyć wytrzymałość tego typu infrastruktury, 12 lutego 2013[1] prezydent Obama wydał Dekret 13636 (D) „Poprawa Cyberbezpieczeństwa Krytycznej Infrastruktury". Dekret nawołuje do opracowania dobrowolnych Ram Cyberbezpieczeństwa („Ramy") zapewniających „hierarchiczne, elastyczne, powtarzalne, oparte na wynikach i wydajne podejście" zarządzanie zagrożeniami cybernetycznymi w odniesieniu do tych procesów, informacji i systemów, które są bezpośrednio zaangażowane w realizację usług krytycznej infrastruktury. Ramy opracowane we współpracy z przemysłem zapewniają organizacji wytyczne w zakresie zarządzania zagrożeniami cybernetycznymi.

Krytyczna infrastruktura zdefiniowana jest w D jako „systemy i aktywa, fizyczne lub wirtualne, tak istotne dla Stanów Zjednoczonych, że niewydolność lub zniszczenie takich systemów i aktywów miałoby negatywny wpływ na bezpieczeństwo, bezpieczeństwo ekonomiczne kraju, zdrowie i bezpieczeństwo publiczne lub ich kombinacje". Z uwagi na rosnącą presję zagrożeń zewnętrznych i wewnętrznych, organizacje odpowiedzialne za krytyczną infrastrukturę muszą mieć spójne i iteracyjne podejście do identyfikacji, oceny i zarządzania zagrożeniami cybernetycznymi. Podejście to jest konieczne niezależnie od wielkości organizacji, narażenia na zagrożenia lub zaawansowania dzisiejszego cyberbezpieczeństwa.

Społeczność infrastruktury krytycznej obejmuje właścicieli publicznych i prywatnych oraz operatorów i inne jednostki pełniące rolę podczas zabezpieczania krajowej infrastruktury. Członkowie każdego sektora krytycznej infrastruktury pełnią funkcje wspomagane przez technologie informacyjne (ang. information technology – IT) i systemy sterowania przemysłowego (ang. industrial control system – ICS)[2]. Zależność tego typu od technologii, komunikacji i wzajemnych połączeń IT i ICS zmieniło się, poszerzyło zakres potencjalnych słabości i zwiększyło potencjalne ryzyko operacji. Na przykład, w miarę jak ICS i dane wygenerowane podczas operacji ICS wykorzystywane są w coraz większym zakresie, w celu zapewnienia krytycznych usług i podjęcia decyzji dotyczących działalności rozważyć należy potencjalny wpływ incydentu związanego z cyberbezpieczeństwem na działalność organizacji, aktywa, zdrowie i bezpieczeństwo ludzi i środowisko. Aby umożliwić zarządzanie zagrożeniami związanymi z cyberbezpieczeństwem, wymagane jest wyraźne zrozumienie stymulantów działalności i uwarunkowań dotyczących bezpieczeństwa, charakterystycznych dla wykorzystania IT i ICS. Ponieważ ryzyko w każdej z organizacji jest inne, wraz z IT i ICS zmieniać się będą również narzędzia i metody stosowane dla uzyskania wyników opisanych w Ramach.

Rozpoznając rolę, jaką odgrywa ochrona prywatności i swobód obywatelskich w procesie tworzenia większego zaufania publicznego, Dekret wymaga, aby Ramy obejmowały metodologię ochrony prywatności osób i wolności obywatelskich, w czasie realizacji przez organizacje infrastruktury krytycznej czynności związanych z cyberbezpieczeństwem. Wiele organizacji wdrożyło już procesy odnoszące się do prywatności i wolności obywatelskich. Zaprojektowana została metodologia uzupełniająca takie procesy i zapewniająca wytyczne ułatwiające zarządzaniem ryzyka względem prywatności w sposób spójny z podejściem organizacji do zarządzania zagrożeniami cybernetycznymi. Integrowanie prywatności i cyberbezpieczeństwa może przydać się organizacjom, zwiększając zaufanie klienta, umożliwiając bardziej znormalizowaną wymianę informacji i upraszczając operacje pomiędzy różnymi schematami prawnymi.

---

[1] Dekret nr 13636. *Poprawa Cyberbezpieczeństwa Krytycznej Infrastruktury*, DCPD-201300091, 12 lutego 2013. http:/Avvvvv.gDQ.gov/fdsvs/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[2] Program Krytycznej Infrastruktury DHS zapewnia listę sektorów i powiązanych z nimi krytycznych funkcji i łańcuchów wartości. http://www.dhs.gov/critical-infrastructure-sectors

Aby zapewnić możliwość rozszerzenia i umożliwić innowacje techniczne, Ramy są neutralne pod względem technologii. Ramy wykorzystują różnego rodzaju istniejące normy, wytyczne i praktyki, by umożliwić osiągnięcie wytrzymałości przez dostawców usług krytycznych. Polegając na tego typu globalnych normach, wytycznych i praktykach opracowanych, zarządzanych i aktualizowanych przez przemysł, dostępne narzędzia i metody dla osiągnięcia wyników Ram będą przekraczać granice, potwierdzając globalny charakter zagrożeń cybernetycznych i ewoluując wraz z postępem technicznym i wymogami działalności. Stosowanie istniejących i nowych norm umożliwi wykorzystanie ekonomii skali i stymulować będzie rozwój realnych produktów, usług i praktyk, spełniających zidentyfikowane potrzeby rynku. Konkurencja rynkowa promuje również szybszą dyfuzję tego typu technologii i praktyk i wdrożenie wielu korzyści przez interesariuszy w tych sektorach.

Budowanie na podstawie takich norm, wytycznych i praktyk sprawia, że Ramy zapewniają organizacjom wspólną taksonomię i mechanizm, w celu:

1) Opisywania ich obecnej postawy w zakresie cyberbezpieczeństwa;
2) Opisywania ich docelowego stanu w zakresie cyberbezpieczeństwa;
3) Identyfikowania i priorytetyzowania szans doskonalenia w kontekście ciągłego i powtarzalnego procesu;
4) Oceny postępu w stronę stanu docelowego;
5) Komunikacji z wewnętrznymi i zewnętrznymi interesariuszami w kwestiach ryzyka związanego z cyberbezpieczeństwem.

Ramy uzupełniają, a nie zastępują procesu zarządzania ryzykiem i programu cyberbezpieczeństwa w organizacji. Organizacja może wykorzystywać swoje obecne procesy i Ramy do zidentyfikowania możliwości wzmocnienia i przekazywać swojemu zarządowi informacje dotyczące zagrożeń cybernetycznych, dostosowując jednocześnie praktyki przemysłowe. Alternatywnie organizacja nieposiadająca istniejącego programu cyberbezpieczeństwa może wykorzystywać Ramy jako punkt odniesienia dla jego powołania.

Tak jak Ramy nie są dedykowane dla danej gałęzi przemysłu, tak samo ogólna taksonomia standardów, wytycznych i praktyk, które zapewniają, nie są określone dla jednego kraju. Organizacje spoza Stanów Zjednoczonych również mogą stosować Ramy dla wzmocnienia swoich wysiłków związanych z cyberbezpieczeństwem, a Ramy mogą przyczynić się do opracowania wspólnej terminologii stosowanej podczas międzynarodowej współpracy w zakresie cyberbezpieczeństwa krytycznej infrastruktury.

1.1 Informacje ogólne na temat Ram

Ramy stanowią podejście na bazie ryzyka dotyczące zarządzania zagrożeniami cybernetycznymi i składają się z trzech części: Rdzenia Ram, Poziomów Wdrożeń Ram i Profilów Ram. Każdy komponent Ram wzmacnia połączenie pomiędzy stymulatorami działań, a czynnościami związanymi z cyberbezpieczeństwem.
Komponenty są objaśnione poniżej.

- *Rdzeń Ram* to zbiór czynności związanych z cyberbezpieczeństwem, pożądanych wyników i możliwych do zastosowania odniesień, które są wspólne pośród sektorów krytycznej infrastruktury. Rdzeń przedstawia normy przemysłowe, wytyczne i praktyki w sposób umożliwiający komunikowanie czynności związanych z cyberbezpieczeństwem i wyników w organizacji od poziomu wykonawczego po poziom wdrożeń / operacyjny. Rdzeń Ram składa się z pięciu jednoczesnych i ciągłych Funkcji – Identyfikacja, Ochrona, Detekcja, Reagowanie, Przywracanie. Rozważane wspólnie Funkcje te zapewniają ogólny strategiczny ogląd cyklu życia zarządzania ryzykiem związanym z cyberbezpieczeństwem w organizacji. Rdzeń Ram następnie

identyfikuje główne kluczowe Kategorie i Podkategorie dla każdej z Funkcji i dopasowuje je do przykładowych Referencji Informacyjnych, na przykład istniejących norm, wytycznych i praktyk dla każdej spośród Podkategorii.

- *Poziomy Wdrożeń Ram* („Poziomy") zapewniają kontekst tego, w jaki sposób organizacja widzi zagrożenia cybernetyczne i procesy zarządzania takim ryzykiem. Poziomy opisują stopień, w jakim praktyki zarządzania ryzykiem związanym z cyberbezpieczeństwem wykazują charakterystykę zdefiniowaną w Ramach (np. świadome, powtarzalne i adaptacyjne ryzyko i zagrożenia). Poziomy charakteryzują praktyki organizacyjne w określonym zakresie od Częściowych (Poziom 1) po Adaptacyjne (Poziom 4). Poziomy te odzwierciedlają rozwój od nieformalnych reakcji reaktywnych po podejścia skuteczne i świadome ryzyka. W trakcie procesu wyboru Poziomu, organizacja powinna rozważyć swoje obecne praktyki zarządzania ryzykiem, środowisko zagrożeń, wymagania prawne i ustawowe, cele biznesowe / misję oraz ograniczenia organizacyjne.
- *Profil Ram* ("Profil") reprezentuje wyniki na podstawie potrzeb działalności wybrane przez organizację spośród Kategorii i Podkategorii Ram. Profil scharakteryzować można jako dostosowanie norm, wytycznych i praktyk do Rdzenia Ram w określonym scenariuszu wdrożeniowym. Proces ten wykorzystać można do zidentyfikowania szans poprawy stanu cyberbezpieczeństwa, porównując „Obecny" Profil (stan „jak jest") z Profilem „Docelowym" (stan „ma być"). Aby opracować Profil, organizacja może przeanalizować wszystkie Kategorie i Podkategorie i, na podstawie stymulantów działalności i oceny ryzyka, określić to, które są najistotniejsze; mogą one, w miarę potrzeb, wprowadzać Kategorie i Podkategorie, by odnieść się do zagrożeń organizacji. Profil Obecny można następnie wykorzystać dla wsparcia priorytetyzacji i pomiaru postępów w kierunku Profilu Docelowego, pośrednicząc jednocześnie w innych potrzebach biznesowych, takich jak wydajność kosztowa i innowacyjność. Profile wykorzystać można do przeprowadzenia samooceny i przekazywania informacji w lub pomiędzy organizacjami.

1.2 Zarządzanie Ryzykiem i Ramy Cyberbezpieczeństwa

Zarządzanie ryzykiem to ciągły proces identyfikacji, oceny i reagowania na ryzyko. Aby zarządzać ryzykiem, organizacje powinny zrozumieć prawdopodobieństwo tego, że zdarzenie się wydarzy oraz jego wpływ. Dzięki takim informacjom organizacje mogą wyznaczyć dopuszczalny poziom ryzyka dla dostawy usług i mogą wyrazić to w postaci swojej tolerancji ryzyka.

Rozumiejąc ryzyko tolerancji, organizacje mogą priorytetyzować czynności związane z cyberbezpieczeństwem, umożliwiając organizacjom podejmowanie świadomych decyzji na temat wydatków związanych z cyberbezpieczeństwem. Wdrożenie programów zarządzania ryzykiem oferuje organizacjom możliwość pomiaru i komunikacji dostrojeń programów cyberbezpieczeństwa. Organizacje mogą radzić sobie z ryzykiem na różne sposoby łącznie z minimalizacją ryzyka, przenoszeniem ryzyka, unikaniem ryzyka lub akceptowaniem ryzyka w zależności od jego potencjalnego wpływu na dostawę krytycznych usług.

Ramy wykorzystują procesy zarządzania ryzykiem, by umożliwić organizacjom przekazywanie i priorytetyzowanie decyzji dotyczących cyberbezpieczeństwa. Obejmują one ocenę nawracającego ryzyka i walidację stymulantów działalności, aby pomóc organizacjom wybrać docelowe stany czynności cyberbezpieczeństwa odzwierciedlające wymagane wyniki. Tym samym Ramy zapewniają organizacjom możliwość dynamicznego wyboru i bezpośredniego doskonalenia w zakresie zarządzania zagrożeniami cybernetycznymi w środowiskach IT i ICS.

Ramy są adaptacyjne i zapewniają elastyczne wdrożenie na bazie ryzyka, którą stosować można w szerokim spektrum procesów zarządzania ryzykiem dotyczącym cyberbezpieczeństwa. Przykłady procesów zarządzania ryzykiem cybernetycznym obejmują normę Międzynarodowej Organizacji Normalizacyjnej (ang. International Organization for Standardization – ISO) 31000:2009[3], ISO/IEC 27005:2011[4], Narodowego Instytutu Standaryzacji i Technologii (ang. National Institute of Standards and Technology – NIST) Specjalna Publikacja (SP) 800-39[5], i wytyczne dotyczące *Procesu Zarządzania Ryzykiem Cybernetycznym w Podsektorze Elektryczności (ang. Electricity Subsector Cybersecurity Risk Management Process* – RMP)[6].

1.3 Informacje ogólne na temat dokumentu

W dalszej części dokumentu znajdują się poniższe rozdziały i załączniki:

- Rozdział 2 opisuje komponenty Ram: Rdzeń Ram, Poziomy i Profile.
- Rozdział 3 przedstawia przykłady tego, w jaki sposób Ramy można stosować.
- Załącznik A przedstawia Rdzeń Ram w postaci tabelarycznej: Funkcje, Kategorie, Podkategorie i Referencje Informacyjne.
- Załącznik B zawiera glosariusz wybranych pojęć.
- Załącznik C zawiera listę skrótów stosowanych w niniejszym dokumencie.

[3] Międzynarodowa Organizacja Normalizacyjna *Zarządzanie ryzykiem – Zasady i wytyczne.* ISO 31000:2009. 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[4] Międzynarodowa Organizacja Normalizacyjna / Międzynarodowa Komisja Elektrotechniczna. *Technologia informacyjna – Techniki bezpieczeństwa – Zarządzanie ryzykiem związanym z bezpieczeństwem informacji,* ISO/IEC 27005:2011. 2011. http://www.iso.org/iso/catalogne detail?csnumber=56742

[5] Inicjatywa Transformacyjna Wspólnej Grupy Zadaniowej. *Zarządzanie Ryzykiem Bezpieczeństwa Informacyjnego: Organizacja, Misja oraz Pogląd na System Informacji,* Specjalna Publikacja NIST 800-39. Marzec 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP80Q-39-final.pdf

[6] Departament Energetyki USA, *Elektryczność! Cyberbezpieczeństwo Podsektora! Proces Zarzadzania Ryzykiem.* DOE/OE-0003, Maj 2012. http://energv.gov/sites/prod/files/Cvbersecuritv%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20Mav%202012 .pdf

2.0 Podstawy Ram

Ramy zapewniają wspólną terminologię ułatwiającą zrozumienie, zarządzanie i wyrażanie zagrożeń cybernetycznych zarówno wewnętrznych, jak i zewnętrznych. Można z nich skorzystać podczas identyfikacji i priorytetyzowania czynności mających na celu redukcję zagrożeń cybernetycznych; stanowią narzędzie dostosowujące politykę, działania i podejścia technologiczne w celu zarządzania takimi zagrożeniami. Można je wykorzystać do zarządzania zagrożeniami cybernetycznymi w całej organizacji lub skupić się na dostarczeniu krytycznych usług w ramach organizacji. Różne rodzaje jednostek – łącznie ze strukturami koordynującymi sektor, związkami, i organizacjami – mogą wykorzystywać Ramy dla różnych celów łącznie z tworzeniem ogólnych Profilów.

2.1 Rdzeń Ram

Rdzeń Ram zapewnia zbiór czynności pozwalających osiągnąć określone wyniki związane z cyberbezpieczeństwem, oraz przytacza przykłady prowadzące do uzyskania takich wyników. Rdzeń nie stanowi listy kontrolnej wykonywanych czynności. Prezentuje kluczowe wyniki odnoszące się do cyberbezpieczeństwa zidentyfikowane przez przemysł jako pomocne podczas zarządzania tego typu zagrożeniami. Rdzeń składa się z czterech elementów: Funkcje, Kategorie, Podkategorie i Odniesienia Informacyjne, przedstawione na **rysunku 1:**

Elementy Rdzenia Ram współpracują ze sobą w następujący sposób:

- **Funkcje** organizują podstawowe czynności związane z cyberbezpieczeństwem na najwyższym poziomie. Funkcjami tymi są Identyfikacja, Ochrona, Detekcja, Reagowanie i Przywracanie. Wspomagają one organizację podczas wyrażania jej sposobu zarządzania ryzykiem cybernetycznym organizując informacje, umożliwiając podjęcie decyzji związanych z zarządzaniem zagrożeniami, odpowiadając na zagrożenia i ulepszając wyciąganie wniosków z poprzednich czynności. Funkcje pokrywają się również z istniejącymi metodologiami zarządzania incydentami i pomagają pokazać wpływ inwestycji na cyberbezpieczeństwo. Na przykład inwestycje w planowanie i ćwiczenia wspierają odpowiednie możliwości reagowania i czynności przywracania zmniejszające wpływ na dostawę usług.
- **Kategorie** stanowią podpodziały Funkcji na grupy wyników cyberbezpieczeństwa ściśle powiązane z programowymi potrzebami i określonymi czynnościami. Przykładami kategorii są „Zarządzanie Aktywami”, „Kontrola Dostępu” i „Procesy Detekcji”.

- **Podkategorie** stanowią dalszy podział Kategorii zapewniając określone wyniki czynności technicznych i / lub zarządzania. Zapewniają one zbiór wyników, które pomimo tego, że nie są wyczerpujące, to pomagają osiągnąć cele w każdej Kategorii. Przykłady Podkategorii obejmują „Zewnętrzne systemy informacyjne są skatalogowane", „Dane stacjonarne są chronione" i „Powiadomienia z systemów detekcji są kontrolowane".
- **Odniesienia Informacyjne** to określone rozdziały norm, wytycznych i praktyk powszechnych pośród sektorów infrastruktury krytycznej przedstawiających sposób osiągnięcia wyników związanych z każdą Podkategorią. Odniesienia Informacyjne przedstawione w Rdzeniu Ram są przykładowe i niewyczerpujące. Opierają się na wytycznych międzysektorowych, które są najczęściej przytaczane w procesie opracowywania Ram[7].

Poniżej zdefiniowano pięć Funkcji Rdzenia Ram. Celem tych Funkcji nie jest nakreślenie ścieżki lub doprowadzenie do statycznego pożądanego stanu końcowego. Zamiast tego Funkcje stosować można jednocześnie i w sposób ciągły, aby utworzyć kulturę organizacyjną dynamicznych zagrożeń cybernetycznych. W Załączniku A znajduje się kompletna lista dotycząca Rdzenia Ram.

- **Identyfikacja –** rozwija organizacyjne zrozumienie pozwalające zarządzać zagrożeniami związanymi z cyberbezpieczeństwem systemów, aktywów, danych i możliwości.

  Czynności realizowane w ramach Funkcji Identyfikacja są fundamentalne dla skutecznego wykorzystania Ram. Zrozumienie kontekstu biznesowego, zasobów wspierających najważniejsze funkcje i powiązanego z tym cyberzagrożenia, pozwala organizacji skupić się i priorytetyzować swoje wysiłki równolegle ze strategią zarządzania ryzykiem i potrzebami biznesowymi. Przykłady wyników Kategorii w ramach tej Funkcji obejmują: Zarządzanie Aktywami; Otoczenie Biznesowe; Zarządzanie, Ocenę Ryzyka i Strategię Zarządzania Ryzykiem.

- **Ochrona –** pozwala opracować i wdrożyć odpowiednie środki ochrony zapewniające zrealizowanie najważniejszych usług infrastrukturalnych.

  Funkcja Ochrony wspiera możliwości ograniczenia wpływu potencjalnego zdarzenia związanego z cyberbezpieczeństwem. Przykłady wyników Kategorii w ramach tej Funkcji obejmują: Kontrolę Dostępu, Zaznajomienie i Szkolenie; Bezpieczeństwo Danych; Procesy i Procedury Ochrony Informacji; Utrzymanie i Technologie Zabezpieczające.

- **Detekcja** – opracowanie i wdrożenie odpowiednich czynności w celu zidentyfikowania wystąpienia zdarzenia związanego z cyberbezpieczeństwem.

  Funkcja Detekcji pozwala na czas odkryć zdarzenia związane z cyberbezpieczeństwem. Przykłady wyników Kategorii w ramach tej Funkcji obejmują: Anomalie i Zdarzenia; Ciągłe Monitorowanie Bezpieczeństwa i Procesy Detekcji.

- **Reagowanie** – opracowanie i wdrożenie odpowiednich czynności w celu podjęcia działania związanego z cyberbezpieczeństwem.

[8.] W NIST opracowano Kompendium odniesień informacyjnych zebranych z Wniosków o udzielenie informacji (ang. Request for Information – RFI), warsztatów na temat Ram Cyberbezpieczeństwa i zaangażowania interesariuszy w trakcie procesu opracowywania Ram. Kompendium zawiera normy, wytyczne i praktyki wspomagające wrożenie. Kompendium nie stanowi wyczerpującej listy, ale jest punktem początkowym wykorzystującym początkowe informacje od interesariuszy. Kompedium i inne materiały dodatkowe znajdują się na stronie http://www.nist.gov/cyberframev ork/.

Funkcja Reagowania wspiera możliwości ograniczenia wpływu potencjalnego zdarzenia związanego z cyberbezpieczeństwem. Przykłady wyników Kategorii w ramach tej Funkcji obejmują: Planowanie Reakcji; Komunikację; Analizę; Łagodzenie i Udoskonalenia.

- **Przywracanie –** opracowanie i wdrożenie odpowiednich czynności w celu utrzymania planów odporności i przywrócenia możliwości lub usług, na które wpływ miało zdarzenie cybernetyczne.

  Funkcja Przywracania wspiera przywrócenie normalnych operacji, aby zredukować wpływ na zdarzenie związane z cyberbezpieczeństwem. Przykłady wyników Kategorii w ramach tej Funkcji obejmują: Planowanie Przywrócenia; Usprawnienia i Komunikacja.

2.2 Poziomy Implementacji Ram

Poziomy Wdrożeń Ram („Poziomy") zapewniają kontekst na temat tego, w jaki sposób organizacja widzi zagrożenia cybernetyczne i procesy zarządzania takim ryzykiem. Zakres Poziomów biegnie od Częściowych (Poziom 1) po Adaptacyjne (Poziom 4) i opisuje rosnący stopień rygoru i wyrafinowania w zakresie praktyk zarządzania ryzykiem cybernetycznym i zakres, w jakim zarządzanie tego rodzaju ryzykiem opiera się na potrzebach działalności i jest zintegrowane w ogólnych praktykach zarządzania ryzykiem organizacji. Uwarunkowania zarządzania ryzykiem obejmują wiele aspektów cyberbezpieczeństwa łącznie ze stopniem do jakiego prywatność i wolności obywatelskie zintegrowane są w zarządzaniu cyberbezpieczeństwem organizacji i reakcjach na potencjalne ryzyko.

W trakcie procesu wyboru Poziomu organizacja rozważa swoje obecne praktyki zarządzania ryzykiem, środowisko zagrożeń, wymagania prawne i ustawowe, cele biznesowe / misję oraz ograniczenia organizacyjne. Organizacje powinny określić pożądany Poziom, upewniając się, że wybrany Poziom spełnia cele organizacji, jest możliwy do wdrożenia i ogranicza zagrożenia cybernetyczne względem krytycznych aktywów do poziomów akceptowalnych dla organizacji. Organizacje powinny rozważyć wykorzystanie zewnętrznych informacji uzyskanych z wydziałów i agencji federalnych, centrów informacji i analiz (ang. Information Sharing and Analysis Centers – ISAC), istniejących modeli dojrzałości lub innych źródeł, by pomóc podczas określania swojej pożądanego Poziomu.

Pomimo tego, że organizacje określone jako Poziom 1 (Częściowe) zachęcane są do wzięcia pod uwagę przejścia w stronę Poziomu 2 lub wyższego, Poziomy nie wyznaczają dojrzałości. Zachęca się do przejścia do wyższych Poziomów, gdy zmiana taka ograniczy zagrożenie cybernetyczne i będzie wydajne pod względem kosztów. Pomyślne wdrożenie Ram opiera się na osiągnięciu wyników opisanych w Profilu Docelowym organizacji i po wyznaczeniu Poziomu.

Definicje Poziomów są następujące:

Poziom 1: Częściowe

- *Proces Zarządzania Ryzykiem* – organizacyjne praktyki związane z zarządzaniem zagrożeniami cybernetycznymi nie są sformalizowane, a ryzykiem zarządza się w sposób ad hoc, niekiedy w sposób reaktywny. Priorytetyzacja czynności związanych z cyberbezpieczeństwem może nie wynikać bezpośrednio z celów związanych z ryzykiem organizacyjnym otoczenia zagrożeń lub wymogów działalności / misji.
- *Zintegrowany Program Zarządzania Ryzykiem* – istnieje ograniczona świadomość zagrożeń cybernetycznych na poziomie organizacyjnym, a organizacyjne podejście do zarządzania zagrożeniami cybernetycznymi nie zostało opracowane. Organizacja regularnie realizuje procesy zarządzania zagrożeniami cybernetycznymi, w każdym z przypadków, z uwagi na zróżnicowane doświadczenie lub informacje zebrane ze źródeł zewnętrznych. Organizacja może nie dysponować procesami pozwalającymi na przekazywanie informacji na temat cyberbezpieczeństwa w ramach organizacji.
- *Uczestnictwo Zewnętrzne* – organizacja może nie posiadać wdrożonych procesów, aby uczestniczyć w koordynacji lub współpracy z innymi jednostkami.

Poziom 2: Świadome ryzyka

- *Proces Zarządzania Ryzykiem* – praktyki zarządzania ryzykiem zostały dopuszczone przez zarząd, ale mogą nie być określone jako polityka organizacyjna. Priorytetyzacja czynności związanych z cyberbezpieczeństwem wynika bezpośrednio z celów dotyczących ryzyka organizacyjnego, otoczenia zagrożeń lub wymogów działalności / misji.
- *Zintegrowany Program Zarządzania Ryzykiem* – istnieje świadomość zagrożeń cybernetycznych na poziomie organizacyjnym, ale organizacyjne podejście do zarządzania zagrożeniami cybernetycznymi nie zostało opracowane. Procesy i procedury biorące pod uwagę ryzyko i zatwierdzone przez zarząd zostały zdefiniowane i wdrożone, personel posiada wystarczające zasoby do wykonywania swoich obowiązków związanych z cyberbezpieczeństwem. Informacje na temat cyberbezpieczeństwa są przekazywane w organizacji w postaci nieformalnej.
- *Uczestnictwo Zewnętrzne* – organizacja zna swoją rolę w szerszym ekosystemie, ale nie sformalizowała swoich możliwości, by współpracować i przekazywać informacje na zewnątrz.

Poziom 3: Powtarzalne

- *Proces Zarządzania Ryzykiem* – praktyki zarządzania ryzykiem w organizacji zostały formalnie dopuszczone i wyrażone w postaci strategii. Organizacyjne praktyki cyberbezpieczeństwa są regularnie aktualizowane na podstawie stosowania procesów zarządzania ryzykiem względem zmian wymogów biznesowych / misji i zmieniającego się otoczenia zagrożeń i technologicznego.
- *Zintegrowany Program Zarządzania Ryzykiem* – istnieje organizacyjne podejście do zarządzania zagrożeniami cybernetycznymi. Polityka, procesy i procedury świadome ryzyka zostały zdefiniowane, wdrożone zgodnie z oczekiwaniami i skontrolowane. Wdrożone zostały spójne metody dla skutecznego reagowania na zmiany ryzyka. Personel posiada wiedzę i umiejętności do realizacji swoich wyznaczonych ról i odpowiedzialności.
- *Uczestnictwo Zewnętrzne* – organizacja rozumie wzajemne zależności i partnerów i odbiera informacje od tych partnerów umożliwiające współpracę i podejmowanie decyzji dotyczących zarządzania na bazie ryzyka w organizacji w odpowiedzi na zdarzenia.

Poziom 4: Adaptacyjne

- *Proces Zarządzania Ryzykiem* – organizacja dostosowuje swoje praktyki w zakresie cyberbezpieczeństwa na podstawie doświadczeń i przewidywalnych wskaźników uzyskanych z poprzednich i obecnych czynności związanych z cyberbezpieczeństwem. W drodze ciągłego doskonalenia obejmującego zaawansowane technologie i praktyki cyberbezpieczeństwa, organizacja aktywnie adaptuje się do zmieniającego się otoczenia cyberbezpieczeństwa i w odpowiednim czasie reaguje na ewoluujące i złożone zagrożenia.
- *Zintegrowany Program Zarządzania Ryzykiem* – opracowane jest organizacyjne podejście do zarządzania zagrożeniami cybernetycznymi wykorzystujące świadomą zagrożeń strategię, procesy i procedury, aby odnieść się do potencjalnych wydarzeń związanych z cyberbezpieczeństwem. Zarządzanie ryzykiem związanym z cyberbezpieczeństwem stanowi część kultury organizacyjnej i ewoluuje od znajomości poprzednich czynności, informacji uzyskanych z innych źródeł i ciągłej wiedzy o funkcjonowaniu ich systemów i sieci.
- *Uczestnictwo Zewnętrzne* – organizacja zarządza ryzykiem i aktywnie wymienia informacje pomiędzy partnerami, by zapewnić, że dokładne i aktualne informacje są rozdzielane i wchłaniane w celu poprawy cyberbezpieczeństwa, zanim dojdzie do zdarzenia z nim związanego.

2.3 Profil Ram

Profil Ram („Profil”) stanowi dostosowanie Funkcji, Kategorii i Podkategorii do wymogów działalności, tolerancji ryzyka i zasobów organizacji. Profil pozwala organizacjom opracować mapę drogową prowadzącą do redukcji zagrożeń cybernetycznych, która jest odpowiednio dostosowana do celów organizacyjnych i sektorowych, uwzględnia wymagania prawne / ustawowe i najlepsze praktyki przemysłowe i odzwierciedla priorytety zarządzania ryzykiem. Biorąc pod uwagę złożoność wielu organizacji, mogą one zdecydować o posiadaniu kilku profilów dostosowanych do określonych komponentów i odpowiadających ich poszczególnym potrzebom.

Profile Ram wykorzystać można do opisania obecnego stanu lub wymaganego stanu docelowego określonych czynności związanych z cyberbezpieczeństwem. Obecny Profil wskazuje na wyniki cyberbezpieczeństwa, które są aktualnie uzyskiwane. Profil Docelowy wskazuje na wyniki niezbędne do osiągnięcia celów zarządzania zagrożeniami cybernetycznymi. Profile obejmują również wymagania biznesowe / misję i pomagają w przekazywaniu zagrożeń w i pomiędzy organizacjami. Niniejszy dokument Ramowy nie podaje szablonów Profilów, przez co umożliwia elastyczność wdrożenia.

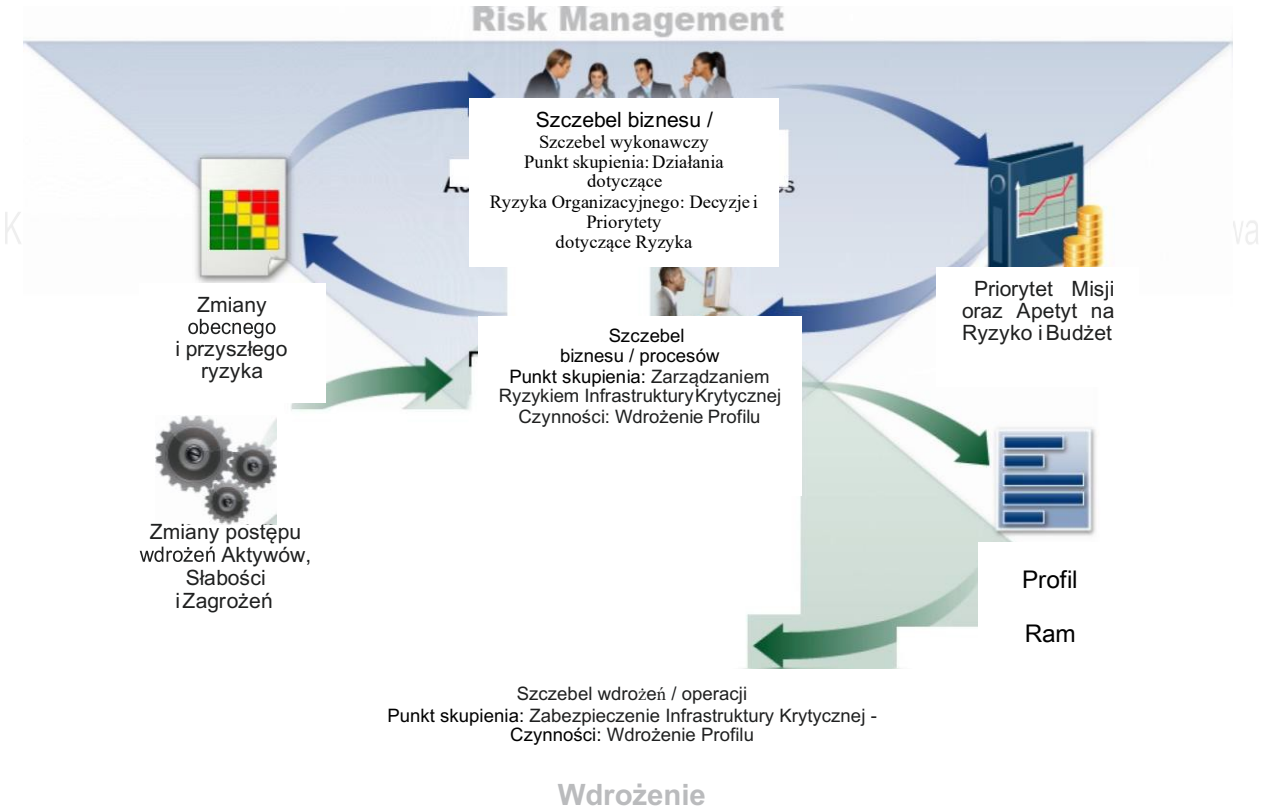
Porównanie Profilów (np. Profil Obecny i Profil Docelowy) może ujawnić wiele luk, którym należy zaradzić, by spełnić cele związane z zarządzaniem zagrożeniami cybernetycznymi. Plan działania mający na celu zareagowanie na te luki może przyczynić się do powstawania wyżej opisanej mapy drogowej. Priorytetyzowanie minimalizacji luk wynika z potrzeb biznesowych i procesów zarządzania ryzykiem w organizacji. Tego typu podejście na podstawie ryzyka pozwala organizacji mierzyć szacunki dotyczące zasobów (np. personel, fundusze), aby osiągnąć cele cyberbezpieczeństwa w sposób wydajny i zhierarchizowany.

2.4 Koordynacja Wdrożeń Ram

Ilustracja 2 opisuje ogólny przepływ informacji i decyzji na poniższych szczeblach w organizacji:

- Wykonawczy
- Biznes / Procesy
- Wdrożenie / Operacje

Szczebel wykonawczy przekazuje priorytety misji, dostępne zasoby oraz ogólną tolerancję ryzyka do poziomu biznesu / procesów. Szczebel biznesu / procesów wykorzystuje informacje jako informacje wejściowe do procesu zarządzania ryzykiem, a następnie współpracuje ze szczeblem wdrożeń / operacji, by przekazać potrzeby biznesowe i utworzyć Profil. Szczebel Wdrożeń / operacji przekazuje postęp w zakresie wdrożenia Profilu do szczebla biznesu / procesów. Szczebel biznesu / procesów wykorzystuje te informacje w celu przeprowadzenia oceny wpływu. Zarząd szczebla biznesu / procesów przesyła wyniki oceny wpływu do szczebla wykonawczego, by poinformować o ogólnym procesie zarządzania ryzykiem w organizacji i do poziomu wdrożeń / operacji w celu uświadomienia wpływu na biznes.



Rys. 2: Przepływ Informacji Podstawowych i Decyzji w Organizacji

3.0 W jaki sposób Korzystać z Ram

Organizacja może korzystać z Ram jako kluczowej części swoich systematycznych procesów identyfikacji, oceny i zarządzania ryzykiem cybernetycznym. Ramy nie są zaprojektowane tak, by zastąpić istniejące procesy; organizacja może wykorzystywać swoje obecne procesy i nakładać je na Ramy, by określić luki w obecnie stosowanym podejściu do ryzyka cybernetycznego i opracować mapę drogową poprawy. Dzięki stosowaniu Ram jako narzędzia zarządzania bezpieczeństwem cybernetycznym, organizacja może określić czynności najistotniejsze dla dostawy usług krytycznych i priorytetyzować wydatki, aby zmaksymalizować wpływ inwestycji.

Ramy zaprojektowane są tak, by uzupełniać istniejące operacje biznesowe i związane z cyberbezpieczeństwem. Mogą służyć jako podwaliny nowego programu cyberbezpieczeństwa lub mechanizm poprawy istniejącego programu. Ramy dają możliwość wyrażania wymogów cyberbezpieczeństwa partnerom biznesowym i klientom i mogą pomóc zidentyfikować luki w praktykach dotyczących cyberbezpieczeństwa. Udostępniają one również ogólny zbiór uwarunkowań i procesów umożliwiający rozważenie implikacji względem prywatności i swobód obywatelskich w kontekście programu cyberbezpieczeństwa.

W poniższych rozdziałach zawarto różne sposoby, dzięki którym organizacje mogą wykorzystywać Ramy.

3.1 Podstawowa Kontrola Praktyk Cyberbezpieczeństwa

Ramy wykorzystać można do porównania obecnych czynności związanych z cyberbezpieczeństwem w organizacji z tymi określonymi w Rdzeniu Ram. Dzięki utworzeniu Obecnego Profilu organizacje mogą skontrolować zakres, w jakim osiągają wyniki opisane w Głównych Kategoriach i Podkategoriach względem pięciu ogólnych Funkcji: Identyfikacji, Ochrony, Detekcji, Reagowania i Przywracania. Organizacja może zauważyć, że już osiągnęła pożądane wyniki, zarządzając cyberbezpieczeństwem proporcjonalnie do znanych rodzajów ryzyka. Może też nastąpić sytuacja odwrotna - organizacja może dojść do wniosku, że ma istnieje możliwość (lub konieczność) poprawy. Organizacja może wykorzystać uzyskane informacje do opracowania planu działania na rzecz wzmocnienia istniejących praktyki i ograniczenia ryzyka cybernetycznego. Organizacja może również dostrzec, iż przeinwestowuje w celu uzyskania określonych wyników. Może wykorzystać te informacje, by ponownie zhierarchizować zasoby dla wzmocnienia innych praktyk cyberbezpieczeństwa.

Pomimo tego, że nie zastępują one procesu zarządzania ryzykiem, tych pięć ogólnych Funkcji zapewnia wyższemu kierownictwu i innym osobom spójną metodę wyodrębnienia fundamentalnych koncepcji dotyczących zagrożeń cybernetycznych, aby mogło ocenić to, w jaki sposób zidentyfikowane zagrożenia są zarządzane oraz w jaki sposób ich organizacja utrzymuje wysoki poziom istniejących norm, wytycznych i praktyk cyberbezpieczeństwa. Ramy mogą również pomóc organizacji odpowiedzieć na fundamentalne pytania, łącznie z tym „Jak nam idzie?". Następnie mogą w bardziej świadomy sposób przejść do ulepszenia swoich praktyk związanych z cyberbezpieczeństwem, tam, gdzie i kiedy uznają to za konieczne.

3.2 Opracowywanie lub Doskonalenie Programu Cyberbezpieczeństwa

Poniższe etapy przedstawiają to, w jaki sposób organizacja może stosować Ramy podczas tworzenia nowego lub doskonalenia istniejącego programu cyberbezpieczeństwa. Etapy te należy powtarzać w miarę konieczności, by stale doskonalić cyberbezpieczeństwo.

Etap 1: Priorytety i Zakres. Organizacja identyfikuje swoje cele biznesowe / misję i priorytety organizacyjne wysokiego szczebla. Dzięki tym informacjom organizacja podejmuje strategiczne decyzje dotyczące wdrożenia cyberbezpieczeństwa i określa zakres systemów i aktywów wspierających wybraną linię działań lub proces. Ramy można dostosować tak, by wspierały różne linie działalności lub procesy w organizacji, które mogą wykazywać różne potrzeby biznesowe i tolerancje ryzyka.

Etap 2: Orientacja. Po wyznaczeniu zakresu programu cyberbezpieczeństwa dla linii działalności lub procesu, organizacja identyfikuje powiązane systemy i aktywa, wymagania ustawowe i ogólne podejście do ryzyka. Organizacja identyfikuje zagrożenia i słabości względem takich systemów i aktywów.

Etap 3: Tworzenie Obecnego Profilu. Organizacja opracowuje Obecny Profil wskazując to, które wyniki Kategorii i Podkategorii z Rdzenia Ram są aktualnie osiągane.

Etap 4: Przeprowadzenie Oceny Ryzyka. Ocena ta może być kierowana procesem zarządzania ryzykiem ogólnym organizacji lub przeprowadzona na podstawie wcześniejszych czynności związanych z oceną ryzyka. Organizacja analizuje środowisko robocze w celu rozpoznania prawdopodobieństwa zdarzenia związanego z cyberbezpieczeństwem oraz wpływ takiego zdarzenia na organizację. Ważne jest, aby organizacje łączyły dane na temat pojawiającego się ryzyka, zagrożeń i słabości, by ułatwić dogłębne zrozumienie prawdopodobieństwa i wpływu zdarzenia związanego z cyberbezpieczeństwem.

Etap 5: Tworzenie Docelowego Profilu. Organizacja tworzy Profil Docelowy, skupiający się na ocenie Kategorii i Podkategorii Ram opisujących pożądane wyniki dotyczące cyberbezpieczeństwa organizacji. Organizacje mogą również opracowywać własne dodatkowe Kategorie i Podkategorie, by uwzględnić specyficzne zagrożenia dla organizacji. Organizacja może również uwzględnić wpływ i wymagania zewnętrznych interesariuszy takich jak jednostki sektorowe, klienci i partnerzy biznesowi podczas tworzenia Profilu Zewnętrznego.

Etap 6: Wyznaczenie, Analiza i Priorytetyzowanie Luk. Aby określić luki, organizacja porównuje Obecny Profil z Profilem Docelowym. Następnie tworzy zhierarchizowany plan działania, by odpowiednio zareagować na te luki, a który to plan opiera się na stymulantach misji, analizie zysków i strat oraz zrozumieniu ryzyka, by osiągnąć wyniki w Profilu Docelowym. Następnie organizacja określa zasoby niezbędne do wyeliminowania takich luk. Wykorzystywanie w ten sposób Profilów pozwala podjąć organizacji świadomą decyzję dotyczącą czynności związanych z cyberbezpieczeństwem, wspiera zarządzanie ryzykiem i umożliwia organizacji przeprowadzenie wydajnych i nakierowanych usprawnień.

Etap 7: Wdrożenie Planu Działania. Organizacja określa to, które plany działania zrealizować w przypadku luk zidentyfikowanych w poprzednim etapie. Następnie monitoruje swoje obecne praktyki związane z cyberbezpieczeństwem względem Profilu Docelowego. Dodatkowo Ramy identyfikują przykładowe Odniesienia Informacyjne dotyczące Kategorii i Podkategorii, ale mimo tego organizacje powinny określić to, które normy, wytyczne i praktyki, łącznie z tymi dedykowanymi sektorom, sprawdzają się najlepiej w ich przypadku.

Organizacja może powtarzać etapy w miarę potrzeb, by w sposób ciągły oceniać i doskonalić swoje cyberbezpieczeństwo. Przykładowo, organizacja może uznać, że większa częstotliwość etapu orientacji

poprawia jakość oceny ryzyka. Ponadto mogą monitorować postęp w drodze iteracyjnych aktualizacji Obecnego Profilu, porównując następnie go z Profilem Docelowym. Organizacje mogą również wykorzystać ten proces, by dostosować swój program cyberbezpieczeństwa względem pożądanego Szczebla Wdrożeń Ram.

3.3 Przekazywanie Informacji na temat Wymogów Cyberbezpieczeństwa Interesariuszom

Ramy zapewniają wspólną terminologię komunikacji wymogów pośród wzajemnie powiązanych interesariuszy odpowiedzialnych za dostawę kluczowych, krytycznych usług infrastrukturalnych. Przykłady obejmują:

- Organizacja może wykorzystać Profil Docelowy do poinformowania zewnętrznego dostawcy usług o wymogach w zakresie zarządzania ryzykiem cybernetycznym (np. dostawca usług w chmurze, do której eksportowane są dane).
- Organizacja może wyrazić swój stan cyberbezpieczeństwa za pomocą Obecnego Profilu, by złożyć raport na temat wyników lub porównać je z wymogami w zakresie pozyskiwania środków.
- Właściciel / operator krytycznej infrastruktury po zidentyfikowaniu zewnętrznego partnera, od którego infrastruktura ta jest zależna, może wykorzystać Profil Docelowy, by zakomunikować wymagane Kategorie i Podkategorie.
- Sektor infrastruktury krytycznej może opracować Profil Docelowy, który może być wykorzystany przez jego odbiorców jako wstępny Profil Podstawowy, za pomocą którego tworzone są dedykowane Profile Docelowe.

3.4 Identyfikowanie Szans dla Nowych lub Zweryfikowanych Odniesień Informacyjnych

Ramy wykorzystać można do zidentyfikowania możliwości dla nowych lub zrewidowanych norm, wytycznych lub praktyk, w których dodatkowe Odniesienia Informacyjne pomogłyby organizacjom spełnić pojawiające się potrzeby. Organizacja wdrażająca daną Podkategorię lub opracowująca nową Podkategorię, może dostrzec, że istnieje niewiele – jeśli w ogóle istnieją - Odniesień Informacyjnych dotyczących danej czynności. Aby stawić czoła takiej potrzebie, organizacja może współpracować z liderami technologii i / lub organami ds. norm w celu naszkicowania, opracowania i skoordynowania norm, wytycznych lub praktyk.

3.5 Metodologia Ochrony Prywatności i Swobód Obywatelskich

W rozdziale tym opisano metodologię wymaganą przez Dekret, odnoszącą się do implikacji w zakresie prywatności i swobód obywatelskich do jakich może dojść w wyniku operacji związanych z cyberbezpieczeństwem. Celem tej metodologii jest zapewnienie ogólnego zbioru postanowień i procesów, ponieważ implikacje dotyczące prywatności i swobód obywatelskich mogą się różnić w zależności od sektora lub zmieniać w miarę upływu czasu, a organizacje mogą odnosić się do takich uwarunkowań i procesów korzystając z szerokiej gamy rozwiązań technicznych. Niemniej jednak nie wszystkie czynności zawierające się w programie cyberbezpieczeństwa mogą stanowić podstawę takim uwarunkowaniom. Zgodnie z ustaleniami Rozdziału 3.4 konieczne może okazać się opracowanie norm, wytycznych i dodatkowych najlepszych praktyk w zakresie prywatności technicznej, by zapewnić wsparcie usprawnionym wdrożeniom technicznym.

Implikacje dotyczące prywatności i swobód obywatelskich mogą pojawić się, gdy podczas prowadzonych przez organizację czynności związanych z cyberbezpieczeństwem wykorzystywane, gromadzone, przetwarzane, utrzymywane lub ujawniane są informacje osobowe. Niektóre z przykładów czynności, które mogą być związane z uwarunkowaniami dotyczącymi prywatności lub swobód obywatelskich mogą obejmować: czynności związane z cyberbezpieczeństwem prowadzące do nadmiernego gromadzenia lub przechowywania informacji osobowych; ujawnienia lub wykorzystania informacji osobowych niezwiązanych z czynnościami dotyczącymi cyberbezpieczeństwa; czynności osłabienia cyberbezpieczeństwa prowadzące do odmowy usługi lub innych potencjalnie

niekorzystnych sytuacji, łącznie z czynnościami takimi jak pewne typy detekcji lub monitorowania incydentów, mogącymi wpływać na swobodę ekspresji lub stowarzyszania.

Rząd i jego przedstawiciele ponoszą bezpośrednią odpowiedzialność za ochronę swobód obywatelskich wynikających z czynności związanych z cyberbezpieczeństwem. Zgodnie z poniższą metodologią rząd lub jego przedstawiciele, którzy są właścicielami lub obsługują infrastrukturę krytyczną, powinni wdrożyć proces wspierający zgodność czynności cyberbezpieczeństwa z obowiązującym prawem, przepisami i wymogami konstytucyjnymi.

W przypadku implikacji dla prywatności organizacje mogą rozważyć to, w jaki sposób w okolicznościach, w których środki takie są odpowiednie, program cyberbezpieczeństwa może stosować zasady prywatności takie jak: minimalizowanie gromadzenia danych, ujawniania i przechowywania informacji osobowych dotyczących incydentu związanego z cyberbezpieczeństwem; ograniczenia użytkowania poza czynnościami związanymi z cyberbezpieczeństwem w stosunku do dowolnych informacji zebranych zwłaszcza w odniesieniu do czynności dotyczących cyberbezpieczeństwa; transparentności pewnych czynności związanych z cyberbezpieczeństwem; zgody osób i rekompensat za szkodliwy wypływ wykorzystania danych osobowych podczas czynności związanych z cyberbezpieczeństwem; jakości, integralności i bezpieczeństwa danych; oraz odpowiedzialności, jak również kontroli.

Ponieważ w Załączniku A organizacje oceniają Rdzeń Ram, poniższe procesy i czynności można uznać jako środki odnoszące się do przytoczonych powyżej implikacji względem prywatności i swobód obywatelskich:

Zarządzanie ryzykiem dotyczącym cyberbezpieczeństwa

- Ocena ryzyka dotyczącego cyberbezpieczeństwa i potencjalnych reakcji na ryzyko w organizacji bierze pod uwagę implikacje programu cyberbezpieczeństwa względem prywatności
- Osoby odpowiedzialne za prywatność związaną z cyberbezpieczeństwem informują odpowiednie kierownictwo i posiadają właściwe przeszkolenie
- Opracowany jest proces wspierający zgodność czynności dotyczących cyberbezpieczeństwa z obowiązującym prawem, przepisami i wymaganiami konstytucji
- Opracowany jest proces oceny wdrożenia powyższych środków organizacyjnych i kontroli

Podejścia do identyfikacji i uwierzytelniania osób mających dostęp do aktywów i systemów organizacji

- Podejmowane są kroki mające na celu identyfikację i odniesienie się do implikacji dotyczących prywatności wynikających ze środków kontroli dostępu w zakresie, w jakim obejmują one gromadzenie, ujawnianie lub wykorzystywanie informacji osobowych

Wiedza i środki szkoleniowe

- Obowiązujące informacje wynikające z polityki prywatności organizacji ujęte są w szkoleniu siły roboczej i czynnościach uświadamiających
- Dostawcy usług związanych z cyberbezpieczeństwem na rzecz organizacji są poinformowani w zakresie obowiązującej w organizacji polityki prywatności

Detekcja czynności nietypowych oraz monitorowanie systemu i aktywów

- Opracowany jest proces przeprowadzania kontroli prywatności odnośnie wykrywania nietypowych czynności i monitorowania cyberbezpieczeństwa

Czynności związane z reagowaniem łącznie z wymianą informacji i innymi pracami łagodzącymi wpływ

- Opracowany proces oceny tego, czy, kiedy, jak i w jakim zakresie informacje osobowe przekazywane są na zewnątrz organizacji jako część czynności wymiany informacji w zakresie cyberbezpieczeństwa
- Opracowany proces przeprowadzania kontroli prywatności odnośnie prac mających na celu ograniczenie wpływu cyberbezpieczeństwa

Załącznik A: Rdzeń Ram

W załączniku tym przedstawiono Rdzeń Ram: lista Funkcji, Kategorii, Podkategorii i Odniesień Informacyjnych, opisujących określone czynności dotyczące cyberbezpieczeństwa, powszechne we wszystkich sektorach infrastruktury. Wybrany format prezentacji Rdzenia Ram nie sugeruje określonej kolejności wdrożeń, ani nie narzuca stopnia istotności Kategorii, Podkategorii i Odniesień Informacyjnych. Rdzeń Ram przedstawiony w niniejszym załączniku zawiera ogólny zbiór czynności dotyczących zarządzania ryzykiem związanym z cyberbezpieczeństwem. Pomimo tego, że Ramy nie są wyczerpujące, to istnieje możliwość ich rozbudowy, pozwalająca organizacjom, sektorom i innym jednostkom wykorzystywać Podkategorie i Odniesienia Informacyjne, które są wydajne i skuteczne podczas zarządzania własnym ryzykiem dotyczącym cyberbezpieczeństwa. Czynności wybrać można spośród Rdzenia Ram na etapie procesu tworzenia Profilu i do takiego Profilu dodać można Kategorie, Podkategorie i Odniesienia Informacyjne. Proces zarządzania ryzykiem w organizacji, wymagania prawne / ustawowe, cele biznesowe / misja i ograniczenia organizacyjne kierunkują wybór takich czynności podczas tworzenia Profilu. Oceniając ryzyko względem bezpieczeństwa oraz środki ochrony, informacja osobowa postrzegana jest jako składnik danych lub aktywo ujęte w Kategoriach.

Pomimo tego, że zamierzone wyniki zidentyfikowane w Funkcjach, Kategoriach i Podkategoriach są takie same dla IT i ICS, to środowiska robocze i uwarunkowania IT i ICS różnią się. ICS ma bezpośredni wpływ na świat fizyczny łącznie z potencjalnymi zagrożeniami zdrowia i bezpieczeństwa osób oraz wpływ na środowisko. Dodatkowo ICS ma wyjątkowe wymagania w zakresie wydajności i niezawodności w porównaniu do IT, a podczas wdrożeń środków cyberbezpieczeństwa pod uwagę należy wziąć cele bezpieczeństwa i wydajność.

Dla ułatwienia użytkowania, w każdym przypadku każdemu komponentowi Rdzenia Ram nadany jest niepowtarzalny identyfikator. Funkcje i Kategorie posiadają niepowtarzalny identyfikator alfabetyczny, jak pokazano w tabeli 1.
Podkategorie w każdej spośród Kategorii opisane są numerycznie; niepowtarzalny identyfikator dla każdej Podkategorii uwzględniony jest w tabeli 2.

Dodatkowe materiały wspomagające dotyczące Ram znajdują się na stronie NIST pod adresem http://www.nist.gov/cyberframework/.

Tabela 1: Niepowtarzalne Identyfikatory Funkcji i Kategorii

Niepowtarzalny Identyfikator Funkcji	Funkcja	Niepowtarzalny Identyfikator Kategorii	Kategoria
ID	Identyfikacja	ID.AM	Zarządzanie aktywami
		ID.BE	Otoczenie biznesu
		ID.GV	Zarządzanie
		ID.RA	Ocena ryzyka
		ID.RM	Strategia zarządzania ryzykiem
PR	Ochrona	PR.AC	Kontrola dostępu
		PR.AT	Wiedza i szkolenie
		PR.DS	Bezpieczeństwo danych
		PR.IP	Procesy i procedury ochrony informacji
		PR.MA	Konserwacja
		PR.PT	Technologia zabezpieczająca
DE	Detekcja	DE.AE	Anomalie i zdarzenia
		DE.CM	Ciągłe monitorowanie bezpieczeństwa
		DE.DP	Procesy detekcji
RS	Reakcja	RS.RP	Planowanie reakcji
		RS.CO	Komunikacja
		RS.AN	Analiza
		RS.MI	Minimalizowanie
		RS.IM	Usprawnienia
RC	Przywrócenie	RC.RP	Planowanie przywrócenia
		RC.IM	Usprawnienia
		RC.CO	Komunikacja

Tabela 2: Rdzeń Ram

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
IDENTYFIKACJA (ID)	**Zarządzanie Aktywami (ID.AM):** Dane, personel, urządzenia, systemy i zakłady umożliwiające osiągnięcie celów biznesowych przez organizację zostały zidentyfikowane i zarządzane są według ich istotności względem celów biznesowych i strategii w zakresie ryzyka organizacji.	**ID.AM-1:** Fizyczne urządzenia i systemy w organizacji zostały zinwentaryzowane	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3 4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1. A.8.1.2 • **NIST SP 800-53 Wer. 4** CM-8
		ID.AM-2: Platformy programowe i aplikacje w organizacji zostały zinwentaryzowane	• **CCS CSC** 2 • **COBIT 5** BAI09.01. BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Wer. 4** CM-8
		ID.AM-3: Komunikacja i przepływ danych w organizacji zostały zmapowane	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3 4 • **ISO/IEC 27001:2013** A 13.2.1 • **NIST SP 800-53 Wer. 4** ACM, CAM. CA-9. PL-8
		ID.AM-4: Zewnętrzne systemy informacyjne są skatalogowane	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A. 11.2.6 • **NIST SP 800-53 Wer. 4** AC-20, SA-9
		ID.AM-5: Zasoby (np. sprzęt, urządzenia, dane i oprogramowanie) są priorytetyzowane według klasyfikacji, krytyczności i wartości biznesowej	• **COBIT 5** APO03.03. AP003.04. BAI09.02 • **ISA 62443-2-1:2009** 4.2.3 6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Wer. 4** CP-2, RAM. SA-14
		ID.AM-6: Opracowane zostały role cyberbezpieczeństwa i odpowiedzialności za siłę roboczą i zewnętrznych interesariuszy (np. dostawców, klientów, partnerów)	• **COBIT 5** APO01.02. DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3 3 • **ISO/IEC 27001:2013** A.6.1.1

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
			• **NIST SP 800-53 Wer. 4** CP-2. PS-7. PM-11
	Otoczenia biznesu (ID.BE): Misja, cele, interesariusze i czynności organizacji są zrozumiałe i zhierarchizowane: są wykorzystywane dla przekazania informacji na temat ról cyberbezpieczeństwa, odpowiedzialności i podjęcia decyzji związanych z zarządzaniem ryzykiem.	**ID.BE-1:** Rola organizacji w łańcuchu dostaw jest zidentyfikowana i przekazana do wiadomości	• **COBIT 5** AP008.04. AP008.05. APO10.03, APO10.04. APO10.05 • **ISO/IEC 27001:2013** A.15.1.3. A.15.2.1. A.15.2.2 • **NIST SP 800-53 Wer. 4** CP-2. SA-12
		ID.BE-2: Położenie organizacji w ramach najważniejszej infrastruktury i jej sektora przemysłowego zostało zidentyfikowane i przekazane do wiadomości	• **COBIT 5** APO02.06. APO03.01 • **NIST SP 800-53 Wer. 4** PM-8
		ID.BE-3: Priorytety misji organizacyjnej, celów i czynności są opracowane i przekazane do wiadomości	• **COBIT 5** APO02.01. APO02.06. APO03.01 • **ISA 62443-2-1:2009** 4.2.2.1. 4.2.3.6 • **NIST SP 800-53 Wer. 4** PM-11. SA-14
		ID.BE-4: Zależności i funkcje krytyczne dostarczania usług krytycznych są opracowane.	• **ISO/IEC 27001:2013** A. 11.2.2. A.l 1.2.3. A. 12.1.3 • **NIST SP 800-53 Wer. 4** CP-8. PE-9. PE-11. PM-8. SA-14
		ID.BE-5: Wymagania niezawodności mające na celu wsparcie krytycznych usług zostały opracowane.	• **COBIT 5** DSS04.02 • **ISO/IEC 27001:2013** A 11.1.4, A.17.1.1. A.17.1.2. A.17.2.1 • **NIST SP 800-53 Wer. 4** CP-2. CP-11. SA-14
	Zarządzanie (ID.GV): Strategie, procedury i procesy zarządzania i monitorowania wymogów ustawowych, prawnych, dotyczących ryzyka, środowiska i operacyjnych w organizacji są zrozumiałe, a zarząd jest poinformowany o zagrożeniach cybernetycznych.	**ID.GV-1:** Opracowana jest strategia bezpieczeństwa informacji w organizacji	• **COBIT 5** APO01.03. EDM01.01, EDM01.02 • **ISA 62443-2-1:2009** 4.3.2 6 • **ISO/IEC 27001:2013** A.5.1.1 • **NIST SP 800-53 Wer. 4** -1 środki kontroli pochodzące z wszystkich grup
		ID.GV-2: Role i obowiązki związane z bezpieczeństwem informacji są koordynowane i pokrywają się względem ról wewnętrznych i partnerów zewnętrznych	• **COBIT 5** APO13.12 • **ISA 62443-2-1:2009** 4.3.2.3 3 • **ISO/IEC 27001:2013** A.6.1.1. A.7.2.1 • **NIST SP 800-53 Wer. 4** PM-1, PS-7
		ID.GV-3: Wymagania prawne i ustawowe cyberbezpieczeństwa,	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3 7

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
		w tym zobowiązań dotyczących prywatności i swobód obywatelskich, zostały zrozumiane i są kontrolowane	• **ISO/IEC 27001:2013** A.18.1 • **NIST SP 800-53 Wer. 4** -1 środki kontroli pochodzące z wszystkich grup (za wyjątkiem PM-1)
		ID.GV-4: Kierownictwo i procesy zarządzania ryzykiem odpowiadają na zagrożenia związane z cyberbezpieczeństwem	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3.1. 4.2.3.3. 4.2.3.8. 4.2.3.9. 4.2.3.11. 4.3.2.4.3. 4.3.2.6.3 • **NIST SP 800-53 Wer. 4** PM-9. PM-11
	Ocena ryzyka (ID.RA): Organizacja rozumie ryzyko związane z cyberbezpieczeństwem dotyczące operacji organizacyjnych (łącznie z misją, funkcjami, wizerunkiem lub reputacją), aktywów organizacji i osób.	**ID.RA-1:** Słabości aktywów są identyfikowane i dokumentowane	• **CCS CSC** 4 • **COBIT 5** APO12.01. APO12.02. APO12.03. APO12.04 • **ISA 62443-2-1:2009** 4.2.3. 4.2.3.7. 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.12.6.1. A.18.2.3 • **NIST SP 800-53 Wer. 4** CA-2. CA-7. CA-8. RA-3. RA-5. SA-5. SA-11. SI-2. SI-4. SI-5
		ID.RA-2: Informacje na temat zagrożeń i słabości uzyskane zostały z for i innych źródeł współdzielenia informacji	• **ISA 62443-2-1:2009** 4.2.3. 4.2.3.9. 4.2.3.12 • **ISO/IEC 27001:2013** A.6.1.4 • **NIST SP 800-53 Wer. 4** PM-15. PM-16. SI-5
		ID.RA-3: Zagrożenia, zarówno wewnętrzne jak i zewnętrzne, są zidentyfikowane i udokumentowane	• **COBIT 5** APO12.01. APO12.02. APO12.03. APO12.04 • **ISA 62443-2-1:2009** 4.2.3. 4.2.3.9. 4.2.3.12 • **NIST SP 800-53 Wer. 4** RA-3. SI-5. PM-12. PM-16
		ID.RA-4: Potencjalny wpływ na działania i prawdopodobieństwa są zidentyfikowane	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3. 4.2.3.9. 4.2.3.12 • **NIST SP 800-53 Wer. 4** RA-2. RA-3. PM-9. PM-11. SA-14
		ID.RA-5: Zagrożenia, słabości, prawdopodobieństwa i wpływ wykorzystywane są do określania ryzyka	• **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Wer. 4** RA-2. RA-3, PM-16
		ID.RA-6: Reakcje na ryzyko zostały zidentyfikowane i	• **COBIT 5** APO12.05. APO13.02

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
		zhierarchizowane	• **NIST SP 800-53 Wer. 4** PM-4. PM-9
	Strategia zarządzania ryzykiem (ID.RM): Priorytety, ograniczenia, tolerancja ryzyka i założenia organizacji są opracowane i służą wsparciu decyzji w zakresie ryzyka operacyjnego.	**ID.RM-1:** Procesy zarządzania ryzykiem są opracowane, zarządzane i uzgodnione z interesariuszami organizacji	• **COBIT 5** APO12.04. APO12.05. APO13.02. BAI02.03. BAI04.02 • **ISA 62443-2-1:2009** 4 3.4.2 • **NIST SP 800-53 Wer. 4** PM-9
		ID.RM-2: Tolerancja ryzyka przez organizację jest określona i jasno wyrażona	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.2.6.5 • **NIST SP 800-53 Wer. 4** PM-9
		ID.RM-3: Wyznaczenie tolerancji ryzyka organizacji wyrażone jest na podstawie pełnionej roli w krytycznej infrastrukturze oraz analizy ryzyka w danym sektorze	• **NIST SP 800-53 Wer. 4** PM-8. PM-9. PM-11. SA-14
OCHRONA (PR)	**Kontrola dostępu (PR.AC):** Dostęp do aktywów i powiązanych zakładów jest ograniczony do użytkowników uprawnionych, procesów lub urządzeń, oraz do uprawnionych czynności i transakcji.	**PR.AC-1:** Tożsamości i dane uwierzytelniające są zarządzane dlauprawnionych urządzeń i użytkowników	• **CCS CSC** 16 • **COBIT 5** DSS05.04. DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1. SR 1.2. SR 1.3. SR 1.4. SR 1.5. SR 1.7. SR 1.8. SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1. A.9.2.2. A.9.2.4. A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Wer. 4** AC-2. Grupa IA
		PR.AC-2: Dostęp fizyczny do aktywów jest kontrolowany i chroniony	• **COBIT 5** DSS01.04. DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2. 4.3.3.3.8 • **ISO/IEC 27001:2013** A. 11.1.1. A. 11.1.2. A.11.1.4. A 11.1.6, A.11.2.3 • **NIST SP 800-53 Wer. 4** PE-2. PE-3. PE-4. PE-5. PE-6. PE-9
		PR.AC-3: Dostęp zdalny jest kontrolowany	• **COBIT 5** APO13.01. DSS01.04. DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13. SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2. A.13.1.1. A.13.2.1

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
			• **NIST SP 800-53 Wer. 4** AC-17, AC-19, AC-20
		PR.AC-4: Uprawnienia dostępu są kontrolowane poprzez wykorzystanie zasad najmniejszego uprzywilejowania i podziału obowiązków	• **CCS CSC** 12, 15 • **ISA 62443-2-1:2009** 4 3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2. A.9.1.2. A.9.2.3. A.9.4.1, A.9.4.4 • **NIST SP 800-53 Wer. 4** AC-2. AC-3. AC-5. AC-6. AC-16
		PR.AC-5: Integralność sieci jest chroniona, łącznie z segregacją sieci, w miarę możliwości	• **ISA 62443-2-1:2009** 4.3.3 4 • **ISA 62443-3-3:2013** SR 3.1. SR 3.8 • **ISO/IEC 27001:2013** A.13.1.1. A.13.1.3. A.13.2.1 • **NIST SP 800-53 Wer. 4** AC-4. SC-7
	Świadomość i szkolenie (PR.AT): Personel i partnerzy organizacji mają zapewnioną edukację w zakresie wiedzy na temat cyberbezpieczeństwa i zostali odpowiednio przeszkoleni do wykonywania swoich obowiązków i odpowiedzialności związanych z bezpieczeństwem, zgodnie z odpowiednimi strategiami, procedurami i umowami.	**PR.AT-1:** Wszyscy użytkownicy zostali poinformowani i przeszkoleni	• **CCS CSC** 9 • **COBIT 5** APO07.03. BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4 2 • **ISO/IEC 27001:2013** A.7.2.2 • **NIST SP 800-53 Wer. 4** AT-2. PM-13
		PR.AT-2: Uprzywilejowani użytkownicy rozumieją role i odpowiedzialności	• **CCS CSC** 9 • **COBIT 5** APO07.02. DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.4.2. 4.3.2.4.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Wer. 4** AT-3. PM-13
		PR.AT-3: Interesariusze zewnętrzni (np. dostawcy, klienci, partnerzy) rozumieją role i odpowiedzialności	• **CCS CSC** 9 • **COBIT 5** APO07.03, APO10.04. APO10.05 • **ISA 62443-2-1:2009** 4.3.2 4,2 • **ISO/IEC 27001:2013** A.6.1.1. A.7.2.2 • **NIST SP 800-53 Wer. 4** PS-7. SA-9

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
		PR.AT-4: Zarząd wyższego szczebla rozumie role i odpowiedzialności	• **CCS CSC** 9 • **COBIT 5** APO07.03

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
			• **ISA 62443-2-1:2009** 4.3.2.4 2 • **ISO/IEC 27001:2013** A.6.1.1. A.7.2.2. • **NIST SP 800-53 Wer. 4** AT-3. PM-13
		PR.AT-5: Personel ds. bezpieczeństwa fizycznego i informacji rozumie role i odpowiedzialności	• **CCS CSC** 9 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.42 • **ISO/IEC 27001:2013** A.6.1.1. A.7.2.2. • **NIST SP 800-53 Wer. 4** AT-3. PM-13
	Bezpieczeństwo danych (PR.DS): Informacje i dokumentacja (dane) kontrolowane są zgodnie ze strategią ryzyka w organizacji, aby chronić poufność, integralność i dostępność informacji.	**PR.DS-1:** Dane stacjonarne są chronione	• **CCS CSC** 17 • **COBIT 5** APO01.06. BAI02.01. BAI06.01. DSS06.06 • **ISA 62443-3-3:2013** SR 3.4. SR 4.1 • **ISO/IEC 27001:2013** A.8.2.3 • **NIST SP 800-53 Wer. 4** SC-28
		PR.DS-2: Dane przesyłane są chronione	• **CCS CSC** 17 • **COBIT 5** APO01.06. DSS06.06 • **ISA 62443-3-3:2013** SR 3.1. SR 3.8. SR 4.1. SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3. A.13.1.1. A.13.2.1. A.13.2.3. A.14.1.2. A.14.1.3 • **NIST SP 800-53 Wer. 4** SC-8
		PR.DS-3: Aktywa są formalnie zarządzane podczas usuwania, przesyłu i użytkowania	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4. 4.3.3.3.9. 4.3.4.4.1 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3. A.8.3.1. A.8.3.2. A.8.3.3, A. 11.2.7 • **NIST SP 800-53 Wer. 4** CM-8. MP-6. PE-16
		PR.DS-4: Utrzymana jest odpowiednia wydajność dla zapewnienia dostępności	• **COBIT 5** APO13.01 • **ISA 62443-3-3:2013** SR 7.1. SR 7.2 • **ISO/IEC 27001:2013** A.12.3.1

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
			• **NIST SP 800-53 Wer. 4** AU-4, CP-2, SC-5
		PR.DS-5: Ochrona przed wyciekami danych jest wdrożona	• **CCS CSC** 17 • **COBIT 5** APO01.06 • **ISA 62443-3-3:2013** SR 5.2 • **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2. A.8.2.3, A.9.1.1, A.9.1.2. A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3. A.13.2.4, A.14.1.2. A.14.1.3 • **NIST SP 800-53 Wer. 4** AC-4. AC-5, AC-6, PE-19, PS-3, PS-6. SC-7. SC-8. SC-13. SC-31. SI-4
		PR.DS-6: Mechanizmy kontroli integralności służą do weryfikacji software, firmware i integralności informacji	• **ISA 62443-3-3:2013** SR 3.1. SR 3.3. SR 3.4. SR 3.8 • **ISO/IEC 27001:2013** A.12.2.1. A.12.5.1. A.14.1.2. A.14.1.3 • **NIST SP 800-53 Wer. 4** SI-7
		PR.DS-7: Środowisko opracowywania i testowania jest oddzielone od środowiska produkcyjnego	• **COBIT 5** BAI07.04 • **ISO/IEC 27001:2013** A.12.1.4 • **NIST SP 800-53 Wer. 4** CM-2
	Procesy i procedury ochrony informacji (PR.IP): Strategia, procesy i procedury bezpieczeństwa (odnoszące się do celów, zakresu, ról, odpowiedzialności, zaangażowania zarządu i koordynacji pomiędzy jednostkami organizacji) są utrzymywane i wykorzystywane do zarządzania ochroną systemów informacyjnych i aktywów.	**PR.IP-1:** Podstawowa konfiguracja systemów technologii informacyjnych / sterowania przemysłowego została utworzona i jest utrzymywana	• **CCS CSC** 3.10 • **COBIT 5** BAI10.01. BAI10.02. BAI10.03. BAI10.05 • **ISA 62443-2-1:2009** 4.3.4.3.2. 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2. A.12.5.1. A.12.6.2. A.14.2.2. A.14.2.3. A.14.2.4 • **NIST SP 800-53 Wer. 4** CM-2. CM-3. CM-4. CM-5. CM-6. CM-7. CM-9. SA-10
		PR.IP-2: Cykl Życia Opracowania Systemu dla celów zarządzania systemami jest wdrożony	• **COBIT 5** APO 13.01 • **ISA 62443-2-1:2009** 4.3.4.3 3 • **ISO/IEC 27001:2013** A.6.1.5. A.14.1.1. A. 14.2.1. A. 14.2.5

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
			• **NIST SP 800-53 Wer. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Opracowane zostały procesy kontroli zmiany konfiguracji	**COBIT 5** BAI06.01, BAI01.06 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Wer. 4** CM-3, CM-4, SA-10
		PR.IP-4: Okresowo tworzone, utrzymywane i testowane są kopie zapasowe informacji	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.9 • **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • **NIST SP 800-53 Wer. 4** CP-4, CP-6, CP-9
		PR.IP-5: Strategia i przepisy dotyczące fizycznego środowiska roboczego względem aktywów organizacyjnych są wypełnione	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • **NIST SP 800-53 Wer. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Dane niszczone są zgodnie ze strategią	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.4.4.4 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • **NIST SP 800-53 Wer. 4** MP-6
		PR.IP-7: Procesy ochrony są stale doskonalone	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3,

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
	4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **NIST SP 800-53 Wer. 4** CA-2, CA-7, CP-2, IR-		

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
			8. PL-2. PM-6
		PR.IP-8: Informacje na temat skuteczności technologii zabezpieczających są przesyłane odpowiednim stronom	• **ISO/IEC 27001:2013** A. 16.1.6 • **NIST SP 800-53 Wer. 4** AC-21. CA-7. SI-4
		PR.IP-9: Plany reagowania (Reagowanie na Incydenty i Ciągłość Działania) i plany przywracania (Przywracanie of Incydencie i Przywracanie Po Katastrofie) zostały opracowane i są kontrolowane	• **COBIT 5** DSS04.03 • **ISA 62443-2-1:2009** 4.3.2.5.3. 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.1. A.17.1.1. A. 17.1.2 • **NIST SP 800-53 Wer. 4** CP-2. IR-8
		PR.IP-10: Plany reagowania i przywracania są testowane	• **ISA 62443-2-1:2009** 4.3.2.5.7. 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Wer.4** CP-4. IR-3. PM-14
		PR.IP-11: Cyberbezpieczeństwo uwzględnione jest w procesach związanych z zasobami ludzkimi (np. usuwanie danych i dostępu, przesiew personelu)	• **COBIT 5** APO07.01. APO07.02. APO07.03, APO07.04. APO07.05 • **ISA 62443-2-1:2009** 4.3.3.2.1. 4.3.3.2.2. 4.3.3.2.3 • **ISO/IEC 27001:2013** A.7.1.1. A.7.3.1. A.8.1.4 • **NIST SP 800-53 Wer. 4** Grupa PS
		PR.IP-12: Plan zarządzania słabościami jest opracowany i wdrożony	• **ISO/IEC 27001:2013** A.12.6.1. A.18.2.2 • **NIST SP 800-53 Wer. 4** RA-3. RA-5. SI-2
	Utrzymanie (PR.MA): Utrzymanie i naprawy składników systemu sterowania i informacyjnego realizowane jest spójnie ze strategiąi procedurami.	**PR.MA-1:** Utrzymanie i naprawa aktywów organizacyjnych jest realizowana i rejestrowana w odpowiednim czasie za pomocą dopuszczonych do użytku i kontrolowanych narzędzi.	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.3.3 7 • **ISO/IEC 27001:2013** A.11.1.2. A.11.2.4. A.ll.2.5 • **NIST SP 800-53 Wer. 4** MA-2. MA-3. MA-5

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
		PR.MA-2: Zdalna konserwacja aktywów organizacyjnych jest dopuszczona do użytku, rejestrowana i realizowana w sposób zapobiegający nieuprawnionemu dostępowi.	• **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5. 4.3.3.6.6. 4.3.3.6.7. 4.4.4.6.8 • **ISO/IEC 27001:2013** A.11.2.4. A. 15.1.1. A.15.2.1

		Informative References
Technologia zabezpieczająca (PR.PT): Rozwiązania dotyczące bezpieczeństwa technicznego są kontrolowane po to, by zapewnić bezpieczeństwo i wytrzymałość systemów i aktywów, zgodnie z polityką, procedurami i umowami.	**PR.PT-1:** Dokumenty audytowe / raporty są określone, udokumentowane, wdrożone i kontrolowane zgodnie ze strategią	• **NIST SP 800-53 Wer. 4** MA-4 • **CCS CSC** 14 • **COBIT 5** APO11.04 • **ISA 62443-2-1:2009** 4.3.3.3.9. 4.3.3.5.8. 4.3.4.4.7. 4.4.2.1. 4.4.2.2. 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8. SR 2.9. SR 2.10. SR 2.11. SR 2.12 • **ISO/IEC 27001:2013** A.12.4.1. A.12.4.2. A. 12.4.3, A. 12.4.4, A.12.7.1 • **NIST SP 800-53 Wer. 4** Grupa AU • **COBIT 5** DSS05.02. APO13.01
	PRPT-2: Wyjmowalne nośniki są chronione, a ich użycie odbywa się zgodnie ze strategią	• **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.2. A.8.2.3. A.8.3.1. A.8.3.3. A.11.2.9 **NIST SP 800-53 Wer. 4** MP-2. MP-4. MP-5. MP-7
	PR.PT-3: Dostęp do systemów i aktywów jest kontrolowany, wykorzystując zasadę najmniejszej funkcjonalności	**COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.3.3.5.1. 4.3.3.5.2. 4.3.3.5.3. 4.3.3.5.4. 4.3.3.5.5. 4.3.3.5.6. 4.3.3.5.7. 4.3.3.5.8. 4.3.3.6.1, 4.3.3.6.2. 4.3.3.6.3. 4.3.3.6.4. 4.3.3.6.5. 4.3.3.6.6. 4.3.3.6.7. 4.3.3.6.8. 4.3.3.6.9. 4.3.3.7.4. 4.3.3.7.2.4.3.3.7.3.4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1. SR 1.2. SR 1.3 kJIV kJIV 1., SR 1.4. SR 1.5. SR 1.6. SR 1.7. SR 1.8. SR 1.9. SR 1.10. SR 1.11. SR 1.12, SR 1.13. SR 2.1. SR 2.2. SR 2.3. SR 2.4. SR 2.5. SR 2.6. SR 2.7 • **ISO/IEC 27001:2013** A.9.1.2 • **NIST SP 800-53 Wer. 4** AC-3. CM-7
	PR.PT-4: Sieci komunikacyjne i sterujące są chronione .	• **CCS CSC** 7 **COBIT 5** DSS05.02. APO13.01 **ISA 62443-3-3:2013** SR 3.1. SR 3.5. SR 3.8 SR 4.1, SR 4.3, SR5.1. SR 5.2. SR 5.3. SR 7.1.

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
			SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1. A.13.2.1 • **NIST SP 800-53 Wer. 4** AC-4. AC-17. AC-18. CP-8. SC-7
DETEKCJA (DE)	**Anomalie i zdarzenia (DE.AE):** Nietypowe zdarzenia wykrywane są w odpowiednim momencie, a ich potencjalny wpływ jest znany.	**DE.AE-1:** Podstawy operacji sieciowych i oczekiwane przepływy danych odnośnie użytkowników i systemów są opracowane i kontrolowane.	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3 3 • **NIST SP 800-53 Wer. 4** AC-4. CA-3. CM-2. SI-4
		DE.AE-2: Wykryte zdarzenia są analizowane, by zrozumieć cele i metody ataku	• **ISA 62443-2-1:2009** 4.3.4.5.6. 4.3.4.5.7. 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8. SR 2.9, SR 2.10, SR 2.11. SR 2.12. SR 3.9. SR 6.1. SR 6.2 • **ISO/IEC 27001:2013** A.16.1.1. A.16.1.4 • **NIST SP 800-53 Wer. 4** AU-6. CA-7. IR-4. SI-4
		DE.AE-3: Dane dotyczące zdarzeń z wielu źródeł i czujników są zbierane i korelowane	• **ISA 62443-3-3:2013** SR 6.1 • **NIST SP 800-53 Wer. 4** AU-6. CA-7. IR-4. IR-S' IR-8. SI-4
		DE.AE-4: Wpływ zdarzeń jest określony	• **COBIT 5** APO12.06 • **NIST SP 800-53 Wer. 4** CP-2. IR-4. RA-3. SI - 4
		DE.AE-5: Wartości progowe alarmowania incydentów są opracowane	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.2.3.10 • **NIST SP 800-53 Wer. 4** IR-4. IR-5, IR-8
	Ciągłe monitorowanie bezpieczeństwa (DE.CM): System informacyjny i aktywa są monitorowane w regularnych odstępach czasu, by zidentyfikować zdarzenia związane z cyberbezpieczeństwem i sprawdzić skuteczność środków zabezpieczających.	**DE.CM-1:** Sieć jest monitorowana, by wykrywać potencjalne zdarzenia związane z cyberbezpieczeństwem	• **CCS CSC** 14. 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Wer. 4** AC-2. AU-12. CA-7. CM-3. SC-5. SC-7. SI-4
		DE.CM-2: Środowisko fizyczne jest	• **ISA 62443-2-1:2009** 4.3.3.3.8

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
		Monitorowane, by wykrywać potencjalne zdarzenia związane z cyberbezpieczeństwem	• **NIST SP 800-53 Wer. 4** CA-7. PE-3. PE-6. PE-20
		DE.CM-3: Czynności personelu są monitorowane, by wykrywać potencjalne zdarzenia związane z cyberbezpieczeństwem	• **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A. 12.4.1 • **NIST SP 800-53 Wer. 4** AC-2. AU-12. AU-13. CA-7. CM-10. CM-11
		DE.CM-4: Szkodliwe kody są wykrywane	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.3.4.3.8 • **ISA 62443-3-3:2013** SR 3.2 • **ISO/IEC 27001:2013** A. 12.2.1 • **NIST SP 800-53 Wer. 4** SI-3
		DE.CM-5: Wykrywane są nieuprawnione kody mobilne	• **ISA 62443-3-3:2013** SR 2.4 • **ISO/IEC 27001:2013** A. 12.5.1 • **NIST SP 800-53 Wer. 4** SC-18. SI-4. SC-44
		DE.CM-6: Monitorowane są poczynania zewnętrznego dostawcy usług, by wykrywać potencjalne zdarzenia związane z cyberbezpieczeństwem	• **COBIT 5** APO07.06 • **ISO/IEC 27001:2013** A.14.2.7. A.15.2.1 • **NIST SP 800-53 Wer. 4** CA-7. PS-7. SA-4. SA-9, SI-4
		DE.CM-7: Realizowane jest monitorowanie nieupoważnionego personelu, podłączeń, urządzeń i oprogramowania	• **NIST SP 800-53 Wer. 4** AU-12. CA-7. CM-3. CM-8, PE-3. PE-6. PE-20. SI-4
		DE.CM-8: Realizowane jest skanowanie słabości	• **COBIT 5** BAI03.10 • **ISA 62443-2-1:2009** 4.2.3.1. 4.2.3.7 • **ISO/IEC 27001:2013** A. 12.6.1 • **NIST SP 800-53 Wer. 4** RA-5
	Procesy detekcji (DE.DP): Procesy i procedury detekcji są utrzymywane i testowane, aby zapewnić odpowiednią	**DE.DP-1:** Role i odpowiedzialności w zakresie detekcji są dobrze zdefiniowane, by zapewnić odpowiedzialność	• **CCS CSC** 5 • **COBIT5** DSS05.01 • **ISA 62443-2-1:2009** 4.4.3.1 • **ISO/IEC 27001:2013** A.6.1.1

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
	wiedzę na temat nietypowych zdarzeń w odpowiednim czasie.		• **NIST SP 800-53 Wer. 4** CA-2, CA-7, PM-14
		DE.DP-2: Czynności związane z detekcją spełniają wszystkie obowiązujące wymagania	• **ISA 62443-2-1:2009** 4.4.3.2 • **ISO/IEC 27001:2013** A.18.1.4 • **NIST SP 800-53 Wer. 4** CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Procesy detekcji zostały przetestowane	• **COBIT 5** APO13.02 • **ISA 62443-2-1:2009** 4.4.3.2 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.14.2.8 • **NIST SP 800-53 Wer. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Informacja na temat detekcji zdarzenia przekazywana jest odpowiednim stronom	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.9 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Wer. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Procesy detekcji są stale doskonalone	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Wer. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
REAKCJA (RS)	**Planowanie reakcji (RS.RP):** Procesy i procedury reagowania są realizowane i utrzymywane, aby zapewnić odpowiednią reakcję na wykryte zdarzenia związane z cyberbezpieczeństwem	**RS.RP-1:** Plan reakcji realizowany jest podczas lub po zdarzeniu	• **COBIT 5** BAIO 1.10 • **CCS CSC** 18 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A. 16.1.5 • **NIST SP 800-53 Wer. 4** CP-2. CP-10. IR-4, IR-8
	Komunikacja (RS.CO): Czynności związane z reakcją są koordynowane z wewnętrznymi i zewnętrznymi interesariuszami, by uwzględnić zewnętrzne wsparcie przedstawicieli prawa.	**RS.CO-1:** W przypadku, gdy wymagana jest reakcja, personel zna swoje role i kolejność działań	• **ISA 62443-2-1:2009** 4.3.4.5.2. 4.3.4.5.3. 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A. 16.1.1 • **NIST SP 800-53 Wer. 4** CP-2, CP-3. IR-3, IR-8
		RS.CO-2: Zdarzenia zgłaszane są zgodnie z ustalonymi kryteriami	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A. 16.1.2 • **NIST SP 800-53 Wer. 4** AU-6, IR-6. IR-8
		RS.CO-3: Informacje przekazywane są zgodnie z planami reagowania	• **ISA 62443-2-1:2009** 4.3.4.5 2 • **ISO/IEC 27001:2013** A. 16.1.2 • **NIST SP 800-53 Wer. 4** CA-2, CA-7. CP-2, IR-4, IR-8. PE-6, RA-5, SI-4
		RS.CO-4: Koordynacja z interesariuszami odpowiada planom reagowania	• **ISA 62443-2-1:2009** 4.3.4.5 5 • **NIST SP 800-53 Wer. 4** CP-2. IR-4, IR-8
		RS.CO-5: Ustanowione jest dobrowolne dzielenie się informacjami z zewnętrznymi interesariuszami dla osiągnięcia większej wiedzy sytuacyjnej związanej z cyberbezpieczeństwem	• **NIST SP 800-53 Wer. 4** PM-15. SI-5
	Analiza (RS.AN): Analiza przeprowadzana jest aby zapewnić odpowiednią reakcję i wsparcie czynności naprawczych.	**RS. AN-1:** Powiadomienia z systemów detekcji są weryfikowane	• **COBIT 5** DSS02.07 • **ISA 62443-2-1:2009** 4.3.4.5.6. 4.3.4.5.7. 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1. A.12.4.3. A.16.1.5 • **NIST SP 800-53 Wer. 4** AU-6, CA-7, IR-4, IR-

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
PRZYWRACANIE (RC)			5. PE-6. SI-4
		RS.AN-2: Wpływ incydentu jest zrozumiany	• **ISA 62443-2-1:2009** 4.3.4.5.6. 4.3.4.5.7. 4.34.5.8 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Wer. 4** CP-2. IR-4
		RS.AN-3: Czynności dochodzeniowe są realizowane	• **ISA 62443-3-3:2013** SR 2.8. SR 2.9. SR 2.10. SR 2.11. SR 2.12. SR 3.9. SR 6.1 • **ISO/IEC 27001:2013** A.16.1.7 • **NIST SP 800-53 Wer. 4** AU-7. IR-4
		RS.AN-4: Incydenty są zaklasyfikowane jako zgodnie z planami reagowania	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISO/IEC 27001:2013** A. 16.1.4 • **NIST SP 800-53 Wer. 4** CP-2. IR-4. IR-5. IR-8
	Łagodzenie (RS.MI): Realizowane są czynności, aby zapobiec propagacji zdarzenia dla łagodzenia jego skutków i jego likwidowania	**RS.MI-1:** Incydenty są kontrolowane	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISA 62443-3-3:2013** SR 5.1. SR 5.2. SR 5.4 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Wer. 4** IR-4
		RS.MI-2: Incydenty są minimalizowane	• **ISA 62443-2-1:2009** 4.3.4.5.6. 4.3.4.5.10 • **ISO/IEC 27001:2013** A.12.2.1. A.16.1.5 • **NIST SP 800-53 Wer. 4** IR-4
		RS.MI-3: Nowo zidentyfikowane słabości są minimalizowane lub dokumentowane jako dopuszczalne ryzyko	• **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Wer. 4** CA-7. RA-3. RA-5
	Usprawnienia (RS.IM): Organizacyjne czynności związane z reagowaniem są doskonalone, wykorzystując doświadczenia z obecnych i przyszłych czynności detekcji / reakcji.	**RS.IM-1:** Plany reagowania obejmują pozyskane doświadczenia	• **COBIT 5** BAI01.13 • **ISA 62443-2-1:2009** 4.3.4.5.10. 1934-04-04 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Wer. 4** CP-2. IR-4. IR-8
		RS.IM-2: Strategie reagowania są aktualizowane	• **NIST SP 800-53 Wer. 4** CP-2. IR-4. IR-8

	Planowanie przywracania (RC.RP): Procesy i procedury przywracania są realizowane i utrzymywane, aby zapewnić odpowiednie	**RC.RP-1:** Plan przywracania realizowany jest podczas lub po zdarzeniu	• **CCS CSC** 8 • **COBIT 5** DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5

Funkcja	Kategoria	Podkategoria	Odniesienia Informacyjne
	przywrócenie systemów lub aktywów dotkniętych zdarzeniem cybernetycznym.		• **NIST SP 800-53 Wer. 4** CP-10. IR-4. IR-8
	Usprawnienia (RC.IM): Planowanie i procesy przywracania są doskonalone, wykorzystując doświadczenia w przyszłych czynnościach	**RC.IM-1:** Plany przywracania obejmują pozyskane doświadczenia	• **COBIT 5** BAI05.07 • **ISA 62443-2-1:2009** 4.4.3 4 • **NIST SP 800-53 Wer. 4** CP-2. IR-4. IR-8
		RC.IM-2: Strategie przywracania są aktualizowane	• **COBIT 5** BAI07.08 • **NIST SP 800-53 Wer. 4** CP-2. IR-4. IR-8
	Komunikacja (RC.CO): Czynności przywracania są koordynowane ze stronami wewnętrznymi i zewnętrznymi, na przykład centrami koordynacji, Dostawcami Usług Internetowych, właścicielami systemów atakujących, ofiarami, innymi CSIRT i dostawcami.	**RC.CO-1:** Kwestie związane z PR są kontrolowane	• **COBIT 5 EDM03.02**
		RC.CO-2: Reputacja po zdarzeniu została naprawiona	• **COBIT 5** MEA03.02
		RC.CO-3: Informacje na temat czynności związanych z przywróceniem zostały przekazane wewnętrzny interesariuszom, zarządowi wykonawczemu i zespołom kierowniczym	• **NIST SP 800-53 Wer. 4** CP-2, IR-4

Informacje dotyczące Odniesień Informacyjnych opisanych w Załączniku A znaleźć można w:

- Cele Kontroli dla Technologii Informatycznych i Powiązanych (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Rada ds. Cyberbezpieczeństwa (CCS) Najważniejszych 20 Krytycznych Kontroli Bezpieczeństwa (CSC): http://www.counciloncybersecurity.org
- ANSI/ISA-62443-2-1 (99.02.01)-2009, *Bezpieczeństwo Przemysłowej Automatyzacji i Systemów Kontroli: Ustanowienie Programu Bezpieczeństwa Przemysłowej Automatyzacji i Systemów Kontroli.* httD://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisDlay.cfm&ProductID=10243
- ANSVISA-62443-3-3 (99.03.03)-2013, *Bezpieczeństwo Przemysłowej Automatyzacji i Systemów Kontroli: Wymagania i Poziomy Kontroli Systemów Bezpieczeństwa.* http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420
- ISO/IEC 27001-1, *Technologia informacyjna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania* http://www.iso.org/iso/home/store/catalogue ics/catalogue detail ics.htm?csnumber=54534
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, *Kontrole Bezpieczeństwa i Prywatności Federalnych Systemów Informatycznych i Organizacji,* kwiecień 2013 (łącznie z aktualizacją z 15 stycznia 2014). http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Mapowania pomiędzy Podkategoriami Rdzenia Ram i określonymi sekcjami w Odniesieniach Informacyjnych wskazują ogólne powiązanie, a ich celem nie jest definitywne określenie tego, czy określone rozdziały w Odniesieniach Informacyjnych zapewniają dany wynik Podkategorii.

Załącznik B: Glosariusz

W załączniku tym zdefiniowano wybrane pojęcia stosowane w publikacji.

Kategoria	Podpodział Funkcji na grupy wyników cyberbezpieczeństwa ściśle powiązanych z programowymi potrzebami i określonymi czynnościami. Przykładami kategorii są „Zarządzanie Aktywami”, „Kontrola Dostępu” i „Procesy Detekcji”.
Infrastruktura Krytyczna	Systemy i aktywa, fizyczne lub wirtualne, tak istotne dla Stanów Zjednoczonych, że niewydolność lub zniszczenie takich systemów i aktywów miałoby osłabiający wpływ na bezpieczeństwo, bezpieczeństwo ekonomiczne kraju, zdrowie i bezpieczeństwo publiczne lub ich kombinacje.
Cyberbezpieczeństwo	Proces ochrony informacji w drodze zapobiegania, wykrywania i reagowania na ataki.
Zdarzenie Cyberbezpieczeństwa	Zmiana cyberbezpieczeństwa, która może mieć wpływ na operacje organizacyjne (łącznie z misją, możliwościami i reputacją).
Detekcja (funkcja)	Opracowanie i wdrożenie odpowiednich czynności, w celu zidentyfikowania wystąpienia zdarzenia związanego z cyberbezpieczeństwem.
Ramy	Podejście na bazie ryzyka dotyczące redukcji zagrożeń cybernetycznych, składające się z trzech części: Rdzenia Ram, Profilu Ram i Poziomów Wdrożeń Ram. Znane również jako „Ramy Cyberbezpieczeństwa”.
Rdzeń Ram	Zbiór czynności związanych z cyberbezpieczeństwem i referencji wspólnych dla wszystkich sektorów krytycznej infrastruktury i odnoszą się do określonych wyników. Rdzeń Ram składa się z czterech rodzajów elementów: Funkcje, Kategorie, Podkategorie i Odniesienia Informacyjne
Poziom Wdrożenia Ramy	Soczewka, za pomocą której zobaczyć można charakterystykę podejścia organizacji do ryzyka – to, w jaki sposób organizacja widzi ryzyko cybernetyczne i procesy w celu złagodzenia zagrożeń.
Profil Ram	Przedstawienie wyników, którą określony system lub organizacja wybrała spośród Kategorii i Podkategorii Ram.

Funkcja	Jeden z głównych komponentów Ram. Funkcje stanowią najwyższy szczebel struktury dla celów zorganizowania czynności cyberbezpieczeństwa do postaci Kategorii i Podkategorii. Pięcioma tymi funkcjami są Identyfikacja,

	Ochrona, Detekcja, Reagowanie i Przywracanie.
Identyfikacja (funkcja)	Rozwija organizacyjne zrozumienie pozwalające zarządzać zagrożeniami związanymi z cyberbezpieczeństwem systemów, aktywów, danych i możliwości.
Informacyjne	Określone rozdziały norm, wytycznych i praktyk ogólne pośród sektorów infrastruktury krytycznej, przedstawiające sposób osiągnięcia wyników związanych z każdą Podkategorią. Przykładem Odniesień Informacyjnych jest norma ISO/IEC 27001 Kontrola A. 10.8.3, która odnosi się do Podkategorii „Dane przesyłane są chronione" Kategorii „Bezpieczeństwo Danych" Funkcji „Ochrona".
Kod mobilności	Program (np. skrypt, makro lub inna funkcja przenośna), który można przesłać w postaci niezmienionej do heterogenicznego zbioru platform i zrealizować dzięki identycznej składni.
Ochrona (funkcja)	Pozwala opracować i wdrożyć odpowiednie środki ochrony, by zapewnić zrealizowanie najważniejszych usług infrastrukturalnych.
Uprzywilejowany użytkownik	Użytkownik upoważniony jest (a tym samym zaufany) do pełnienia odpowiednich funkcji bezpieczeństwa, których zwykli użytkownicy nie mogą wykonywać.
Przywracanie (funkcja)	Opracowanie i wdrożenie odpowiednich czynności w celu utrzymania planów odporności i przywrócenia możliwości lub usług, na które wpływ miało zdarzenie cybernetyczne.
Reakcja (funkcja)	Opracowanie i wdrożenie odpowiednich czynności, w celu podjęcia działania związanego z cyberbezpieczeństwem.
Ryzyko	Miara stopnia w jakim jednostka jest zagrożona przez potencjalne okoliczności lub zdarzenie i zazwyczaj jest funkcją: (i) niekorzystnego wpływu do jakiego może dojść w przypadku wystąpienia okoliczności lub zdarzeń; i (ii) prawdopodobieństwo zdarzenia.
Zarządzanie Ryzykiem	Proces identyfikacji, oceny i reagowania na ryzyko.
Podkategoria	Podpodział Kategorii zapewniający określone wyniki czynności technicznych i / lub zarządzania. Przykłady Podkategorii obejmują „Zewnętrzne systemy informacyjne są skatalogowane", „Dane stacjonarne są chronione" i „Powiadomienia z systemów detekcji są kontrolowane".

Załącznik C: Akronimy

W załączniku tym zdefiniowano wybrane pojęcia stosowane w publikacji.

CCS	Council on CyberSecurity [Rada ds. Cyberbezpieczeństwa]
COBIT	Control Objectives for Information and Related Technology
DCS	Distributed Control System [Rozproszony System Sterowania]
DHS	Department of Homeland Security [Departament Bezpieczeństwa Krajowego]
EO	Executive Order [Dekret]
ICS	Industrial Control Systems [Przemysłowe Systemy Sterowania]
IEC	International Electrotechnical Commission [Międzynarodowa Komisja Elektrotechniczna]
IR	Interagency Report [Wewnętrzny Raport Agencji]
ISA	International Society of Automation [Międzynarodowe Stowarzyszenie Automatyki]
ISAC	Information Sharing and Analysis Center [Centrum Wymiany i Analizy Informacji]
ISO	International Organization for Standardization (Międzynarodowa Organizacja Normalizacyjna)
IT	Technologia Informacyjna
NIST	Instytut Narodowy ds. Norm i Technologii
RFI	Request for Information [Prośba o Informacje]
RMP	Risk Management Process [Proces Zarządzania Ryzykiem]
SCADA	Supervisory Control and Data Acquisition [System Kontroli Nadzorczej i Gromadzenia Danych]
SP	Special Publication [Publikacja Specjalna]