NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	Narodowy Standard Cyberbezpieczeństwa		
Nazwa standardu	Symbol	Wersja	Data wydania
Zarządzanie ryzykiem bezpieczeństwa informacji *Przegląd struktury organizacyjnej, misji i systemu informatycznego*	**NSC 800-39**	1.0	01/04/2022

Zarządzanie ryzykiem bezpieczeństwa informacji

Przegląd struktury organizacyjnej, misji i systemu informatycznego

PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA

Warszawa 2022

Szanowni Państwo,

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

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

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

- NSC[2] 199, *Standardy kategoryzacji bezpieczeństwa* – na podstawie FIPS 199;
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych* – na podstawie FIPS 200;
- NSC 500-292, *Architektura referencyjna chmury obliczeniowej – rekomendacje* – na podstawie NIST SP 500-292;
- NSC 800-18, *Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych* – na podstawie NIST SP 800- 18;

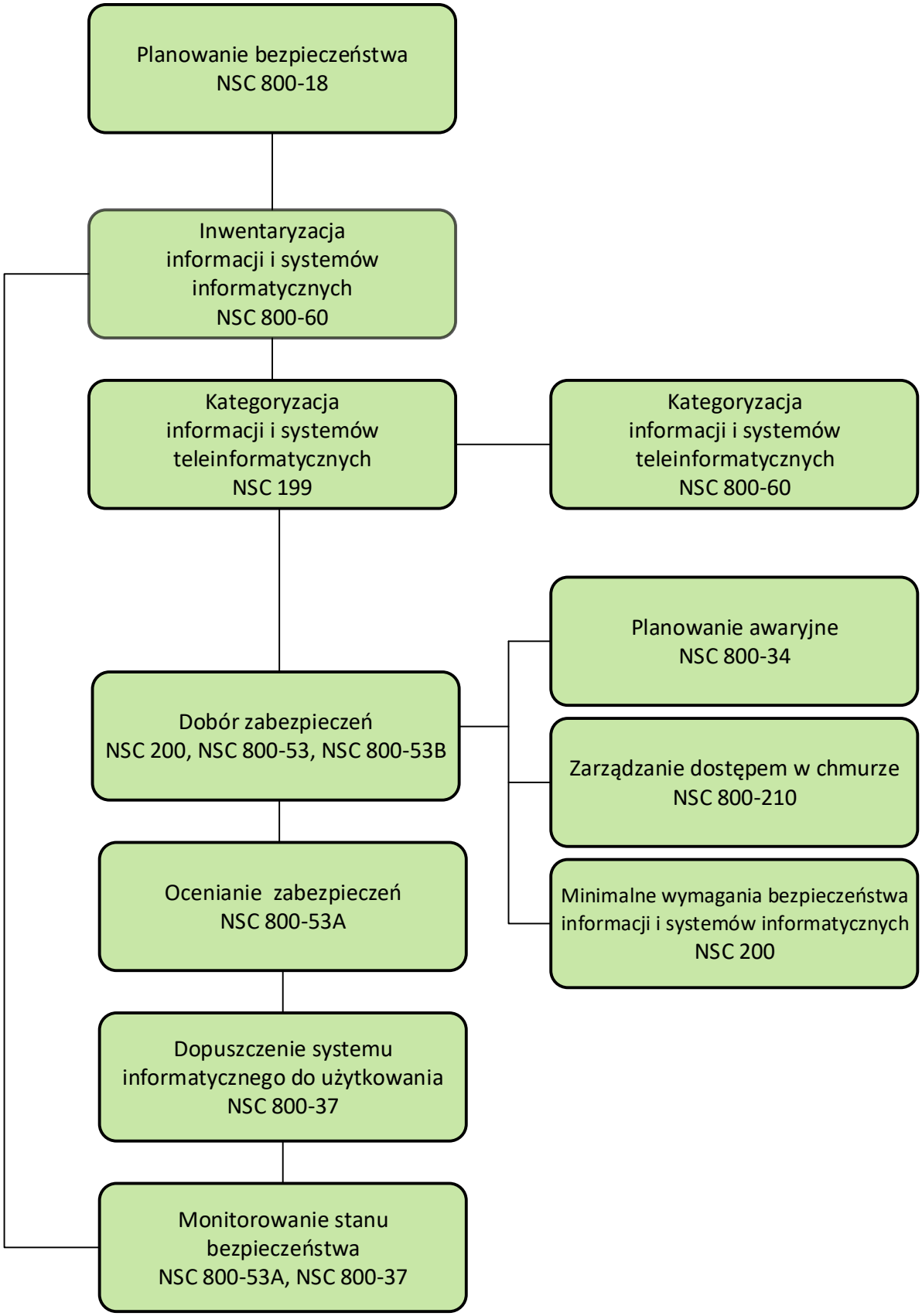
[1] Wymienione są podstawowe dokumenty. Każdy z nich może się odwoływać w rozdziale *Referencje* do szeregu powiązanych publikacji, które składają się na całościowy proces osiągania cyberbezpieczeństwa.

[2] NSC – Narodowy Standard Cyberbezpieczeństwa.

- NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne* – na podstawie NIST SP 800-30;
- NSC 800-34, *Poradnik planowania awaryjnego* – na podstawie NIST SP 800-34;
- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* – na podstawie NIST SP 800-37;
- NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53;
- NSC 800-53A, *Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny* – na podstawie NIST SP 800-53A;
- NSC 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53B;
- NSC 800-60, *Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego* – na podstawie NIST SP 800-60;
- NSC 800-61, *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* – na podstawie NIST SP 800-61;
- NSC 800-210, *Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej* – na podstawie NIST SP 800-210.

Korzystając z tych publikacji można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem bazujący na publikacjach NIST wykorzystuje następujące dokumenty:


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

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował wiele standardów i wytycznych w celu zapewnienia wspólnego podejścia do problematyki bezpieczeństwa informacji i systemów teleinformatycznych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji, bezpieczeństwa systemów teleinformatycznych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością operacji organizacyjnych i majątku, osób fizycznych, innych organizacji i Państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informatycznych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych, a także dzięki jednolitemu podejściu, ułatwia wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznymi i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (np. ISO), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania innych standardów.

Publikacje NIST, co do zasady, nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dozwolone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejście do zagadnień związanych z bezpieczeństwem informacji, systemów teleinformatycznych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST, jako godne zaufania i rekomendują stosowanie ich przez polskie podmioty w opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Identyfikacja taka nie ma na celu nakłaniania do nich lub ich poparcia, nie ma też na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w tym obszarze.

W niniejszym Narodowym Standardzie Cyberbezpieczeństwa mogą znajdować się odniesienia do innych publikacji opracowywanych obecnie przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa zgodnie z przypisanymi mu obowiązkami ustawowymi. Informacje zawarte w tej publikacji, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji, obowiązują aktualne wymagania, wytyczne i procedury, jeśli takie istnieją. W celach planistycznych i wprowadzania zmian, organizacje będą mogły uważnie śledzić rozwój tych nowych publikacji opracowywanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Niniejsza publikacja, ***Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informatycznego,*** opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View* (March 2011).

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

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

Prolog

"... W procesie zarządzania ryzykiem, liderzy muszą rozważyć ryzyko interesów Państwa płynące ze strony przeciwników wykorzystujących cyberprzestrzeń do osiągania swoich korzyści oraz ze strony naszych własnych wysiłków zmierzających do wykorzystania globalnego charakteru cyberprzestrzeni do osiągania celów w operacjach wojskowych, wywiadowczych i biznesowych...".

"... Przy opracowywaniu planów operacyjnych, powinna być oceniana kombinacja zagrożeń, podatności i wpływów w celu zidentyfikowania istotnych trendów i podjęcia decyzji, w jakich obszarach należy zastosować stosowne działania, aby wyeliminować lub ograniczyć możliwości zagrożeń; wyeliminować lub ograniczyć podatności; oraz ocenić, skoordynować i dokonać dekonfliktu wszystkich operacji w cyberprzestrzeni..."

"... Liderzy wszystkich szczebli są odpowiedzialni za zapewnienie gotowości i bezpieczeństwa w takim samym stopniu, jak w każdej innej dziedzinie..."

--THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

SPIS TREŚCI

ROZDZIAŁ PIERWSZY WPROWADZENIE 11

1.1. Cel i zastosowanie 14

1.2. Odbiorcy docelowi 15

1.3. Powiązane publikacje 16

1.4. Organizacja niniejszej publikacji 17

ROZDZIAŁ DRUGI PODSTAWY 19

2.1. Elementy zarządzania ryzykiem 19

2.2. Wielopoziomowe zarządzanie ryzykiem 25

2.3. Poziom 1 - widok organizacji 28

2.4. Poziom 2 - widok misji/procesów biznesowych 39

2.5. Poziom 3 - widok systemów informatycznych 47

2.6. Zaufanie i wiarygodność 51

2.7. Kultura organizacyjna 58

2.8. Związek między kluczowymi koncepcjami ryzyka 61

ROZDZIAŁ TRZECI PROCES 65

3.1. Ryzyko ramowe 67

3.2. Ocenianie ryzyka 79

3.3. Reagowanie na ryzyko 88

3.4. Monitorowanie ryzyka 97

ZAŁĄCZNIK A REFERENCJE 108

ZAŁĄCZNIK B SŁOWNIK 112

ZAŁĄCZNIK C AKRONIMY 113

ZAŁĄCZNIK D ROLE I OBOWIĄZKI 114

ZAŁĄCZNIK E ZADANIA PROCESU ZARZĄDZANIA RYZYKIEM 115

ZAŁĄCZNIK F MODELE ZARZĄDZANIA 118

ZAŁĄCZNIK G MODELE ZAUFANIA 120

ZAŁĄCZNIK H STRATEGIE REAGOWANIA NA RYZYKO 124

ROZDZIAŁ PIERWSZY WPROWADZENIE

POTRZEBA INTEGRACJI ZARZĄDZANIA RYZYKIEM W ORGANIZACJI

Technologia informacyjna jest powszechnie uznawana za motor napędzający gospodarkę krajową, dający przemysłowi przewagę konkurencyjną na rynkach światowych, umożliwiający rządowi świadczenie lepszych usług dla obywateli i ułatwiający większą produktywność Państwa. Organizacje[3] w sektorze publicznym i prywatnym są uzależnione od *systemów informatycznych*[4] intensywnie wykorzystujących technologie, aby z powodzeniem realizować swoje misje i funkcje biznesowe. Systemy informatyczne mogą obejmować różnorodne jednostki, począwszy od wysokiej klasy superkomputerów, stacji roboczych, komputerów osobistych, telefonów komórkowych i osobistych asystentów cyfrowych, aż po bardzo wyspecjalizowane systemy (np. systemy uzbrojenia, systemy telekomunikacyjne, systemy sterowania przemysłowego i systemy kontroli środowiska). Systemy informatyczne narażone są na szczególne *zagrożenia,* które mogą mieć negatywny wpływ na działalność organizacyjną (tj. misje, funkcje, wizerunek lub reputację), aktywa organizacyjne, osoby, inne organizacje oraz Państwo, wykorzystując zarówno znane, jak i nieznane podatności w celu narażenia na kompromitację poufności, integralności lub dostępności informacji przetwarzanych, przechowywanych lub przekazywanych przez te systemy. Zagrożenia informacji i systemów informatycznych mogą obejmować celowe ataki, zakłócenia środowiskowe oraz błędy ludzkie i maszynowe, co może skutkować szkodami dla interesów bezpieczeństwa narodowego i gospodarczego Państwa. Z tego względu konieczne jest, aby liderzy i menedżerowie na wszystkich szczeblach rozumieli swoje obowiązki i byli odpowiedzialni za zarządzanie ryzykiem związanym z bezpieczeństwem informacji, czyli ryzykiem związanym z działaniem i wykorzystaniem systemów informatycznych, które wspierają misje i funkcje biznesowe ich organizacji.

[3] Definicja: patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*.

[4] *Tamże.* W kontekście niniejszej publikacji definicja ta obejmuje środowisko, w którym działa system informatyczny (tj. ludzi, procesy, technologie, obiekty i cyberprzestrzeń).

Ryzyko organizacyjne może obejmować wiele rodzajów ryzyka (np. program zarządzania ryzykiem, ryzyko inwestycyjne, ryzyko budżetowe, ryzyko odpowiedzialności prawnej, ryzyko związane z ochroną, ryzyko związane z zapasami, ryzyko związane z łańcuchem dostaw oraz ryzyko związane z bezpieczeństwem). Ryzyko bezpieczeństwa związane z funkcjonowaniem i użytkowaniem systemów informatycznych jest tylko jednym z wielu elementów ryzyka organizacyjnego, którym liderzy wyższego szczebla/kadra zarządzająca zajmują się w ramach swoich obowiązków związanych z zarządzaniem ryzykiem. Skuteczne zarządzanie ryzykiem wymaga, aby organizacje działały w wysoce złożonych, wzajemnie powiązanych środowiskach, korzystając z najnowocześniejszych i dziedziczonych systemów informatycznych - systemów, od których organizacje są uzależnione w realizacji swoich misji i wykonywaniu ważnych funkcji biznesowych. Liderzy muszą zdawać sobie sprawę, że konieczne jest podejmowanie jednoznacznych, świadomych decyzji opartych na analizie ryzyka, aby zrównoważyć korzyści płynące z działania i użytkowania systemów informatycznych z ryzykiem, że te same systemy staną się narzędziem, za pomocą którego celowe ataki, zakłócenia środowiskowe lub błędy ludzkie spowodują niepowodzenie misji lub działalności. Zarządzanie ryzykiem związanym z bezpieczeństwem informacji, podobnie jak zarządzanie ryzykiem w ogóle, nie jest nauką ścisłą. Łączy w sobie najlepsze wspólne oceny osób i grup w organizacjach odpowiedzialnych za planowanie strategiczne, nadzór, zarządzanie i codzienne operacje - zapewniając zarówno niezbędne, jak i wystarczające środki reagowania na ryzyko, aby odpowiednio chronić misje i funkcje biznesowe tych organizacji.

Złożone relacje pomiędzy misjami, procesami biznesowymi oraz systemami informatycznymi wspierającymi te misje/procesy wymagają zintegrowanego, obejmującego całą organizację spojrzenia na zarządzanie ryzykiem[5]. O ile nie określono inaczej, odniesienia do *ryzyka* w niniejszej publikacji dotyczą ryzyka związanego z bezpieczeństwem informacji, wynikającego z działania i użytkowania organizacyjnych systemów informatycznych, w tym procesów, procedur i struktur w organizacji, które wpływają na projektowanie, rozwój,

[5] Agregacja różnych rodzajów ryzyka w całej organizacji wykracza poza zakres niniejszej publikacji.

wdrażanie i bieżące funkcjonowanie tych systemów. Rola bezpieczeństwa informacji w zarządzaniu ryzykiem wynikającym z działania i użytkowania systemów informatycznych jest również kluczowa dla sukcesów organizacji w osiąganiu ich strategicznych celów i zadań. W przeszłości, wyższego szczebla liderzy/kadra kierownicza mieli bardzo wąskie spojrzenie na bezpieczeństwo informacji, albo jako na kwestię techniczną, albo jako na zagadnienie niezależne od ryzyka organizacyjnego i tradycyjnych procesów zarządzania i cyklu życia. Ta niezwykle ograniczona perspektywa często skutkowała niedostatecznym rozważeniem tego, w jaki sposób ryzyko związane z bezpieczeństwem informacji, podobnie jak inne ryzyka organizacyjne, wpływa na prawdopodobieństwo pomyślnej realizacji misji i funkcji biznesowych organizacji. Niniejsza publikacja umieszcza bezpieczeństwo informacji w szerszym kontekście organizacyjnym, jakim jest osiągnięcie sukcesu w realizacji misji/biznesu. Celem jest:

- Zapewnienie, że wyższego szczebla liderzy/kadra kierownicza uznają znaczenie zarządzania ryzykiem związanym z bezpieczeństwem informacji i ustanawiają odpowiednie struktury zarządzania takim ryzykiem.
- Zapewnienie, że proces zarządzania ryzykiem w organizacji jest skutecznie prowadzony na trzech poziomach: organizacji, misji/procesów biznesowych oraz systemów informatycznych.
- Wspieranie atmosfery organizacyjnej, w której ryzyko związane z bezpieczeństwem informacji jest rozważane w kontekście projektowania procesów powiązanych z misją/biznesem, definiowania nadrzędnej architektury korporacyjnej oraz procesów cyklu życia rozwoju systemu.
- Niesienie pomocy osobom odpowiedzialnym za wdrożenie lub eksploatację systemów informatycznych w celu lepszego zrozumienia, w jaki sposób ryzyko związane z bezpieczeństwem informacji związane z ich systemami przekłada się na ryzyko w całej organizacji, które może ostatecznie wpłynąć na powodzenie misji/biznesu.

W celu skuteczniej realizacji misji organizacyjnych i funkcji biznesowych w procesach zależnych od systemów informatycznych, wyższego szczebla liderzy/kadra zarządzająca

muszą być zaangażowani w nadanie zarządzaniu ryzykiem charakteru podstawowego wymogu misji/biznesu. Takie zaangażowanie na najwyższym szczeblu kadry kierowniczej zapewnia dostępność wystarczających zasobów do opracowania i wdrożenia skutecznych, ogólnoorganizacyjnych programów zarządzania ryzykiem. Zrozumienie i uwzględnienie ryzyka jest *strategiczną* zdolnością i *czynnikiem umożliwiającym realizację* misji i funkcji biznesowych w całej organizacji. Efektywne zarządzanie ryzykiem w zakresie bezpieczeństwa informacji w całej organizacji wymaga następujących kluczowych elementów:

- Przypisania odpowiedzialności za zarządzanie ryzykiem liderom/kadrze kierowniczej wyższego szczebla.
- Stałego rozpoznawania i rozumienia przez liderów/kadrę kierowniczą wyższego szczebla ryzyka związanego z bezpieczeństwem informacji odnoszącego się do działań i aktywów organizacji, osób, innych organizacji i Państwa, wynikającego z działania i korzystania z systemów informatycznych.
- Ustanowienia organizacyjnej tolerancji ryzyka i informowanie o tolerancji ryzyka w całej organizacji, w tym udzielanie wytycznych dotyczących wpływu tolerancji ryzyka na bieżące działania decyzyjne[6].
- Ustanowienia odpowiedzialności liderów/kadry kierowniczej wyższego szczebla za podejmowane przez nich decyzje dotyczące zarządzania ryzykiem oraz za wdrażanie skutecznych programów zarządzania ryzykiem w całej organizacji.

1.1. CEL I ZASTOSOWANIE

Publikacja NSC 800-39 jest sztandarowym dokumentem z serii opracowanych rekomendacji dotyczących bezpieczeństwa informacji. Celem publikacji NSC 800-39 jest dostarczenie wytycznych do ustanowienia zintegrowanego, obejmującego całą organizację programu zarządzania ryzykiem w zakresie bezpieczeństwa informacji w działalności organizacji (tj. misji, funkcji, wizerunku i reputacji), aktywów organizacji, osób, innych organizacji i Państwa. NSC 800-39 zapewnia uporządkowane, elastyczne podejście do zarządzania ryzykiem, które

[6] Ocena *ryzyka rezydualnego* (zmieniającego się w czasie) w celu określenia ryzyka akceptowalnego zależy od progu wyznaczonego przez organizacyjną *tolerancję ryzyka*.

jest celowo szeroko zakrojone, a szczegółowe informacje dotyczące szacowania, reagowania i bieżącego monitorowania ryzyka są zawarte w innych wspierających narodowych standardach cyberbezpieczeństwa (NSC). Rekomendacje zawarte w niniejszej publikacji nie mają na celu zastąpienia lub podważenia innych działań, programów, procesów lub podejść związanych z ryzykiem, które organizacje wdrożyły lub zamierzają wdrożyć w odniesieniu do obszarów zarządzania ryzykiem objętych innymi przepisami, dyrektywami, politykami, inicjatywami programowymi lub wymaganiami misji/biznesu. Opisane tu wskazówki dotyczące zarządzania ryzykiem mają charakter uzupełniający i powinny być stosowane, jako część kompleksowego programu zarządzania ryzykiem w przedsiębiorstwie (*ang. Enterprise Risk Management - ERM*).

Rekomendacje zawarte w niniejszej publikacji mają zastosowanie do wszystkich systemów informatycznych innych niż systemy określone, jako systemy bezpieczeństwa narodowego. Zostały opracowane z technicznego punktu widzenia w celu uzupełnienia podobnych zaleceń odnoszących się do systemów bezpieczeństwa narodowego i mogą być stosowane w takich systemach za zgodą odpowiednich organów państwowych sprawujących funkcje władcze nad takimi systemami. Zachęca się organy administracji państwowej, samorządowej i lokalnej, a także organizacje sektora prywatnego do rozważenia zastosowania tych rekomendacji, w zależności od potrzeb.

1.2. ODBIORCY DOCELOWI

Niniejsza publikacja jest przeznaczona dla zróżnicowanej grupy profesjonalistów zajmujących się zarządzaniem ryzykiem, w tym osoby:

- odpowiedzialne za nadzór nad zarządzaniem ryzykiem (np. szefowie agencji, dyrektorzy generalni, dyrektorzy operacyjni);
- odpowiedzialne za realizację misji/funkcji biznesowych organizacji (np. właściciele misji/biznesu, właściciele informacji/władający informacją, osoby autoryzujące);
- odpowiedzialne za nabywanie produktów, usług lub systemów informatycznych (np. personel ds. zakupów, zamówień publicznych, umów);

- odpowiedzialne za nadzór nad bezpieczeństwem informacji, zarządzające bezpieczeństwem i wykonujący obowiązki operacyjne (np. CIO, SAISO/SISO, menadżerowie bezpieczeństwa informacji, właściciele systemów informatycznych, dostawcy zabezpieczeń wspólnych)[7];
- odpowiedzialne za projektowanie, opracowywanie i wdrażanie systemów informatycznych/bezpieczeństwa (np. kierownicy programów, architekci korporacyjni, architekci bezpieczeństwa informacji, inżynierowie systemów informatycznych/bezpieczeństwa; integratorzy systemów informatycznych); oraz
- odpowiedzialne za ocenianie i monitorowanie bezpieczeństwa informacji (np. osoby testujące system, testerzy penetracyjni, osoby oceniające środki bezpieczeństwa, niezależni weryfikatorzy, inspektorzy, audytorzy).

1.3. POWIĄZANE PUBLIKACJE

Podejście do zarządzania ryzykiem opisane w niniejszej publikacji jest wspierane przez szereg standardów bezpieczeństwa i wytycznych niezbędnych do zarządzania ryzykiem związanym z bezpieczeństwem informacji. W szczególności publikacje specjalne opracowane w ramach Inicjatywy Transformacyjnej Połączonych Grup Zadaniowych[8] (*ang. Joint Task Force Transformation Initiative*) wspierające ujednolicone ramy bezpieczeństwa informacji, obejmują:

- NIST SP 800-30, *Guide for Conducting Risk Assessments*[9];
- NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach;*

[7] Opis ról i stanowisk - patrz: NSC 800-37; NSC 7298.

[8] Przegląd każdej publikacji Inicjatywy Transformacyjnej Połączonych Grup Zadaniowych, w formie streszczenia, można uzyskać poprzez odpowiednie biuletyny bezpieczeństwa NIST ITL na stronie http://csrc.nist.gov.

[9] NIST SP 800-39 zastępuje pierwotną publikację specjalną NIST SP 800-30, jako źródło wytycznych dotyczących zarządzania ryzykiem. NIST SP 800-30 jest poddawana przeglądowi w celu zapewnienia wytycznych dotyczących oceny ryzyka, jako dokumentu pomocniczego do publikacji specjalnej NIST SP 800-39.

- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations;* oraz
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*.

Oprócz wymienionych powyżej publikacji Joint Task Force, Międzynarodowa Organizacja Normalizacyjna (*ang. International Organization for Standardization - ISO*) oraz Międzynarodowa Komisja Elektrotechniczna (*ang. International Electrotechnical Commission - IEC*) publikują normy dotyczące zarządzania ryzykiem i bezpieczeństwa informacji, w tym:

- ISO/IEC 31000, *Zarządzanie ryzykiem - Zasady i wytyczne;*
- ISO/IEC 31010, *Zarządzanie ryzykiem - Techniki oceny ryzyka;*
- ISO/IEC 27001, *Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji -- Wymagania*; oraz
- ISO/IEC 27005, *Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania ryzykiem w zakresie bezpieczeństwa informacji*.

Misja NIST obejmuje zharmonizowanie międzynarodowych i krajowych standardów w stosownych przypadkach. Koncepcje i zasady zawarte w niniejszej publikacji mają na celu wdrożenie dla publicznych systemów informatycznych i organizacji, systemu zarządzania bezpieczeństwem informacji oraz procesu zarządzania ryzykiem podobnego do tych opisanych w normach ISO/IEC. Zmniejsza to obciążenie organizacji, które są zobowiązane do przestrzegania zarówno norm ISO/IEC, jak i norm i wytycznych NIST.

1.4. ORGANIZACJA NINIEJSZEJ PUBLIKACJI

Dalsza część tej publikacji jest zorganizowana w następujący sposób:

- **Rozdział drugi** zawiera: (i) elementy zarządzania ryzykiem; (ii) wielopoziomowe podejście do zarządzania ryzykiem; (iii) zarządzanie ryzykiem na poziomie organizacji (warstwa 1); (iv) zarządzanie ryzykiem na poziomie misji/procesu biznesowego (warstwa 2); (v) zarządzanie ryzykiem na poziomie systemu informatycznego (warstwa 3); (vi) ryzyko związane z zaufaniem i wiarygodnością; (vii) wpływ kultury

organizacyjnej na ryzyko; oraz (viii) relacje pomiędzy kluczowymi koncepcjami zarządzania ryzykiem.

- **Rozdział trzeci** opisuje oparty na cyklu życia proces zarządzania ryzykiem w zakresie bezpieczeństwa informacji, w tym: (i) ogólny przegląd procesu zarządzania ryzykiem; (ii) sposób, w jaki organizacje ustalają kontekst dla decyzji opartych na ryzyku; (iii) sposób, w jaki organizacje oceniają ryzyko; (iv) sposób, w jaki organizacje reagują na ryzyko; oraz (v) sposób, w jaki organizacje monitorują ryzyko w czasie.
- **Załączniki** pomocnicze dostarczają dodatkowych informacji z zakresu zarządzania ryzykiem, w tym: (i) referencje ogólne; (ii) definicje i terminy; (iii) akronimy; (iv) role i obowiązki; (v) zadania procesu zarządzania ryzykiem; (vi) modele zarządzania; (vii) modele zaufania; oraz (viii) strategie reagowania na ryzyko.

ROZDZIAŁ DRUGI PODSTAWY

PODSTAWOWE KONCEPCJE ZARZĄDZANIA RYZYKIEM

Niniejszy rozdział opisuje podstawowe koncepcje związane z zarządzaniem ryzykiem w zakresie bezpieczeństwa informacji w organizacji, w tym: (i) elementy zarządzania ryzykiem; (ii) wielopoziomowe podejście do zarządzania ryzykiem; (iii) zarządzanie ryzykiem na poziomie organizacji (warstwa 1); (iv) zarządzanie ryzykiem na poziomie misji/procesu biznesowego (warstwa 2); (v) zarządzanie ryzykiem na poziomie systemu informatycznego (warstwa 3); (vi) zaufanie i wiarygodność; (vii) wpływ kultury organizacyjnej na ryzyko; oraz (viii) relacje pomiędzy kluczowymi koncepcjami zarządzania ryzykiem.

2.1. ELEMENTY ZARZĄDZANIA RYZYKIEM

Zarządzanie ryzykiem jest złożonym, wieloaspektowym działaniem, które wymaga zaangażowania całej organizacji - od wyższego szczebla liderów/kadry kierowniczej zapewniających wizję strategiczną oraz cele i zadania organizacji na najwyższym poziomie, poprzez liderów średniego szczebla planujących, realizujących i zarządzających projektami, aż po osoby na pierwszej linii operacyjnej obsługujące systemy informatyczne wspierające misje/funkcje biznesowe organizacji. Zarządzanie ryzykiem jest kompleksowym procesem, który wymaga od organizacji: (i) ujęcia ryzyka w *ramy (tj.* ustanowienia kontekstu dla decyzji opartych na ryzyku); (ii) *oceny ryzyka; (*iii) *reagowania* na ryzyko po jego określeniu; oraz (iv) bieżącego *monitorowania ryzyka* z wykorzystaniem skutecznej komunikacji organizacyjnej i pętli sprzężenia zwrotnego w celu ciągłego doskonalenia działań organizacji związanych z ryzykiem. Zarządzanie ryzykiem jest prowadzone jako holistyczna, obejmująca całą organizację działalność, która zajmuje się ryzykiem od poziomu strategicznego do taktycznego, zapewniając, że podejmowanie decyzji w oparciu o ryzyko jest zintegrowane z każdym aspektem organizacji[10].

[10] Zintegrowane, obejmujące całe przedsiębiorstwo zarządzanie ryzykiem uwzględnienia przykładowo: (i) strategiczne cele/cele organizacji; (ii) misje organizacyjne/funkcje biznesowe uszeregowane według potrzeb; (iii) procesy misyjne/biznesowe; (iv) architektury korporacyjne i architektury bezpieczeństwa informacji; oraz (v) procesy cyklu życia systemu.

W kolejnych rozdziałach krótko opisano każdy z czterech komponentów zarządzania ryzykiem.

Pierwszy element zarządzania ryzykiem dotyczy sposobu, w jaki organizacje określają *ramy ryzyka* lub ustanawiają kontekst ryzyka - czyli opisują środowisko, w którym podejmowane są decyzje oparte na ryzyku. Celem tego komponentu jest stworzenie *strategii zarządzania ryzykiem*, która odnosi się do tego, jak organizacje zamierzają oceniać ryzyko, reagować na ryzyko i monitorować ryzyko, czyniąc jasnym i przejrzystym postrzeganie ryzyka, które organizacje rutynowo wykorzystują przy podejmowaniu decyzji inwestycyjnych i operacyjnych. Ramy ryzyka ustanawiają podstawę zarządzania ryzykiem i wyznaczają granice w zakresie podejmowania decyzji opartych na ryzyku w organizacji. Ustanowienie realistycznych i wiarygodnych ram ryzyka wymaga od organizacji zidentyfikowania: (i) założeń dotyczących ryzyka (np. założeń dotyczących zagrożeń, podatności, konsekwencji/skutków i prawdopodobieństwa wystąpienia, które wpływają na sposób szacowania ryzyka, reagowania na nie i monitorowania go w czasie); (ii) ograniczeń ryzyka (np. ograniczeń dotyczących rozważanych alternatyw szacowania ryzyka, reagowania na nie i monitorowania go); (iii) tolerancji ryzyka (np. poziomy ryzyka, rodzaje ryzyka oraz stopień niepewności ryzyka, które są akceptowalne); oraz (iv) priorytety i ustępstwa (np. względne znaczenie misji/funkcji biznesowych; kompromisy pomiędzy różnymi rodzajami ryzyka, przed którymi stoją organizacje; ramy czasowe, w których organizacje muszą uwzględniać ryzyko; oraz wszelkie czynniki niepewności, które organizacje biorą pod uwagę w reakcjach na ryzyko). Czynnik dotyczący kształtowania ryzyka oraz związana z nim strategia zarządzania ryzykiem obejmuje również wszelkie decyzje na poziomie strategicznym w zakresie sposobu zarządzania przez wyższego szczebla liderów/kierowników ryzykiem w odniesieniu do operacji i aktywów organizacyjnych, osób, innych organizacji oraz Państwa.

Drugi komponent zarządzania ryzykiem dotyczy sposobu, w jaki organizacje szacują *ryzyko* w kontekście ram ryzyka organizacyjnego. Celem elementu oceny ryzyka jest identyfikacja: (i) zagrożeń dla organizacji (tj. operacji, aktywów lub osób) lub zagrożeń skierowanych przez organizacje przeciwko innym organizacjom lub Państwu; (ii) podatności wewnętrznych

i zewnętrznych dla organizacji[11]; (iii) szkód (tj. konsekwencji/skutków) w organizacji, które mogą wystąpić, biorąc pod uwagę możliwość wykorzystania podatności przez różnego rodzaju zagrożenia; oraz (iv) prawdopodobieństwa wystąpienia szkód. Wynikiem końcowym jest określenie ryzyka (tj. stopnia szkodliwości i prawdopodobieństwa wystąpienia szkody). W celu wsparcia elementu oceny ryzyka, organizacje identyfikują: (i) narzędzia, techniki i metodologie, które są wykorzystywane do szacowania ryzyka; (ii) założenia przyjęte podczas szacowania ryzyka; (iii) ograniczenia, które mogą wpływać na szacowanie ryzyka; (iv) role i obowiązki; (v) sposób gromadzenia, przetwarzania i przekazywania informacji dotyczących szacowania ryzyka w organizacji; (vi) sposób przeprowadzania szacowania ryzyka w organizacji; (vii) częstotliwość przeprowadzania szacowania ryzyka; oraz (viii) sposób pozyskiwania informacji o zagrożeniach (tj. źródła i metody).

Trzeci element zarządzania ryzykiem dotyczy sposobu, w jaki organizacja *reaguje na ryzyko* po jego określeniu na podstawie wyników szacowania ryzyka. Celem komponentu reakcji na ryzyko jest zapewnienie spójnej, obejmującej całą organizację, reakcji na ryzyko zgodnie z ramami ryzyka organizacyjnego poprzez: (i) opracowanie alternatywnych kierunków działań w odpowiedzi na ryzyko; (ii) ocenę alternatywnych kierunków działań; (iii) określenie odpowiednich kierunków działań zgodnych z tolerancją ryzyka organizacyjnego; oraz (iv) wdrożenie reakcji na ryzyko w oparciu o wybrane kierunki działań.

W celu wsparcia komponentu reakcji na ryzyko, organizacje opisują rodzaje reakcji na ryzyko, które mogą być wdrożone (tj. akceptowanie, unikanie, łagodzenie, współdzielenie lub przekazywanie ryzyka). Organizacje identyfikują również narzędzia, techniki i metodologie wykorzystywane do opracowywania kierunków działań w odpowiedzi na ryzyko, sposób oceny kierunków działań oraz sposób komunikowania reakcji na ryzyko w ramach organizacji

[11] Podatności organizacyjne nie ograniczają się tylko do systemów informatycznych, ale mogą obejmować na przykład podatności w strukturach zarządzania, procesach misji/biznesu, architekturze korporacyjnej, architekturze bezpieczeństwa informacji, obiektach, sprzęcie, procesach cyklu życia systemu, działaniach w ramach łańcucha dostaw i u zewnętrznych dostawców usług.

oraz, w razie potrzeby, podmiotom zewnętrznym (np. zewnętrznym usługodawcom, partnerom w łańcuchu dostaw)[12].

Czwarty komponent zarządzania ryzykiem dotyczy sposobu, w jaki organizacje *monitorują ryzyko w* czasie. Celem elementu monitorowania ryzyka jest: (i) sprawdzenie, czy planowane środki reagowania na ryzyko są wdrażane oraz czy spełnione są wymagania dotyczące bezpieczeństwa informacji wynikające z/związane z misjami/funkcjami biznesowymi organizacji, przepisami prawnymi, dyrektywami, regulacjami, standardami i normami oraz wytycznymi; (ii) określenie bieżącej skuteczności środków reagowania na ryzyko po ich wdrożeniu; oraz (iii) zidentyfikowanie zmian wpływających na ryzyko w organizacyjnych systemach informatycznych i środowiskach, w których systemy te działają[13]. W celu wsparcia komponentu monitorowania ryzyka, organizacje opisują, w jaki sposób weryfikowana jest zgodność i jak określana jest bieżąca skuteczność reakcji na ryzyko (np. rodzaje narzędzi, techniki i metodologie wykorzystywane do określania wystarczalności/poprawności reakcji na ryzyko oraz czy środki ograniczania ryzyka są wdrażane prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądane efekty w zakresie redukcji ryzyka). Ponadto organizacje opisują, w jaki sposób monitorowane są zmiany, które mogą mieć wpływ na bieżącą skuteczność reakcji na ryzyko.

Jak wskazano w opisanych powyżej czterech komponentach zarządzania ryzykiem, organizacje biorą również pod uwagę zależności związane z ryzykiem zewnętrznym, stosownie do potrzeb. Organizacje identyfikują podmioty zewnętrzne, z którymi istnieje rzeczywisty lub potencjalny związek ryzyka (tj. organizacje, które mogą powodować ryzyko, przenosić ryzyko lub informować o ryzyku inne organizacje, jak również te, wobec których organizacje mogą powodować ryzyko, przekazywać ryzyko lub informować o ryzyku). Zewnętrzne relacje ryzyka obejmują na przykład dostawców, klientów lub obsługiwane

[12] Wytyczne dotyczące zarządzania ryzykiem w łańcuchu dostaw zawarte są w NIST Interagency Report 7622.

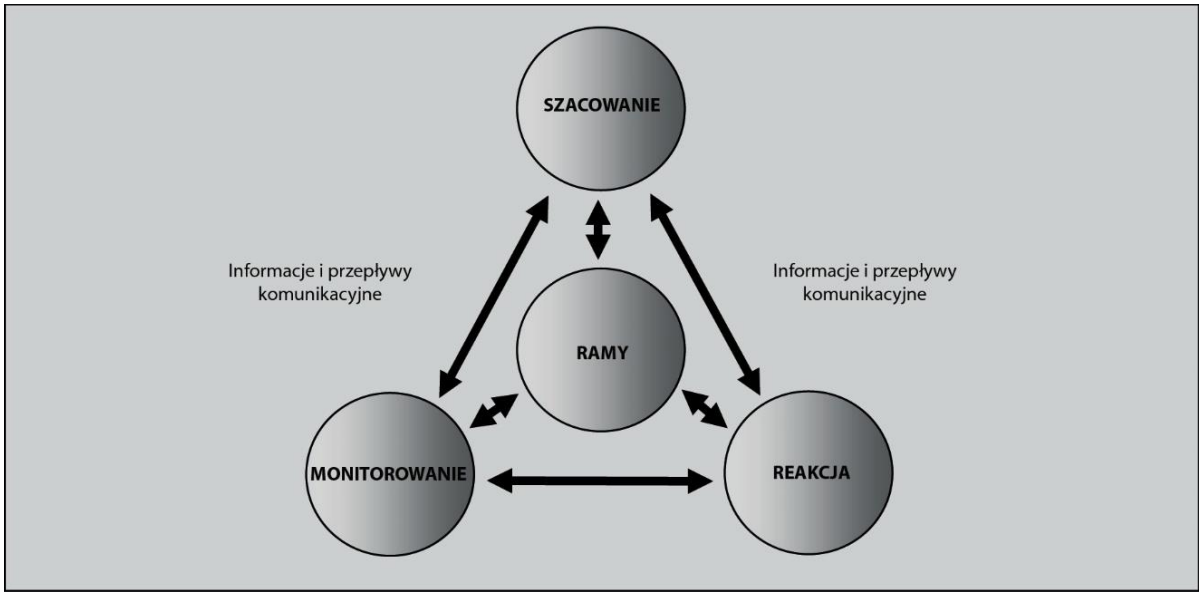
[13] Środowiska operacyjne obejmują, ale nie ograniczają się do: przestrzeni zagrożeń; podatności; misji/funkcji biznesowych; procesów misji/biznesu; architektur bezpieczeństwa korporacyjnego i informacyjnego; technologii informacyjnych; personelu; obiektów; relacji w łańcuchu dostaw; zarządzania/kultury organizacyjnej; procesów zamówień publicznych/nabywania; polityk/procedur organizacyjnych; założeń organizacyjnych, ograniczeń, tolerancji ryzyka i priorytetów/wyborów).

populacje, partnerów biznesowych, i/lub dostawców usług. W organizacjach mających do czynienia z zaawansowanymi trwałymi zagrożeniami (tj. długotrwałym wzorcem ukierunkowanych, wyrafinowanych ataków) ryzyko stwarzane przez partnerów zewnętrznych (zwłaszcza dostawców w łańcuchu dostaw) może stać się bardziej wyraźne. Organizacje ustalają praktyki dzielenia się informacjami związanymi z ryzykiem (np. informacjami o zagrożeniach i podatnościach) z podmiotami zewnętrznymi, w tym z tymi, z którymi organizacje mają relacje niosące ryzyko, jak również z tymi, które mogą dostarczać lub otrzymywać informacje związane z ryzykiem (np. centra wymiany i analizy informacji [*ang. Information Sharing and Analysis Centers - ISAC*], zespoły reagowania na incydenty komputerowe [*ang. Computer Security Incident Response Team*[14] *- CSIRT*]).

Rysunek 1 ilustruje proces zarządzania ryzykiem oraz przepływy informacji i komunikację pomiędzy komponentami. Strzałki reprezentują *główne* przepływy w ramach procesu zarządzania ryzykiem, w którym *określanie ram ryzyka* informuje o wszystkich sekwencyjnych działaniach krok po kroku, począwszy od *szacowania ryzyka,* poprzez *reakcję na ryzyko,* aż do *monitorowania ryzyka*. Na przykład, jednym z podstawowych wyników komponentu określania ryzyka jest opis źródeł i metod, które organizacje wykorzystują do pozyskiwania informacji o zagrożeniach (np. źródła otwarte, niejawne raporty wywiadowcze). Dane wyjściowe dotyczące informacji o zagrożeniach stanowią podstawowe dane wejściowe komponentu oceny ryzyka i są odpowiednio przekazywane do tego komponentu. Inny przykład ilustruje pierwotne dane wyjściowe z komponentu szacowania ryzyka - tj. określenie ryzyka. Dane wyjściowe z elementu szacowania ryzyka są przekazywane do komponentu reakcji na ryzyko i są odbierane przez ten komponent, jako podstawowe dane wejściowe. Kolejnym podstawowym wejściem do komponentu reagowania na ryzyko jest wyjście z komponentu szacowania ryzyka - strategia zarządzania ryzykiem, która definiuje, jak organizacja powinna reagować na ryzyko. Łącznie, te dane wejściowe, wraz z wszelkimi dodatkowymi danymi wejściowymi, są wykorzystywane przez

[14] Nazywany również Zespołem Reagowania na Incydenty Komputerowe (*ang. Computer Incident Response Team - CIRT lub Computer Incident Response Center, Computer Incident Response Capability - CIRC*).

decydentów przy dokonywaniu właściwego wyboru potencjalnych kierunków działania w odpowiedzi na ryzyko.

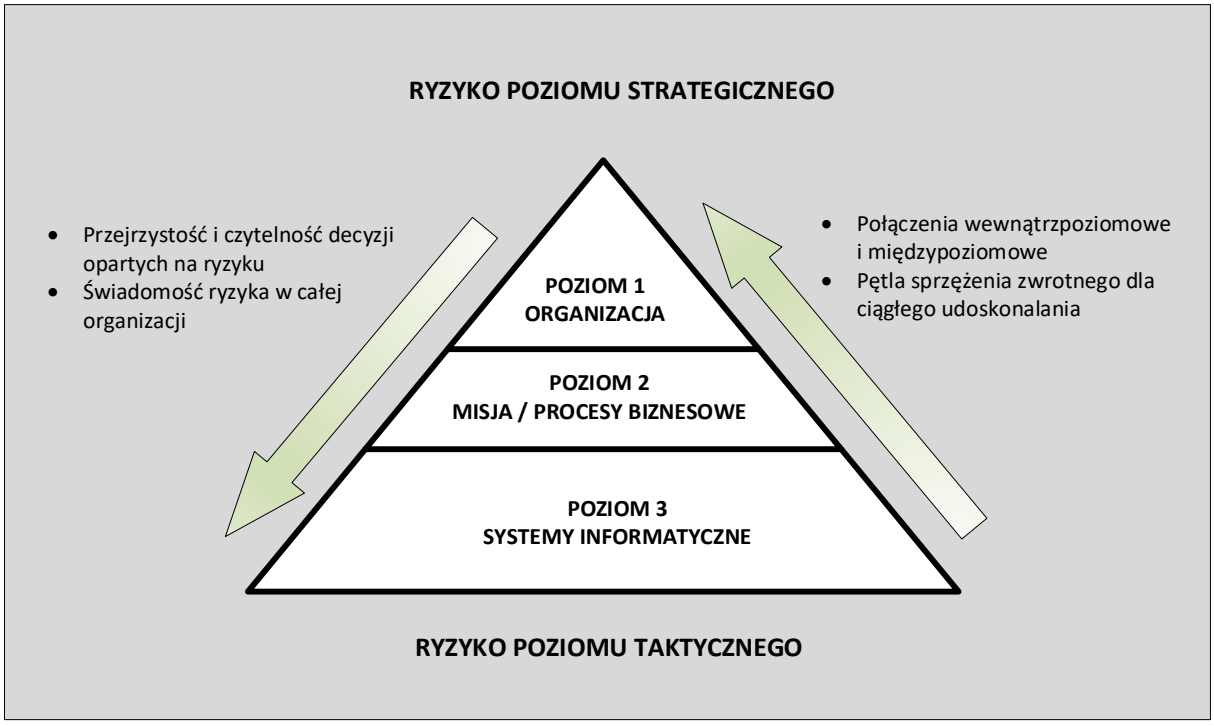


Rysunek 1. Proces zarządzania ryzykiem oraz przepływy informacji i komunikacji pomiędzy komponentami.

Dwukierunkowe strzałki wskazują, że przepływy informacji i komunikacja pomiędzy komponentami zarządzania ryzykiem, jak również kolejność wykonywania komponentów, mogą być elastyczne i dostosowywać się do dynamicznego charakteru procesu zarządzania ryzykiem. Na przykład, nowe przepisy, dyrektywy lub polityki mogą wymagać od organizacji natychmiastowego wdrożenia dodatkowych środków reagowania na ryzyko. Informacja ta jest przekazywana bezpośrednio z komponentu określającego ramy ryzyka do komponentu reagowania na ryzyko, gdzie przeprowadzane są konkretne działania zmierzające do osiągnięcia zgodności z nowymi przepisami, dyrektywami lub politykami. Pokazuje to bardzo dynamiczną i elastyczną naturę informacji podczas jej przepływu przez proces zarządzania ryzykiem. Rozdział trzeci zawiera kompletny opis procesu zarządzania ryzykiem w organizacji, w tym specyfikacje dla danych wejściowych/warunków wstępnych, działań i danych wyjściowych/warunków końcowych.

2.2. WIELOPOZIOMOWE ZARZĄDZANIE RYZYKIEM

W celu integracji procesu zarządzania ryzykiem w organizacji, stosuje się podejście trójwarstwowe, które obejmuje ryzyko na poziomie: (i) *organizacji*; (ii) *misji/procesu biznesowego*; oraz (iii) *systemu informatycznego*. Proces zarządzania ryzykiem jest realizowany w sposób płynny na wszystkich trzech poziomach, a jego nadrzędnym celem jest ciągłe doskonalenie działań podejmowanych przez organizację związanych z ryzykiem oraz efektywna komunikacja między poziomami i wewnątrz nich, prowadzona przez wszystkich interesariuszy mających wspólny interes w realizacji misji/osiągnięciu sukcesu biznesowego organizacji. Rysunek 2 ilustruje trójwarstwowe podejście do zarządzania ryzykiem z uwzględnieniem niektórych jego kluczowych cech.



Rysunek 2. Wielopoziomowe zarządzanie ryzykiem w organizacji.

Poziom 1 odnosi się do ryzyka widzianego z perspektywy *organizacyjnej*. Poziom 1 wdraża pierwszy komponent zarządzania ryzykiem (tj. określanie ram ryzyka), zapewniając kontekst dla wszystkich działań związanych z zarządzaniem ryzykiem prowadzonych przez organizacje.

Działania związane z zarządzaniem ryzykiem na Poziomie 1 mają bezpośredni wpływ na działania prowadzone na Poziomie 2 i 3. Na przykład, misje i funkcje biznesowe zdefiniowane

na Poziomie 1 wpływają na projektowanie i rozwój procesów misyjnych/biznesowych tworzonych na Poziomie 2 w celu realizacji tych misji/funkcji biznesowych. Poziom 1 zapewnia priorytetyzację misji/funkcji biznesowych, które z kolei wyznaczają strategie inwestycyjne i decyzje o finansowaniu, wpływając w ten sposób na rozwój architektury korporacyjnej (w tym wbudowanej architektury bezpieczeństwa informacji) na Poziomie 2 oraz na przydział i rozmieszczenie zarządczych, operacyjnych i technicznych środków bezpieczeństwa na Poziomie 3.

Inne przykłady działań na Poziomie 1, które mają wpływ na działania na Poziomach 2 i 3, obejmują wybór zabezpieczeń wspólnych, przekazywanie osobom autoryzującym (*ang. authorizing official* AO)[15] wskazówek od osób sprawujących funkcje wykonawcze ds. ryzyka (*ang. risk executive (function - RE*)[16] oraz ustalanie kolejności odzyskiwania systemów informatycznych wspierających misje krytyczne i operacje biznesowe. W sekcji 2.3 przedstawiono szerszy opis poszczególnych działań związanych z Poziomem 1.

Poziom 2 odnosi się do ryzyka z perspektywy *misji/procesu biznesowego* i jest określany na podstawie kontekstu ryzyka, decyzji dotyczących ryzyka oraz działań związanych z ryzykiem na Poziomie 1. Działania w zakresie zarządzania ryzykiem na Poziomie 2 obejmują: (i) definiowanie misji/procesów biznesowych niezbędnych do wspierania misji i funkcji biznesowych organizacji; (ii) ustalanie priorytetów misji/procesów biznesowych w odniesieniu do strategicznych celów i zadań organizacji; (iii) definiowanie rodzajów informacji niezbędnych do pomyślnego wykonania misji/procesów biznesowych, krytyczności/wrażliwości informacji oraz przepływów informacji zarówno wewnętrznych, jak i zewnętrznych w stosunku do organizacji; (iv) włączenie wymogów bezpieczeństwa informacji do misji/procesów biznesowych; oraz (v) ustanowienie architektury

[15] Opis ról i stanowisk - patrz: NSC 800-39 oraz dodatkowo: NSC 800-37; NSC 7298.
[16] Tamże.

korporacyjnej[17] z wbudowaną architekturą bezpieczeństwa informacji[18], która promuje opłacalne kosztowo i skuteczne rozwiązania informatyczne zgodne ze strategicznymi celami i zadaniami organizacji oraz miarami wydajności. Działania na Poziomie 2 mają bezpośredni wpływ na działania prowadzone na Poziomie 3. Na przykład element architektury korporacyjnej dotyczący bezpieczeństwa informacji opracowany na Poziomie 2 wpływa na alokację potrzeb w zakresie ochrony informacji i kieruje nią, co z kolei wpływa na przypisywanie i ukierunkowywanie środków bezpieczeństwa do określonych komponentów systemów informatycznych organizacji na Poziomie 3. Decyzje dotyczące architektury korporacyjnej na Poziomie 2 mają wpływ na projektowanie systemów informatycznych na Poziomie 3, w tym na rodzaje technologii informatycznych dopuszczalnych do stosowania przy tworzeniu tych systemów. Działania prowadzone na Poziomie 2 mogą również dostarczać użytecznych informacji zwrotnych Poziomowi 1, co może skutkować zmianami w ramach ryzyka organizacyjnego lub wpływać na działania w zakresie zarządzania ryzykiem prowadzone na Poziomie 1, np. wykonywane przez funkcję wykonawczą ds. ryzyka (RE). Sekcja 2.4 zawiera opis konkretnych działań przypisanych do Poziomu 2.

Poziom 3 dotyczy ryzyka z perspektywy *systemu informatycznego* i opiera się na kontekście ryzyka, decyzjach dotyczących ryzyka oraz działaniach związanych z ryzykiem na Poziomie 1 i 2. Działania związane z zarządzaniem ryzykiem na Poziomie 3 obejmują: (i) kategoryzację organizacyjnych systemów informatycznych; (ii) przydzielanie środków bezpieczeństwa do organizacyjnych systemów informatycznych i środowisk, w których te systemy działają zgodnie z ustaloną architekturą korporacyjną organizacji i wbudowaną architekturą bezpieczeństwa informacji; oraz (iii) zarządzanie wyborem, wdrażaniem, szacowaniem, autoryzacją i bieżącym monitorowaniem przydzielonych środków bezpieczeństwa w ramach

[17] Przykładowo, modele referencyjne architektury korporacyjnej oraz architektury segmentowej i rozwiązań są określone odpowiednio w programie OMB Federal Enterprise Architecture (FEA), *FEA Consolidated Reference Model Document,* Version 2.3, październik 2003 r., oraz OMB *Federal Segment Architecture Methodology (FSAM),* styczeń 2009 r.

[18] Architektura bezpieczeństwa informacji *(ang. information security architecture*) opisuje aspekty architektury korporacyjnej związane z bezpieczeństwem, które zostały włączone do definicji architektury korporacyjnej, jako integralna część opracowywania architektury - jest to subarchitektura wywodząca się z architektury korporacyjnej, a nie oddzielnie zdefiniowana warstwa lub architektura. Patrz: NSC 7298.

zdyscyplinowanego i ustrukturyzowanego procesu cyklu życia systemu wdrożonego w całej organizacji. Na poziomie 3 właściciele systemów informatycznych, dostawcy zabezpieczeń wspólnych, inżynierowie systemów i bezpieczeństwa oraz personel ds. bezpieczeństwa systemów informatycznych podejmują oparte na ryzyku decyzje dotyczące wdrażania, obsługi i monitorowania organizacyjnych systemów informatycznych. Na podstawie tych bieżących decyzji opartych na ryzyku operacyjnym urzędnicy zatwierdzający podejmują kolejne decyzje oparte na ryzyku, dotyczące tego, czy systemy informatyczne są wstępnie upoważnione do działania w wyznaczonych środowiskach operacyjnych lub czy mają być dalej na stałe upoważniane do działania. Te stałe decyzje oparte na ryzyku są podejmowane w ramach procesu zarządzania ryzykiem z uwzględnieniem wytycznych osób sprawujących funkcje wykonawcze ds. ryzyka (RE) oraz z uwzględnieniem różnych uwarunkowań architektonicznych wspierających procesy związane z misją/biznesem. Ponadto, działania na Poziomie 3 dostarczają istotnych informacji zwrotnych dla Poziomów 1 i 2. Na przykład, nowe podatności odkryte w organizacyjnym systemie informatycznym mogą mieć systemowe implikacje, które rozciągają się na całą organizację. Te same podatności mogą spowodować zmiany w architekturze korporacyjnej i wbudowanej architekturze bezpieczeństwa informacji lub mogą wymagać dostosowania tolerancji na ryzyko organizacyjne. Sekcja 2.5 zawiera opis poszczególnych działań związanych z Poziomem 3.

Należy zapewnić niezawodność systemów informatycznych, ponieważ misja i sukces biznesowy organizacji są od nich uzależnione. W celu zapewnienia niezawodności w obliczu wyrafinowanych zagrożeń, systemy informatyczne muszą być wykorzystywane rozważnie, zgodnie z osiągniętym stopniem bezpieczeństwa i odporności.

2.3. POZIOM 1 - WIDOK ORGANIZACJI

Poziom 1 odnosi się do ryzyka z perspektywy *organizacyjnej* poprzez ustanowienie i wdrożenie struktur zarządzania, które są zgodne ze strategicznymi celami i zadaniami organizacji oraz wymaganiami określonymi przez przepisy prawa, dyrektywy, polityki, regulacje, standardy i misje/funkcje biznesowe. Struktury zarządzania zapewniają nadzór nad działaniami w zakresie zarządzania ryzykiem prowadzonymi przez organizacje i obejmują:

(i) ustanowienie i wdrożenie funkcji wykonawczej ds. ryzyka (RE); (ii) ustanowienie strategii zarządzania ryzykiem organizacji, w tym określenie *tolerancji na ryzyko*; oraz (iii) opracowanie i realizację w skali organizacji *strategii inwestycyjnych* w zakresie zasobów informacyjnych i bezpieczeństwa informacji.

2.3.1. Zarządzanie

Ogólnie rzecz biorąc, *zarządzanie* to zbiór obowiązków i praktyk stosowanych przez osoby odpowiedzialne za organizację (np. zarząd i kierownictwo korporacji, kierownik jednostki organizacyjnej), których wyraźnym celem jest: (i) nadanie strategicznego kierunku; (ii) zapewnienie, że są osiągane misja i cele biznesowe organizacji; (iii) zapewnienie odpowiedniego zarządzania ryzykiem; oraz (iv) sprawdzenie, czy zasoby organizacji są wykorzystywane w sposób właściwy[19, 20]. Ryzyko i czynniki ryzyka mogą być związane z różnymi sektorami organizacyjnymi (np. prawnym, finansowym, technologii informacyjnej, zgodności z przepisami, bezpieczeństwa informacji). Poszczególne sektory wymagają specjalistycznej wiedzy, aby móc zarządzać ryzykiem związanym z danym sektorem. W związku z tym, sposób kierowania organizacją jest często zorganizowany według sektorów[21]. Pięć rezultatów kierowania związanych z zarządzaniem ryzykiem w całej organizacji to:

- strategiczne dostosowanie decyzji dotyczących zarządzania ryzykiem do misji i funkcji biznesowych zgodnych z celami i zadaniami organizacji;
- realizacja procesów zarządzania ryzykiem w celu określenia, szacowania, reagowania i monitorowania ryzyka odnoszącego się do działań i aktywów organizacji, osób, innych organizacji i Państwa;

[19] Niniejsza definicja została zaadaptowana przez *IT Governance Institute*. W 2004 r. definicję tę przyjęły również *Chartered Institute of Management Accountants* oraz *International Federation of Accountants*.

[20] *IT Governance Institute* (ITGI) jest oddziałem ISACA (*Information Systems Audit and Control Association*), niezależnego, globalnego stowarzyszenia non-profit zajmującego się rozwojem, przyjęciem i wykorzystaniem globalnie akceptowanej wiedzy i praktyk z zakresu systemów informacyjnych (IS).

[21] Chociaż zarządzanie jest często organizowane w podziale na sektory, organizacjom dobrze służy ustanowienie jednego, ujednoliconego podejścia do zarządzania. Ujednolicone podejście do zarządzania może skoordynować działania poszczególnych sektorów i zapewnić spójne podejście do zarządzania w całej organizacji.

- skuteczna i efektywna alokacja zasobów zarządzania ryzykiem;
- rezultaty oparte na wynikach osiąganych poprzez pomiar, monitorowanie i raportowanie metryk zarządzania ryzykiem w celu zapewnienia, że cele i zadania organizacyjne są osiągane; oraz
- zapewnienie wartości dodanej poprzez optymalizację inwestycji w zarządzanie ryzykiem w celu wsparcia celów organizacyjnych[22].

W ramach ładu organizacyjnego, wyżsi rangą liderzy/kadra kierownicza, w porozumieniu i współpracy z osobami sprawującymi funkcje wykonawcze ds. ryzyka (RE), określają: (i) rodzaje decyzji w zakresie zarządzania ryzykiem, które są zastrzeżone dla określonych ról wyższego szczebla kierownictwa (np. kierownicy jednostek organizacyjnych lub dyrektorzy generalni, dyrektorzy finansowi, CIO, CISO)[23]; (ii) rodzaje decyzji w zakresie zarządzania ryzykiem, które są uznawane za decyzje dotyczące całej organizacji oraz rodzaje decyzji, które mogą być delegowane do podległych organizacji lub do innych ról w organizacji (np. inżynierów systemów i bezpieczeństwa, właścicieli misji/biznesu, architektów korporacyjnych, architektów bezpieczeństwa informacji, dostawców infrastruktury lub usług wspólnych, osób autoryzujących); oraz (iii) sposób, w jaki decyzje dotyczące zarządzania ryzykiem będą przekazywane do i przez osoby sprawujące funkcje wykonawcze ds. ryzyka (RE).

W załączniku F opisano trzy różne rodzaje modeli zarządzania (tj. scentralizowany, zdecentralizowany i hybrydowy). Bez względu na zastosowany(e) model(e) zarządzania, jednoznaczne przypisanie i odpowiedzialność za akceptację ryzyka ma zasadnicze znaczenie dla skutecznego zarządzania ryzykiem.

[22] Wyniki zarządzania bezpieczeństwem informacji zaadaptowane z *IT Governance Institute, Information Security Governance: Guidance for Boards of Directors and Executive Management,* wydanie 2nd, 2006.

[23] Wymieniając różne tytuły w organizacji nie sugeruje się żadnych szczególnych relacji (partnerskich lub innych) ani linii władzy.

Sprawne kierowanie jest najlepszym wskaźnikiem zaangażowania kierownictwa wyższego szczebla w efektywne, spójne zarządzanie ryzykiem w całej organizacji w celu osiągnięcia ciągłego powodzenia misji/biznesu.

2.3.2. Funkcja wykonawcza ds. ryzyka (RE)

Funkcja wykonawcza ds. ryzyka (RE) jest rolą funkcjonalną ustanowioną w organizacji w celu zapewnienia szerszego, obejmującego całą organizację podejścia do zarządzania ryzykiem. Funkcja wykonawcza ds. ryzyka służy, jako wspólne źródło zarządzania ryzykiem przez wyższych rangą liderów/kadrę kierowniczą, właścicieli misji/biznesu, CIO, CISO, właścicieli systemów informatycznych, dostawców zabezpieczeń wspólnych[24], architektów korporacyjnych, architektów bezpieczeństwa informacji, inżynierów systemów informatycznych/bezpieczeństwa, ISSM/ISSO[25] oraz wszystkich innych interesariuszy mających interes w powodzeniu misji/biznesu organizacji. Funkcja wykonawcza ds. ryzyka (RE) koordynuje działania z wyższego szczebla liderami/kadrą zarządzającą, w celu:

- ustanowienia ról i obowiązków w zakresie zarządzania ryzykiem;
- opracowania i wdrożenia w całej organizacji *strategii zarządzania ryzykiem*, która wyznacza kierunek i kształtuje decyzje dotyczące ryzyka organizacyjnego (w tym sposób określania, szacowania, podejmowania działań zapobiegawczych i monitorowania ryzyka w czasie)[26];
- zarządzania informacjami o zagrożeniach i podatnościach w odniesieniu do systemów informatycznych organizacji oraz środowisk, w których te systemy funkcjonują;
- ustanowienia ogólnoorganizacyjnych forów w celu rozważenia wszystkich rodzajów i źródeł ryzyka (w tym ryzyka zagregowanego);

[24] Dostawca zabezpieczeń wspólnych (*ang. Common Control Provider - CCP*) – patrz: NSC 800-37; NSC 7298.

[25] Opis ról i stanowisk - patrz: NSC 800-37; NSC 7298.

[26] Podejmowane decyzje dotyczące ryzyka organizacyjnego obejmują decyzje inwestycyjne (patrz sekcja 2.3.4). Tolerancja ryzyka organizacyjnego jest określana w ramach komponentu określania ryzyka (patrz sekcja 2.3.3) i definiowana w strategii zarządzania ryzykiem.

- określenia ryzyka organizacyjnego na podstawie zagregowanego ryzyka wynikającego z działania i użytkowania systemów informatycznych oraz odpowiednich środowisk działania;
- zapewnienia nadzoru nad działaniami w zakresie zarządzania ryzykiem, prowadzonymi przez organizacje w celu zapewnienia spójnych i skutecznych decyzji opartych na ryzyku;
- rozwinięcia umiejętności pełniejszego zrozumienia ryzyka w odniesieniu do strategicznego spojrzenia na organizacje i ich zintegrowane działania;
- ustanowienia skutecznych narzędzi i pełnienie funkcji centralnego punktu komunikacji i dzielenia się informacjami związanymi z ryzykiem pomiędzy kluczowymi interesariuszami wewnątrz i na zewnątrz organizacji;
- określenia stopnia autonomii podległych organizacji, na jaki zezwalają organizacje macierzyste w odniesieniu do kształtowania, oceny, reagowania i monitorowania ryzyka[27];
- promowania współpracy i współdziałania między osobami autoryzującymi w celu uwzględnienia działań związanych z upoważnieniami do ochrony wymagających wspólnej odpowiedzialności (np. wspólne/dziedziczone autoryzacje)[28];
- zapewnienia, aby decyzje dotyczące autoryzacji w zakresie bezpieczeństwa uwzględniały wszystkie czynniki niezbędne dla powodzenia misji i działalności; oraz

[27] Ponieważ podległe organizacje odpowiedzialne za realizację misji pochodnych lub pokrewnych mogły już zainwestować we własne metody określania, szacowania, reagowania i monitorowania ryzyka, organizacje macierzyste mogą zezwolić na większy stopień autonomii w ramach części organizacji lub całej organizacji w celu zminimalizowania kosztów. Jeżeli dopuszcza się różnorodność działań w zakresie zarządzania ryzykiem, organizacje mogą zdecydować się na zastosowanie, jeżeli jest to wykonalne, pewnych środków interpretacji i/lub syntezy informacji związanych z ryzykiem, uzyskanych w wyniku tych działań, w celu zapewnienia, że wyniki różnych działań mogą być skorelowane w znaczący sposób.

[28] Publikacja NSC 800-37 zawiera wytyczne dotyczące wspólnych i dziedziczonych autoryzacji.

- zapewnienia, że współodpowiedzialność za wspieranie misji i funkcji biznesowych organizacji za pomocą zewnętrznych dostawców jest odpowiednio postrzegana i przekazywana odpowiednim organom decyzyjnym.

Funkcja wykonawcza ds. ryzyka (RE) nie zakłada ani określonej struktury organizacyjnej, ani formalnej odpowiedzialności przypisanej do jednej osoby lub grupy w organizacji. Kierownicy i jednostek organizacyjnych mogą zdecydować o zapewnieniu funkcji wykonawczej ds. ryzyka (RE) lub o jej delegowaniu. Funkcja wykonawcza ds. ryzyka (RE) wymaga kombinacji umiejętności, wiedzy specjalistycznej i perspektyw, aby zrozumieć strategiczne cele organizacji, misje organizacji/funkcje biznesowe, możliwości i ograniczenia techniczne oraz kluczowe zalecenia i wytyczne, które kształtują działania organizacji. Aby zapewnić tę niezbędną kombinację, funkcję wykonawczą ds. ryzyka (RE) może pełnić pojedyncza osoba lub zespół (wspierane przez personel ekspercki) lub wyznaczona grupa (np. rada ds. ryzyka, wykonawczy komitet sterujący, rada kierownicza)[29]. Funkcja wykonawcza ds. ryzyka (RE) wpisuje się w strukturę zarządzania organizacją w taki sposób, aby ułatwić sprawne działanie i zmaksymalizować efektywność. Mimo, że zakres działania całej organizacji sytuuje funkcję wykonawczą ds. ryzyka (RE) na Poziomie 1, jej rola obejmuje bieżącą komunikację z właścicielami misji/biznesu, osobami autoryzującymi, właścicielami systemów informatycznych, dostawcami zabezpieczeń wspólnych, CIO, CISO, inżynierami ds. systemów informatycznych i ds. bezpieczeństwa, ISSO oraz innymi zainteresowanymi stronami na Poziomie 2 i 3.

[29] Organizacje podkreślają potrzebę włączenia do zespołu wykonawczego ds. ryzyka (funkcji) liderów/kierowników wyższego szczebla z obszarów misji/biznesu, aby pomóc w zapewnieniu właściwego planowania bezpieczeństwa informacji, zasobów i zarządzania ryzykiem.

Skuteczność programów zarządzania ryzykiem w całej organizacji wymaga pełnego zaangażowania, bezpośredniego udziału i ciągłego wsparcia ze strony kierownictwa wyższego szczebla. Celem jest zinstytucjonalizowanie zarządzania ryzykiem w codziennych działaniach organizacji, jako priorytetu i integralnej części sposobu prowadzenia operacji w cyberprzestrzeni - zdając sobie sprawę, że jest to niezbędne do skutecznego prowadzenia misji w środowisku operacyjnym pełnym zagrożeń.

2.3.3. Strategia zarządzania ryzykiem

Strategia zarządzania ryzykiem organizacyjnym, będąca jednym z kluczowych rezultatów tworzenia ram ryzyka, odnosi się do tego, jak organizacje zamierzają szacować, reagować i monitorować ryzyko związane z działaniem i wykorzystaniem organizacyjnych systemów informatycznych. Strategia zarządzania ryzykiem określa specyficzne założenia, ograniczenia, tolerancję ryzyka oraz priorytety i kompromisy stosowane w organizacjach przy podejmowaniu decyzji inwestycyjnych i operacyjnych. Strategia zarządzania ryzykiem obejmuje również wszelkie decyzje i rozważania na poziomie strategicznym dotyczące sposobu, w jaki liderzy wyższego szczebla/kadra kierownicza mają zarządzać ryzykiem związanym z bezpieczeństwem informacji w odniesieniu do działań i aktywów organizacji, osób, innych organizacji i Państwa. Strategia zarządzania ryzykiem w całej organizacji obejmuje, na przykład, jednoznaczne określenie tolerancji ryzyka przyjętej przez organizację, akceptowalne metodologie oceny ryzyka, strategie reagowania na ryzyko, proces spójnego oceniania ryzyka w całej organizacji w odniesieniu do dopuszczalnej tolerancji ryzyka organizacji oraz podejścia do monitorowania ryzyka w czasie. Wprowadzenie funkcji wykonawczej ds. ryzyka (RE) może ułatwić spójne, ogólnoorganizacyjne stosowanie strategii zarządzania ryzykiem. Strategia zarządzania ryzykiem w całej organizacji może być wspierana przez dane odnoszące się do ryzyka pochodzące z innych źródeł zarówno wewnętrznych jak i zewnętrznych, w celu zapewnienia, że strategia ta jest zarówno szeroko rozwinięta jak i kompleksowa.

Ważnym działaniem w ramach zarządzania ryzykiem na Poziomie 1, a także częścią ram ryzyka, jest określenie *tolerancji ryzyka*. Tolerancja ryzyka to poziom ryzyka lub stopień

niepewności, który jest akceptowalny przez organizację i jest kluczowym elementem ram ryzyka organizacyjnego. Tolerancja ryzyka wpływa na wszystkie elementy procesu zarządzania ryzykiem - ma bezpośredni wpływ na decyzje w zakresie zarządzania ryzykiem podejmowane przez liderów/personel wykonawczy wyższego szczebla w całej organizacji oraz stanowi istotne ograniczenie dla tych decyzji. Na przykład, tolerancja ryzyka wpływa na charakter i zakres nadzoru nad zarządzaniem ryzykiem w organizacji, zakres i rygor przeprowadzanego szacowania ryzyka oraz treść strategii organizacyjnych dotyczących reagowania na ryzyko. W odniesieniu do szacowania ryzyka, organizacje akceptujące większe tolerancje ryzyka mogą zajmować się tylko tymi zagrożeniami, których doświadczyły inne organizacje, podczas gdy organizacje o mniejszej tolerancji ryzyka mogą rozszerzyć listę o te zagrożenia, które są teoretycznie możliwe, ale które nie zostały zaobserwowane w środowiskach operacyjnych. W odniesieniu do reagowania na ryzyko, organizacje wykazujące mniejszą tolerancję na ryzyko prawdopodobnie będą wymagać dodatkowych argumentów do przekonania o skuteczności wybranych zabezpieczeń i środków zaradczych lub będą preferować zabezpieczenia i środki zaradcze, które są bardziej zaawansowane i mają udokumentowaną historię. Takie organizacje mogą również zdecydować się na stosowanie wielu zabezpieczeń i środków zaradczych pochodzących z różnych źródeł (np. oprogramowanie antywirusowe na klientach i serwerach dostarczane przez różnych dostawców). Innym przykładem ilustrującym wpływ tolerancji ryzyka na reakcję na ryzyko jest fakt, że tolerancja ryzyka może również wpływać na wymagania organizacyjne dotyczące wiarygodności zapewnianej przez określone technologie informatyczne. Każda organizacja może wybrać te same technologie informacyjne, ale ich względny stopień tolerancji ryzyka może wpłynąć na stopień oceny wymagany przed wdrożeniem.

Nie ma określonego dokładnego poziomu tolerancji ryzyka organizacyjnego. Stopień tolerancji ryzyka raczej:

(i) generalnie wskazuje na kulturę organizacyjną; (ii) jest potencjalnie odmienny dla różnych rodzajów strat/kompromitacji; oraz (iii) w dużym stopniu zależy od indywidualnej, subiektywnej tolerancji ryzyka liderów wyższego szczebla/kadry kierowniczej. Niemniej jednak, konsekwencje podejmowania decyzji dotyczących ryzyka w oparciu o tolerancję

ryzyka są potencjalnie daleko idące - organizacje mniej tolerancyjne na ryzyko mogą nie osiągnąć potrzebnych zdolności do realizacji misji/biznesu tylko po to, aby uniknąć tego, co wydaje się być nieakceptowalnym ryzykiem; natomiast organizacje cechujące się większą tolerancją ryzyka mogą skupić się na krótkoterminowej efektywności misji/biznesu kosztem przygotowania się na przyszłe niepowodzenia. Ważne jest, aby organizacje zachowały należytą staranność przy określaniu tolerancji ryzyka - zdając sobie sprawę, jak fundamentalne znaczenie ma ta decyzja dla skuteczności programu zarządzania ryzykiem.

2.3.4. Strategie inwestycyjne

Strategie inwestycyjne[30] odgrywają znaczącą rolę w wysiłkach podejmowanych w zakresie zarządzania ryzykiem organizacyjnym. Strategie te zazwyczaj odzwierciedlają długoterminowe cele strategiczne organizacji oraz związane z nimi strategie zarządzania ryzykiem, opracowane i realizowane w celu zapewnienia powodzenia misji i działalności. U podstaw wszystkich strategii inwestycyjnych leży przekonanie, że istnieje skończona ilość zasobów, które można zainwestować w pomoc organizacjom w efektywnym zarządzaniu ryzykiem, czyli w skutecznym radzeniu sobie z ryzykiem w celu osiągnięcia sukcesu w realizacji misji/biznesu.

Priorytety w zakresie misji i ryzyka

Organizacje zazwyczaj realizują różne misje i są zaangażowane w różne rodzaje funkcji biznesowych. Jest to szczególnie zauważalne w przypadku dużych i złożonych organizacji, które posiadają różne komponenty organizacyjne, z których każdy koncentruje się na jednej lub dwóch podstawowych misjach. Chociaż wszystkie te elementy organizacyjne i związane z nimi misje/funkcje biznesowe są prawdopodobnie istotne i odgrywają kluczową rolę w ogólnym sukcesie organizacji, w rzeczywistości nie są one jednakowo ważne. Im bardziej krytyczne są misje i funkcje biznesowe organizacji, tym większa jest konieczność zapewnienia przez nią odpowiedniego zarządzania ryzykiem. Takie misje i funkcje biznesowe będą

[30] Strategie inwestycyjne mogą obejmować podejścia organizacyjne do: (i) zastępowania starszych systemów informatycznych (np. stopniowe wprowadzanie elementów, całkowita wymiana); (ii) outsourcingu i korzystania z usług zewnętrznych dostawców systemów i usług informatycznych; oraz (iii) wewnętrznego rozwoju vs. nabywanie komercyjnie dostępnych produktów technologii informacyjnej.

prawdopodobnie wymagały większych inwestycji w zarządzanie ryzykiem niż misje/funkcje biznesowe uważane za mniej krytyczne. Określenie względnego znaczenia misji/funkcji biznesowych, a tym samym poziomu inwestycji w zarządzanie ryzykiem, jest czymś, o czym decyduje się na Poziomie 1, co jest realizowane na Poziomie 2 i co wpływa na działania w zakresie zarządzania ryzykiem na Poziomie 3.

Przewidywane potrzeby w zakresie reagowania na ryzyko

Istnieje ogromna różnorodność charakteru potencjalnych zagrożeń, na które narażone są organizacje, począwszy od hakerów próbujących jedynie zniszczyć strony internetowe organizacji (np. cyberwandalizm), poprzez zagrożenia wewnętrzne, aż po wyrafinowane grupy terrorystyczne/zorganizowane grupy przestępcze dążące do eksfiltracji poufnych informacji, a skończywszy na siłach zbrojnych państwa, które próbują zniszczyć lub zakłócić kluczowe misje poprzez atakowanie systemów informatycznych organizacji[31]. Inwestycje strategiczne wymagane do przeciwdziałania zagrożeniom ze strony bardziej tradycyjnych przeciwników (np. hakerów prowadzących działania w małych grupach o ograniczonych możliwościach) znacznie różnią się od inwestycji wymaganych do przeciwdziałania zagrożeniom związanym z zaawansowanymi trwałymi zagrożeniami, które są spójne z bardziej zaawansowanymi przeciwnikami (np. państwami lub grupami terrorystycznymi posiadającymi wysoce zaawansowany poziom wiedzy specjalistycznej i zasoby, które dążą do ustanowienia stałych przyczółków w organizacjach mające na celu utrudnienia realizacji ich misji). W celu przeciwdziałania mniej wyrafinowanym zagrożeniom, organizacje mogą skoncentrować swoje wysiłki na Poziomie 3 - inwestując w zapewnienie, że potrzebne zabezpieczenia i środki zaradcze (np. środki bezpieczeństwa, usługi i technologie bezpieczeństwa) zostały pozyskane, wdrożone prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądane efekty w zakresie spełniania polityk bezpieczeństwa informacji i eliminowania znanych podatności. Oprócz tych podstawowych inwestycji, organizacje mogą również inwestować w procesy ciągłego monitorowania w celu

[31] Opisane powyżej zagrożenia stanowią podzbiór ogólnej przestrzeni zagrożeń, która obejmuje również błędy zaniechania i popełnienia, katastrofy naturalne i wypadki.

zapewnienia, że nabyte środki bezpieczeństwa, usługi i technologie skutecznie funkcjonują przez cały cykl życia systemu.

W przypadku, gdy organizacje muszą zająć się zaawansowanymi trwałymi zagrożeniami, prawdopodobnie nie jest możliwe odpowiednie zaadresowanie powiązanego ryzyka na Poziomie 3, ponieważ niezbędne rozwiązania w zakresie bezpieczeństwa nie są obecnie dostępne na rynku komercyjnym. W takich przypadkach organizacje muszą celowo inwestować środki wykraczające poza Poziom 3, aby uzyskać znaczące możliwości reagowania na Poziomie 2 i do pewnego stopnia na Poziomie 1. Na Poziomie 3 charakter inwestycji prawdopodobnie zmieni się z wdrażania istniejących rozwiązań na dodatkowy strategiczny nacisk na inwestowanie w najnowocześniejsze technologie bezpieczeństwa informacji (eksperymentowanie z innowacyjnymi rozwiązaniami/technologiami bezpieczeństwa i wczesne ich przyjmowanie) lub inwestowanie w badania i rozwój w zakresie bezpieczeństwa informacji w celu wyeliminowania poszczególnych luk technologicznych[32]. Inwestycje w dziedzinie bezpieczeństwa informacji mające na celu przeciwdziałanie zaawansowanym trwałym zagrożeniom mogą wymagać nakładów w ciągu kilku lat, ponieważ nowe rozwiązania i technologie w dziedzinie bezpieczeństwa przechodzą z etapu badań, rozwoju do pełnego wdrożenia. Długoterminowa perspektywa strategicznego inwestowania w potrzeby organizacji w zakresie reagowania na ryzyko może pomóc w zmniejszeniu ciągłej koncentracji na krótkoterminowych podatnościach wykrytych w systemach informatycznych - podatnościach, które istnieją ze względu na złożoność produktów i systemów informatycznych oraz nieodłączne słabości tych produktów i systemów.

Ograniczenia w zakresie inwestycji strategicznych

Zdolność organizacji do zapewnienia strategicznych inwestycji w bezpieczeństwo informacji jest ograniczona. W przypadku, gdy pożądane fundusze na inwestycje strategiczne lub

[32] Ta strategia inwestycyjna stanowi zmianę z zarządzania podatnościami i poprawkami na strategię długoterminową, która ma na celu usunięcie luk w bezpieczeństwie informacji, takich jak brak produktów technologii informacyjnej o wiarygodności niezbędnej do osiągnięcia odporności systemu informatycznego w obliczu zaawansowanych trwałych zagrożeń.

zasoby strategiczne nie są dostępne w celu zaspokojenia określonych potrzeb[33], organizacje mogą być zmuszone do stosowania kompromisów. Na przykład, organizacje mogą wydłużyć ramy czasowe wymagane do osiągnięcia strategicznych celów w zakresie bezpieczeństwa informacji. Alternatywnie, organizacje mogą nadawać priorytety inwestycjom w zakresie zarządzania ryzykiem, decydując się na zapewnienie środków (finansowych lub innych) na zaspokojenie niektórych krytycznych potrzeb strategicznych wcześniej niż innych, mniej krytycznych potrzeb. Wszystkie decyzje inwestycyjne wymagają od organizacji określenia priorytetów ryzyka i oceny potencjalnych skutków związanych z alternatywnymi kierunkami działań.

2.4. POZIOM 2 - WIDOK MISJI/PROCESÓW BIZNESOWYCH

Poziom 2 adresuje ryzyko z perspektywy *misji/procesów biznesowych* poprzez projektowanie, rozwijanie i wdrażanie misji/procesów biznesowych, które wspierają misje/funkcje biznesowe zdefiniowane na Poziomie 1. Procesy misji/biznesu organizacji ukierunkowują i informują o rozwoju architektury korporacyjnej, która zapewnia zdyscyplinowaną i uporządkowaną metodologię zarządzania złożonością infrastruktury informatycznej organizacji. Kluczowym elementem architektury korporacyjnej jest wbudowana architektura bezpieczeństwa informacji, która stanowi mapę drogową zapewniającą, że wymogi bezpieczeństwa informacji wynikające z misji/procesów biznesowych oraz potrzeby w zakresie bezpieczeństwa są zdefiniowane i przypisane do odpowiednich organizacyjnych systemów informatycznych i środowisk, w których te systemy działają.

2.4.1. Misja/procesy biznesowe uwzględniające ryzyko

Działania w zakresie zarządzania ryzykiem na Poziomie 2 rozpoczynają się od identyfikacji i ustanowienia *procesów realizacji misji/biznesu* uwzględniających ryzyko, *w* celu wspierania misji i funkcji biznesowych organizacji. Świadomy ryzyka proces misji/biznesu to taki, który

[33] W niektórych przypadkach mogą to być nie tylko kwestie finansowe, ale również ograniczenia dotyczące liczby osób posiadających odpowiednie umiejętności/wiedzę fachową lub ograniczenia związane ze stanem technologii.

wyraźnie uwzględnia prawdopodobne ryzyko, jakie taki proces spowodowałby, gdyby został wdrożony. Procesy uwzględniające ryzyko są zaprojektowane tak, by zarządzać ryzykiem zgodnie ze strategią zarządzania ryzykiem określoną na Poziomie 1 i wyraźnie uwzględniać ryzyko przy ocenie misji/biznesu i podejmowaniu decyzji na Poziomie 2[34]. Wdrażanie procesów misji/biznesu uwzględniających ryzyko wymaga dogłębnego zrozumienia misji organizacji i funkcji biznesowych oraz relacji między misjami/funkcjami biznesowymi i procesami wspierającymi. To zrozumienie jest warunkiem wstępnym do budowania procesów misji/biznesu wystarczająco odpornych, aby wytrzymać szeroki wachlarz zagrożeń, w tym rutynowe i wyrafinowane cyberataki, błędy/zdarzenia i klęski żywiołowe. Ważnym elementem osiągnięcia procesów uwzględniających ryzyko jest zrozumienie przez liderów/kadrę kierowniczą: (i) rodzajów źródeł zagrożeń i zdarzeń zagrażających, które mogą niekorzystnie wpłynąć na zdolność organizacji do skutecznego wykonywania misji/funkcji biznesowych); (ii) potencjalnego niekorzystnego wpływu/konsekwencji dla operacji i aktywów organizacyjnych, osób, innych organizacji lub Państwa, jeśli poufność, integralność lub dostępność informacji lub systemów informatycznych wykorzystywanych w misji/procesie biznesowym zostanie zagrożona; oraz (iii) prawdopodobnej odporności na takie zagrożenie, którą można osiągnąć przy danej definicji misji/procesu biznesowego, stosując realistyczne oczekiwania dotyczące odporności technologii informacyjnej.

Kluczowym wynikiem zdefiniowania procesów misji/biznesu na Poziomie 2 jest wybrana dla tych procesów strategia reagowania na ryzyko[35] w ramach ograniczeń określonych w strategii zarządzania ryzykiem. Strategia reagowania na ryzyko obejmuje identyfikację potrzeb w zakresie ochrony informacji oraz alokację tych potrzeb pomiędzy komponentami procesu (np. alokację na zabezpieczenia w ramach systemów informatycznych, zabezpieczenia w środowiskach operacyjnych tych systemów oraz alokację na alternatywne ścieżki realizacji misji/biznesu w oparciu o potencjał narażenia na kompromitację).

[34] Identyfikacja misji organizacji/procesów biznesowych obejmuje określenie typów informacji, których organizacja potrzebuje do skutecznej realizacji tych procesów, krytyczności i/lub wrażliwości informacji oraz przepływów informacji zarówno wewnętrznych, jak i zewnętrznych w stosunku do organizacji.

[35] Strategie reagowania na ryzyko opisano w Załączniku H.

2.4.2. Architektura korporacyjna

Istotnym zagadnieniem związanym z ryzykiem dotyczącym zdolności organizacji do skutecznego wypełniania misji i funkcji biznesowych jest złożoność technologii informacyjnej wykorzystywanej w systemach informatycznych. Aby sprostać tej złożoności i związanemu z nią potencjalnemu ryzyku, organizacje potrzebują zdyscyplinowanego i ustrukturyzowanego podejścia do zarządzania aktywami technologii informacyjnej wspierającymi ich misję/procesy biznesowe. Zapewnienie większej przejrzystości i zrozumienia infrastruktury informatycznej organizacji, w tym projektowania i rozwoju powiązanych systemów informatycznych, jest warunkiem wstępnym dla maksymalizacji odporności i rozsądnego wykorzystania tych systemów w obliczu coraz bardziej wyrafinowanych zagrożeń. Tego typu jasność i zrozumienie można skutecznie osiągnąć poprzez opracowanie i wdrożenie architektury korporacyjnej.

Architektura korporacyjna jest praktyką zarządzania stosowaną przez organizacje w celu maksymalizacji efektywności procesów i zasobów informacyjnych, które pomagają w osiągnięciu sukcesu w realizacji misji/biznesu. Architektura korporacyjna ustanawia jasny i jednoznaczny związek między inwestycjami (w tym inwestycjami w bezpieczeństwo informacji), a wymierną poprawą wydajności, niezależnie od tego, czy dotyczy to całej organizacji, czy jej części. Architektura korporacyjna daje również możliwość standaryzacji, konsolidacji i optymalizacji zasobów technologii informacyjnej. Działania te ostatecznie prowadzą do powstania systemów informatycznych, które są bardziej przejrzyste, a przez to łatwiejsze do zrozumienia i ochrony. Poza stworzeniem mapy drogowej dla bardziej efektywnego i oszczędnego wykorzystania technologii informacyjnej w organizacji, architektura korporacyjna zapewnia wspólny język do dyskusji nad kwestiami zarządzania ryzykiem związanymi z misjami, procesami biznesowymi i celami operacyjnymi - umożliwiając lepszą koordynację i integrację wysiłków i inwestycji ponad granicami organizacji i działalności biznesowej. Dobrze zaprojektowana architektura korporacyjna, wdrożona w całej organizacji, promuje bardziej wydajne, efektywne kosztowo, spójne i interoperacyjne możliwości w zakresie bezpieczeństwa informacji, które pomagają

organizacjom lepiej chronić misje i funkcje biznesowe, a w efekcie skuteczniej zarządzać ryzykiem.

Federalna Architektura Korporacyjna (*ang. Federal Enterprise Architecture - FEA*) definiuje zbiór wzajemnie powiązanych *modeli referencyjnych*, w tym Performance, Business, Service Component, Data i Technical, a także bardziej szczegółowe architektury *segmentowe* i *rozwiązań*, które wywodzą się z architektury *korporacyjnej*[36]. Aktywa organizacyjne (w tym programy, procesy, informacje, aplikacje, technologie, inwestycje, personel i obiekty) są mapowane do modeli referencyjnych na poziomie przedsiębiorstwa w celu stworzenia widoku organizacji zorientowanego na segmenty. Segmenty są elementami organizacji opisującymi obszary misji, wspólne/współdzielone usługi biznesowe oraz usługi ogólnoorganizacyjne. Z perspektywy inwestycyjnej architektura segmentowa jest podstawą decyzji dotyczących przypadku biznesowego lub grupy takich przypadków wspierających określone obszary misji lub wspólne/udostępniane usługi. Głównymi interesariuszami architektury segmentowej są właściciele misji/biznesu.

Architektura rozwiązań, ściśle powiązana z architekturą segmentową, definiuje zasoby informatyczne organizacji wykorzystywane do automatyzacji i usprawnienia procesów misji/biznesu. Zakres architektury rozwiązań jest zazwyczaj wykorzystywany do opracowania i wdrożenia wszystkich lub części systemów informatycznych lub rozwiązań biznesowych, w tym rozwiązań z zakresu bezpieczeństwa informacji. Głównymi interesariuszami architektury rozwiązań są deweloperzy i integratorzy systemów informatycznych, właściciele systemów informatycznych, inżynierowie systemów informatycznych/bezpieczeństwa oraz użytkownicy końcowi.

[36] Federalna Architektura Korporacyjna jest opisana w serii dokumentów opublikowanych przez OMB FEA Program Management Office. Dodatkowe informacje na temat modeli referencyjnych FEA oraz architektur segmentowych i rozwiązań można znaleźć odpowiednio w dokumencie FEA Consolidated Reference Model Document oraz FEA Practice Guidance.

Koncepcje FEA, które definiują procesy biznesowe oparte na potrzebach i wynikach, są stosowane przez organizacje, które uznają, że skuteczne zarządzanie ryzykiem, wynikającym z działania w środowisku cyberprzestrzeni charakteryzującym się wysokiej klasy wyrafinowanymi zagrożeniami, jest kluczową potrzebą i wskaźnikiem efektywności.

Architektura korporacyjna promuje również koncepcje *segmentacji*, *redundancji* i eliminacji *pojedynczych punktów awarii* - *wszystkie te* koncepcje mogą pomóc organizacjom w bardziej efektywnym zarządzaniu ryzykiem. Segmentacja jest ważna, ponieważ umożliwia organizacjom oddzielenie misji/funkcji biznesowych i operacji oraz systemów informatycznych, komponentów systemu lub podsystemów wspierających te misje, funkcje i operacje od innych funkcji i operacji oraz systemów wspierających. Segmentacja pomaga zdefiniować lepiej zarządzalne komponenty i potencjalnie zmniejszyć stopień szkód wynikających z udanego wykorzystania podatności przez zagrożenie. Architektura segmentowa wspiera koncepcję segmentacji na najwyższych szczeblach organizacji, a podejście to jest kontynuowane przez architekturę rozwiązań (w tym dekompozycję systemów informatycznych i sieci na podsystemy i podsieci, stosownie do potrzeb).

Koncepcja redundancji jest również bardzo istotna w architekturze korporacyjnej. Przy wysokim prawdopodobieństwie naruszenia lub kompromitacji, gdy zagrożenia wykorzystują podatności w organizacyjnych systemach informatycznych, awaria lub degradacja jednego lub więcej komponentów systemu informatycznego jest nieunikniona. Aby zwiększyć odporność systemu informatycznego w ramach reakcji na ryzyko, organizacyjne systemy informatyczne wprowadzają tryb awaryjny, który pomaga zapewnić, że uszkodzone komponenty uruchamiają odpowiednie komponenty zapasowe o podobnych możliwościach. Ten rodzaj zdolności jest niezbędny do przeciwdziałania zaawansowanym trwałym zagrożeniom w sytuacjach, w których organizacje w warunkach cyberataku mogą być zmuszone do działania w trybie awaryjnym, ale nadal zapewniając wystarczający poziom zdolności do osiągnięcia sukcesu w realizacji misji/biznesu. Architektury segmentowe i rozwiązań wspierają koncepcję redundancji poprzez ustanowienie zdyscyplinowanego i zorganizowanego podejścia do opracowywania i wdrażania kluczowych rozwiązań

architektonicznych, które w stosownych przypadkach ułatwiają replikację krytycznych elementów systemu informatycznego.

Koncepcja pojedynczych punktów awarii i eliminacji takich punktów jest łatwo wspierana przez architekturę korporacyjną. Istotna widoczność i przejrzystość zapewniona w projekcie architektonicznym na poziomie organizacji ujawnia potencjalne pojedyncze punkty awarii już na wczesnym etapie procesu rozwoju. W ten sposób pojedyncze punkty awarii są skutecznie eliminowane przez architektury segmentowe i rozwiązań. Nieuwzględnienie potencjalnych pojedynczych punktów awarii na wczesnym etapie projektowania architektonicznego może mieć poważne lub katastrofalne skutki, gdy te punkty awarii zostaną przeniesione na systemy informatyczne, a faktyczna awaria spowoduje utratę możliwości realizacji misji/biznesu.

2.4.3. Architektura bezpieczeństwa informacji

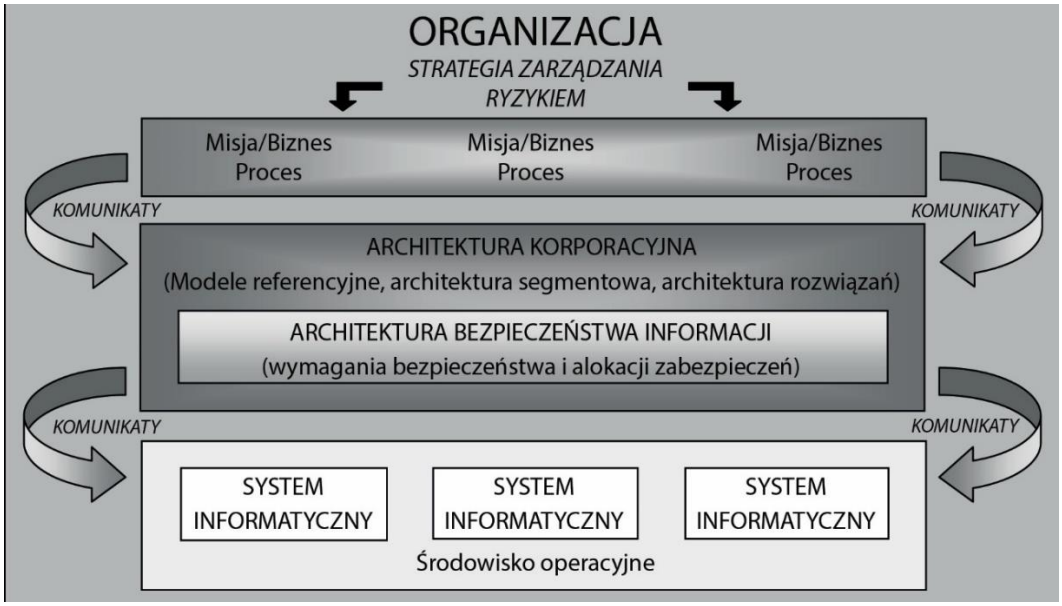
Architektura bezpieczeństwa informacji jest integralną częścią architektury korporacyjnej organizacji. Stanowi ona część architektury korporacyjnej dotyczącą odporności systemu informatycznego i dostarcza informacji architektonicznych do wdrożenia funkcji bezpieczeństwa[37]. Głównym celem architektury bezpieczeństwa informacji jest zapewnienie, że *wymogi bezpieczeństwa informacji* wynikające z misji/procesu biznesowego są konsekwentnie i efektywnie kosztowo osiągane w organizacyjnych systemach informatycznych i środowiskach, w których te systemy działają, zgodnie ze strategią zarządzania ryzykiem organizacyjnym[38]. Architektura bezpieczeństwa informacji uwzględnia również w architekturze segmentowej wymagania bezpieczeństwa zawarte w aktach prawnych, dyrektywach, politykach, przepisach, normach, standardach i wytycznych. Ostatecznie, architektura bezpieczeństwa informacji stanowi szczegółową mapę drogową, która umożliwia śledzenie drogi od strategicznych celów organizacji na najwyższym

[37] Generalnie, istnieje wersja architektury bezpieczeństwa informacji dla każdego z modeli referencyjnych architektury korporacyjnej; w tym Performance, Business, Service Component, Data i Technical.

[38] Organizacje stosują należyte zasady i techniki inżynierii systemów i bezpieczeństwa, aby zapewnić, że wymagania dotyczące bezpieczeństwa informacji są skutecznie wdrażane do organizacyjnych systemów informatycznych.

poziomie, poprzez konkretne potrzeby w zakresie ochrony misji/biznesu, do konkretnych rozwiązań w zakresie bezpieczeństwa informacji, zapewnianych przez ludzi, procesy i technologie.

Wymagania dotyczące bezpieczeństwa informacji zdefiniowane w architekturze segmentowej są implementowane w architekturze rozwiązania w postaci zarządczych, operacyjnych i technicznych *środków bezpieczeństwa*. Środki bezpieczeństwa są stosowane w ramach poszczególnych systemów informatycznych i środowisk, w których te systemy funkcjonują, lub są dziedziczone przez nie. Przydział[39] środków bezpieczeństwa jest zgodny z architekturą bezpieczeństwa informacji, a także z koncepcjami takimi jak „obrona w głąb" (*ang. defense-in-depth*) i „obrona wszerz" (*ang. defense-in-breadth*). Rysunek 3 ilustruje proces integracji wymagań dotyczących bezpieczeństwa informacji z architekturą korporacyjną i powiązanymi z nią systemami informatycznymi wspierającymi misję/procesy biznesowe organizacji.



Rysunek 3. Integracja wymagań w zakresie bezpieczeństwa informacji.

[39] Alokacja środków bezpieczeństwa odbywa się na poziomie komponentów systemu informatycznego, przy czym stosuje się zabezpieczenia w wybranych komponentach systemu, które mają zapewnić określoną zdolność w zakresie bezpieczeństwa. Szczegółowe wytyczne dotyczące sposobu włączania wymogów w zakresie bezpieczeństwa informacji do architektury korporacyjnej znajdują się w profilu bezpieczeństwa i prywatności FEA Security and Privacy Profile.

Podsumowując, kwestie związane z zarządzaniem ryzykiem mogą być uwzględnione, jako integralna część architektury korporacyjnej poprzez:

- opracowanie architektury segmentowej powiązanej ze strategicznymi celami i zadaniami organizacji, zdefiniowanymi misjami/funkcjami biznesowymi oraz związanymi z nimi procesami misyjnymi/biznesowymi;
- określenie obszarów, w których skuteczna reakcja na ryzyko jest krytycznym elementem sukcesu misji organizacji i jej funkcji biznesowych;
- określenie odpowiednich, na poziomie architektury, wymagań dotyczących bezpieczeństwa informacji w ramach zdefiniowanych przez organizację segmentów, w oparciu o strategię zarządzania ryzykiem organizacji;
- włączenie architektury bezpieczeństwa informacji wdrażającej wymagania dotyczące bezpieczeństwa informacji na poziomie architektonicznym;
- przekładanie wymagań dotyczących bezpieczeństwa informacji z architektury segmentowej na konkretne środki bezpieczeństwa systemów informatycznych/środowisk operacyjnych, jako część architektury rozwiązania;
- przydzielanie zarządczych, operacyjnych i technicznych środków bezpieczeństwa do systemów informatycznych i środowisk operacyjnych określonych w architekturze bezpieczeństwa informacji; oraz
- dokumentowanie decyzji w zakresie zarządzania ryzykiem na wszystkich poziomach architektury korporacyjnej[40].

Architektura korporacyjna zapewnia zdyscyplinowane i uporządkowane podejście do konsolidacji, standaryzacji i optymalizacji zasobów informatycznych wykorzystywanych w organizacjach. Zmniejszenie ryzyka można osiągnąć poprzez pełną integrację procesów

[40] Działania wymagane do skutecznego włączenia bezpieczeństwa informacji do architektury korporacyjnej są prowadzone przez kluczowych interesariuszy w organizacjach, w tym właścicieli misji/biznesu, dyrektorów ds. informacji, dyrektorów ds. bezpieczeństwa informacji, urzędników zatwierdzających oraz osoby odpowiedzialne za zarządzanie ryzykiem (funkcja).

zarządzania[41] w całej organizacji, zapewniając w ten sposób wyższy poziom bezpieczeństwa, prywatności, niezawodności i efektywności kosztowej dla misji i funkcji biznesowych realizowanych przez organizacje. To zintegrowane podejście, polegające na włączeniu strategii zarządzania ryzykiem do architektury korporacyjnej, daje liderom i kadrze zarządzającej możliwość podejmowania bardziej świadomych decyzji opartych na ryzyku w dynamicznych środowiskach operacyjnych - decyzji opartych na kompromisach pomiędzy wypełnianiem i doskonaleniem misji i funkcji biznesowych organizacji, a zarządzaniem wieloma rodzajami i źródłami ryzyka, które muszą być brane pod uwagę w ramach obowiązków związanych z zarządzaniem ryzykiem.

Wykorzystanie architektury korporacyjnej może znacznie poprawić podejście organizacji do ryzyka poprzez zapewnienie większej przejrzystości i jasności w działaniach projektowych i rozwojowych - umożliwiając bardziej konsekwentne stosowanie zasady "mądrego wykorzystania" technologii w całej organizacji; optymalizując kompromisy pomiędzy wartością uzyskaną z systemów informatycznych wspierających misje/funkcje biznesowe, a ryzykiem ponoszonym przez te systemy.

2.5. POZIOM 3 - WIDOK SYSTEMÓW INFORMATYCZNYCH

Wszystkie systemy informatyczne, w tym systemy operacyjne, systemy w fazie rozwoju oraz systemy poddawane modyfikacjom, znajdują się w pewnej fazie cyklu życia systemu[42]. Oprócz działań związanych z zarządzaniem ryzykiem prowadzonych na Poziomie 1 i Poziomie 2 (np. odzwierciedlanie strategii zarządzania ryzykiem organizacji w ramach architektury korporacyjnej i wbudowanej architektury bezpieczeństwa informacji), działania związane z zarządzaniem ryzykiem są również zintegrowane z cyklem życia systemów informatycznych

[41] Proces zarządzania to proces planowania i kontroli wykonania lub realizacji działań organizacyjnych (np. programów, projektów, zadań, procesów). Procesy zarządzania są często określane, jako systemy pomiaru wyników i zarządzania.

[42] W cyklach życia systemu wyróżnia się zazwyczaj pięć faz: (i) *inicjacja*; (ii) *rozwój/nabycie;* (iii) *implementacja;* (iv) *eksploatacja/utrzymanie*; oraz (v) *utylizacja*. Organizacje mogą stosować różne procesy cyklu życia systemu, w tym na przykład rozwój kaskadowy (*ang. waterfall*), spiralny (ang. spiral) lub zwinny (ang. agile).

organizacji na Poziomie 3. Działania związane z zarządzaniem ryzykiem na Poziomie 3 odzwierciedlają strategię zarządzania ryzykiem organizacji oraz wszelkie ryzyko związane z kosztami, harmonogramem i wymaganiami dotyczącymi wydajności poszczególnych systemów informatycznych wspierających misję/funkcje biznesowe organizacji. Działania związane z zarządzaniem ryzykiem odbywają się w każdej fazie cyklu życia systemu, a wyniki każdej fazy mają wpływ na kolejne fazy.

Na przykład, definiowanie wymagań[43] jest krytyczną częścią każdego procesu rozwoju systemu i rozpoczyna się bardzo wcześnie w cyklu życia, zazwyczaj w fazie *inicjacji.* Najnowsze informacje o zagrożeniach, które są dostępne dla organizacji, lub aktualne założenia organizacyjne dotyczące zagrożeń, mogą znacząco wpłynąć na wymagania stawiane systemom informatycznym oraz na rodzaje rozwiązań, które są uznawane przez organizacje za akceptowalne (z technologicznego i operacyjnego punktu widzenia) w obliczu takich zagrożeń. Wymagania bezpieczeństwa informacji stanowią podzbiór wymagań funkcjonalnych stawianych systemom informatycznym i są włączane do cyklu życia systemu równocześnie z innymi wymaganiami. Wymagania w zakresie bezpieczeństwa informacji określają niezbędne funkcje bezpieczeństwa[44] dla systemów informatycznych oraz poziom wiarygodności tych funkcji (zob. sekcja 2.6 dotycząca wiarygodności systemów informatycznych).

Organizacje zajmują się również kwestiami zarządzania ryzykiem podczas fazy *rozwoju/nabywania* w ramach cyklu życia systemu (np. projektowanie systemu, rozwój/integracja systemu i demonstracja). Czy to w odpowiedzi na konkretne i wiarygodne informacje o zagrożeniach, czy też założenia dotyczące zagrożeń, potencjalne podatności systemów informatycznych organizacji związane z projektem mogą być ograniczone podczas tej fazy poprzez wybór mniej podatnych alternatyw. Ryzyko związane z łańcuchem dostaw

[43] Wymagania dotyczące bezpieczeństwa informacji można uzyskać z różnych źródeł (np. z przepisów, polityk, dyrektyw, regulacji, standardów, norm oraz misji/biznesu/ wymagań operacyjnych organizacji).

[44] Funkcjonalność bezpieczeństwa to zestaw środków kontroli bezpieczeństwa stosowanych w ramach systemu informatycznego lub środowiska, w którym system ten funkcjonuje, lub dziedziczonych przez nie. Środki kontroli bezpieczeństwa, opisane w specjalnej publikacji NIST 800-53, są wdrażane przez kombinację ludzi, procesów i technologii.

podczas fazy nabycia systemu informatycznego jest również obszarem zainteresowania organizacji. W celu przeciwdziałania ryzyku związanemu z łańcuchem dostaw podczas fazy rozwoju/nabywania, organizacje wdrażają określone środki bezpieczeństwa, które uznają za konieczne. Przy wyborze najodpowiedniejszych środków bezpieczeństwa organizacje biorą również pod uwagę ryzyko z punktu widzenia środowiska, w którym systemy informatyczne mają funkcjonować. Aby zabezpieczenia były skuteczne, muszą się wzajemnie wspierać, być stosowane z realistycznymi oczekiwaniami, co do skuteczności oraz wdrożone, jako część wyraźnej architektury bezpieczeństwa na poziomie systemu informatycznego, która jest spójna z architekturą bezpieczeństwa wbudowaną w architekturę korporacyjną organizacji. Na przykład, gdy niektóre zabezpieczenia techniczne są mniej skuteczne ze względu na osiągalne poziomy wiarygodności systemów informatycznych organizacji, zabezpieczenia zarządzania i operacyjne są stosowane, jako zabezpieczenia kompensacyjne - zapewniając w ten sposób kolejną możliwość zarządzania ryzykiem.

Po inicjacji, rozwoju i nabyciu, faza *wdrożenia* cyklu życia systemu daje organizacji przed rozpoczęciem rzeczywistych operacji, możliwość określenia skuteczności wybranych środków bezpieczeństwa stosowanych w ramach, lub odziedziczonych przez opracowywane systemy informatyczne. Przewidywania wygenerowane podczas tej fazy mogą być porównane z rzeczywistymi zachowaniami w trakcie wdrażania systemów informatycznych. Biorąc pod uwagę aktualne dostępne dla organizacji informacje o zagrożeniach oraz założenia organizacyjne dotyczące zagrożeń, informacje zdobyte podczas oceny efektywności oraz potencjalny niekorzystny wpływ na misje/funkcje biznesowe organizacji, może zachodzić konieczność modyfikacji lub zmiany planowanego wdrożenia systemu informatycznego. W celu uzasadnienia proponowanych zmian mogą być opracowane informacje związane z ryzykiem.

Po zatwierdzeniu do eksploatacji systemy informatyczne przechodzą do fazy eksploatacji/utrzymania w ramach cyklu życia systemu. Monitorowanie skuteczności środków bezpieczeństwa oraz wszelkich zmian w organizacyjnych systemach informatycznych i środowiskach, w których te systemy funkcjonują, zapewnia, że wybrane środki reagowania na ryzyko działają na bieżąco zgodnie z założeniami. Bieżące

monitorowanie ma zasadnicze znaczenie dla utrzymania świadomości sytuacyjnej ryzyka dla misji organizacji i funkcji biznesowych - świadomości, która jest krytyczna dla dokonywania niezbędnych korekt postępowania, gdy ryzyko przekracza tolerancję ryzyka organizacji. Podczas fazy utylizacji w cyklu życia systemu standardową procedurą organizacji jest wiarygodne usunięcie przed utylizacją wszelkich informacji z systemów informatycznych, które mogą mieć negatywny wpływ, jeśli zostaną ujawnione, a także ocena ryzyka związanego z tymi działaniami[45].

Wczesne włączenie wymogów bezpieczeństwa informacji do cyklu życia systemu jest najbardziej efektywną kosztowo metodą wdrażania strategii zarządzania ryzykiem organizacyjnym na Poziomie 3[46]. Włączenie zarządzania ryzykiem do cyklu życia systemu zapewnia, że proces zarządzania ryzykiem nie jest odizolowany od innych procesów zarządzania stosowanych przez organizację w celu opracowania, nabycia, wdrożenia, obsługi i utrzymania systemów informatycznych wspierających misje organizacji i funkcje biznesowe. Aby wesprzeć integrację cyklu życia systemu, zarządzanie ryzykiem (w tym kwestie bezpieczeństwa informacji) jest również włączane do działań związanych z programem, planowaniem i finansowaniem w celu zapewnienia, że odpowiednie zasoby są dostępne w razie potrzeby - ułatwiając w ten sposób realizację etapów programu i projektu ustalonych przez organizacje. Aby uwzględnić zarządzanie ryzykiem w programach, planowaniu i budżetowaniu, specjaliści ds. ryzyka i bezpieczeństwa informacji stanowią integralną część zespołów i struktur wykorzystywanych do spełniania wymagań systemowych i organizacyjnych.

[45] Podczas, gdy prezentacja cyklu życia systemu jest wyrażona jako przepływ liniowy, w rzeczywistości wiedza zdobyta w późniejszej fazie cyklu życia lub zmiany w wymaganiach systemowych lub środowiskach operacyjnych mogą podyktować konieczność powrotu do wcześniejszej fazy. Na przykład, zmiany w środowisku zagrożeń podczas fazy eksploatacji/utrzymania mogą dyktować potrzebę zainicjowania nowej lub zmienionej zdolności systemu.

[46] Ramy zarządzania ryzykiem (RMF), opisane w NSC 800-37, zapewniają ustrukturyzowany proces, który integruje działania związane z zarządzaniem ryzykiem z cyklem życia systemu. RMF działa głównie na Poziomie warstwy 3, ale współdziała również z Poziomami 1 i 2 (np. dostarczając informacji zwrotnych z decyzji autoryzacyjnych do funkcji wykonawczej ds. ryzyka (RE), rozpowszechniając uaktualnione informacje o ryzyku wśród osób autoryzujących, dostawców zabezpieczeń wspólnych i właścicieli systemów informatycznych).

Ogólna *odporność* organizacyjnych systemów informatycznych (tj. to, jak poprawnie systemy działają w warunkach stresu) jest kluczowym czynnikiem i miarą wydajności w określaniu potencjalnej zdolności przetrwania misji/funkcji biznesowych. Wykorzystanie pewnych technologii informacyjnych może wprowadzić do tych systemów nieodłączne słabe punkty - co w rezultacie może spowodować ryzyko, które trzeba będzie zminimalizować poprzez przeprojektowanie obecnych procesów misji/biznesu. *Rozsądne wykorzystanie* technologii informacyjnych podczas projektowania, rozwoju i wdrażania organizacyjnych systemów informatycznych ma ogromne znaczenie w zarządzaniu ryzykiem.

Wprowadzenie wymagań i działań związanych z bezpieczeństwem informacji, jako integralnej części cyklu życia systemu zapewnia, że liderzy wyższego szczebla/kadra kierownicza biorą pod uwagę ryzyko dla działań i aktywów organizacji, osób, innych organizacji i Państwa, wynikające z działania i użytkowania systemów informatycznych oraz podejmują odpowiednie działania w celu zachowania należytej rzetelności organizacji.

2.6. ZAUFANIE I WIARYGODNOŚĆ

Zaufanie jest niezwykle istotnym zagadnieniem związanym z zarządzaniem ryzykiem. To, w jaki sposób organizacje postrzegają kwestię zaufania, wpływa na ich zachowanie oraz wewnętrzne i zewnętrzne relacje oparte na zaufaniu. Ten rozdział wprowadza pewne koncepcyjne sposoby myślenia o zaufaniu, definiuje pojęcie *wiarygodności* i pokazuje, jak koncepcja wiarygodności może być wykorzystana w rozwijaniu relacji opartych na zaufaniu. Załącznik G przedstawia przykłady kilku modeli zaufania, które mogą być zastosowane w kontekście organizacyjnym oraz rozważa sposoby pomiaru zaufania. Omówiono również

znaczenie ładu organizacyjnego, kultury i przejrzystości[47] w odniesieniu do zaufania i jego wpływu na zarządzanie ryzykiem.

Zaufanie to przekonanie, że podmiot zachowa się w przewidywalny sposób w określonych okolicznościach. Podmiotem tym może być osoba, proces, obiekt lub dowolna kombinacja takich składników. Podmiot może mieć dowolną wielkość - od pojedynczego komponentu sprzętowego lub modułu oprogramowania, przez element wyposażenia identyfikowany na podstawie marki i modelu, po miejsce lub lokalizację, organizację, aż po Państwo. Zaufanie, choć z natury jest określeniem subiektywnym, może być oparte na obiektywnych dowodach i elementach subiektywnych. Obiektywne podstawy zaufania mogą obejmować na przykład wyniki testów i oceny produktów technologii informacyjnej. Subiektywne przekonania, poziom pewności i doświadczenie mogą uzupełniać (lub nawet zastępować) obiektywne dowody lub zastępować takie dowody, gdy są one niedostępne. Zaufanie jest zwykle związane z konkretnymi okolicznościami lub sytuacją (np. kwotą pieniędzy zaangażowaną w transakcję, wrażliwością lub krytycznością informacji, lub tym, czy bezpieczeństwo jest kwestią, w której stawką jest ludzkie życie). Zaufanie zazwyczaj nie jest przechodnie (np. ufasz przyjacielowi, ale niekoniecznie przyjacielowi przyjaciela). Wreszcie, na zaufanie zazwyczaj się zapracowuje, na podstawie doświadczenia lub pomiarów. Jednak w niektórych organizacjach zaufanie może być nakazane przez politykę (patrz Załącznik G, *model zaufania obowiązkowego*).

Wiarygodność to cecha osoby lub organizacji, która daje innym pewność, co do kwalifikacji, możliwości i rzetelności tego podmiotu w zakresie wykonywania określonych zadań i wypełniania przypisanych obowiązków. Wiarygodność jest również cechą produktów i systemów informatycznych (patrz punkt 2.6.2 dotyczący *wiarygodności systemów informatycznych*). Atrybut wiarygodności, niezależnie od tego, czy odnosi się do ludzi, procesów czy technologii, może być mierzony, przynajmniej w kategoriach względnych, jeśli

[47] *Przejrzystość* jest osiągana poprzez zapewnienie *wglądu w* zarządzanie ryzykiem i działania związane z bezpieczeństwem informacji prowadzone przez organizacje uczestniczące w partnerstwie (np. stosowanie wspólnych standardów bezpieczeństwa, języka specyfikacji środków bezpieczeństwa, w tym zabezpieczeń wspólnych, procedur oceny, metodologii oceny ryzyka; definiowanie wspólnych artefaktów i dowodów wykorzystywanych przy podejmowaniu decyzji związanych z ryzykiem).

nie ilościowych[48]. Określenie wiarygodności odgrywa kluczową rolę w tworzeniu relacji zaufania pomiędzy osobami i organizacjami. Relacje oparte na zaufaniu są kluczowymi czynnikami w decyzjach dotyczących ryzyka podejmowanych przez liderów/kierowników wyższego szczebla.

2.6.1. Budowanie zaufania pomiędzy organizacjami

Strony nawiązują relacje oparte na zaufaniu na podstawie misji i potrzeb biznesowych[49]. Zaufanie między stronami zazwyczaj istnieje na zasadzie ciągłości, z różnymi stopniami zaufania osiąganymi na podstawie wielu czynników. Organizacje mogą nadal dzielić się informacjami i uzyskiwać usługi informatyczne, nawet jeśli ich relacje nie są w pełni zaufane. Stopień zaufania wymagany do nawiązania współpracy partnerskiej może się znacznie różnić w zależności od wielu czynników, w tym zaangażowanych organizacji i specyfiki sytuacji (np. misji, celów i zadań potencjalnych partnerów, krytyczności/wrażliwości działań związanych z partnerstwem, tolerancji ryzyka organizacji uczestniczących w partnerstwie oraz historycznych relacji między uczestnikami). Wreszcie, stopień zaufania między podmiotami nie jest cechą statyczną, ale może zmieniać się w czasie wraz ze zmianą okoliczności.

W celu realizacji misji i funkcji biznesowych, organizacje stają się coraz bardziej zależne od usług systemów informatycznych[50] i informacji dostarczanych przez organizacje zewnętrzne, a także od partnerstw. Ta zależność skutkuje potrzebą stworzenia *relacji zaufania* pomiędzy organizacjami[51]. W wielu przypadkach relacje oparte na zaufaniu z organizacjami

[48] Obecny stan praktyki w zakresie pomiaru wiarygodności potrafi w sposób wiarygodny rozróżnić bardzo różne poziomy wiarygodności i jest w stanie stworzyć skalę wiarygodności, która jest hierarchiczna pomiędzy podobnymi przypadkami działań pomiarowych (np. wyniki ocen ISO/IEC 15408 [Common Criteria]).

[49] Relacje zaufania mogą być: (i) ustanowione formalnie, na przykład poprzez udokumentowanie informacji związanych z zaufaniem w umowach, porozumieniach o poziomie świadczonych usług, zestawieniach prac, protokołach uzgodnień/porozumieniach lub umowach dotyczących bezpieczeństwa połączeń wzajemnych; (ii) skalowalne i mające charakter międzyorganizacyjny lub wewnątrzorganizacyjny; i/lub (iii) reprezentowane przez proste (dwustronne) relacje między dwoma partnerami lub bardziej złożone relacje między wieloma partnerami.

[50] Zewnętrzne usługi systemu informatycznego to usługi, które są realizowane poza klasycznymi granicami autoryzacji systemu (tzn. usługi, które są wykorzystywane przez system informatyczny organizacji, ale nie stanowią jego integralnej części).

[51] Zewnętrzni dostawcy lub partnerzy biznesowi mogą być podmiotami sektora publicznego lub prywatnego, krajowymi lub międzynarodowymi.

zewnętrznymi, choć generują większą produktywność i efektywność kosztową, mogą również nieść ze sobą większe ryzyko dla organizacji. Ryzyko to jest uwzględniane przez strategie zarządzania ryzykiem ustanowione przez organizacje, które biorą pod uwagę strategiczne cele i zadania organizacji.

Skuteczne przeciwdziałanie ryzyku związanemu z rosnącą zależnością od zewnętrznych dostawców usług oraz partnerstwa z krajowymi i międzynarodowymi uczestnikami sektora publicznego i prywatnego wymaga od organizacji:

- określenia rodzajów usług/informacji, które mają być świadczone na rzecz organizacji lub rodzajów informacji, które mają być dzielone/wymieniane w proponowanych umowach partnerskich;
- określenia stopnia kontroli lub wpływu, jaki organizacje mają na organizacje zewnętrzne uczestniczące w porozumieniach partnerskich;
- opisania sposobów, w jaki usługi/informacje mają być chronione zgodnie z wymogami bezpieczeństwa informacji obowiązującymi w organizacjach;
- uzyskania odpowiednich informacji od organizacji zewnętrznych w celu określenia wiarygodności oraz wsparcia i utrzymania zaufania (np. wgląd w praktyki biznesowe oraz decyzje dotyczące ryzyka/bezpieczeństwa informacji w celu zrozumienia tolerancji na ryzyko);
- odpowiedniego wyważenia wymogów związanych z misją/biznesem w celu wspierania wymiany informacji przy jednoczesnym uwzględnieniu ryzyka współpracy z konkurencyjnymi lub nieprzyjaznymi podmiotami oraz ryzyka, że inne organizacje, choć nie są ani konkurencyjne ani wrogie, mogą stać się drogą ataku takich podmiotów;
- określenia, czy bieżące ryzyko dla działań i aktywów organizacji, osób, innych organizacji lub Państwa, wynikające z dalszego korzystania z usług/informacji lub udziału w partnerstwie, jest na akceptowalnym poziomie; oraz
- uznania, że decyzje o nawiązaniu relacji opartych na zaufaniu są wyrazem akceptowalnego ryzyka.

Stopień zaufania, jakim dana organizacja obdarza organizacje zewnętrzne może być bardzo różny, począwszy od tych, które cieszą się dużym zaufaniem (np. partnerzy biznesowi we wspólnym przedsięwzięciu, którzy mają wspólny model biznesowy i wspólne cele) do tych, które cieszą się mniejszym zaufaniem i mogą stanowić większe źródło ryzyka (np. partnerzy biznesowi w jednym przedsięwzięciu, którzy są jednocześnie konkurentami lub adwersarzami). Specyfika ustanawiania i utrzymywania zaufania może być różna dla różnych organizacji w zależności od misji/wymagań biznesowych, uczestników zaangażowanych w relację zaufania, krytyczności/wrażliwości wymienianych informacji lub rodzaju świadczonych usług, historii pomiędzy organizacjami oraz ogólnego ryzyka dla organizacji nawiązujących relacje. Załącznik G zawiera przykłady kilku modeli zaufania, które organizacje mogą wykorzystać w kontaktach z organizacjami zewnętrznymi.

W wielu sytuacjach zaufanie ustanowione między organizacjami może nie pozwalać na pełne spektrum wymiany informacji lub pełne świadczenie usług. W przypadku, gdy organizacja stwierdzi, że wiarygodność innej organizacji nie pozwala na pełne dzielenie się informacjami lub korzystanie z usług zewnętrznych, organizacja może: (i) złagodzić ryzyko, przenieść ryzyko lub podzielić ryzyko poprzez zastosowanie jednego lub kilku zabezpieczeń kompensacyjnych; (ii) zaakceptować większy stopień ryzyka; lub (iii) uniknąć ryzyka poprzez wykonywanie misji/funkcji biznesowych z ograniczonym poziomem funkcjonowania lub ewentualnie bez jakiegokolwiek działania.

Wyraźne zrozumienie i akceptacja ryzyka ponoszonego w związku z działalnością organizacji, jej aktywami, jednostkami, innymi organizacjami oraz Państwem przez kierownictwo wyższego szczebla (odzwierciedlające tolerancję organizacji na ryzyko) jest realizowane zgodnie ze strategią zarządzania ryzykiem organizacji i stanowi warunek wstępny dla ustanowienia relacji zaufania pomiędzy organizacjami.

2.6.2. Wiarygodność systemów informatycznych

Pojęcie wiarygodności może być również stosowane w odniesieniu do systemów informatycznych oraz produktów i usług technologii informacyjnej, które wchodzą w skład

tych systemów. Wiarygodność wyraża stopień, w jakim można oczekiwać, że systemy informatyczne (w tym produkty technologii informacyjnej, z których zbudowane są te systemy) zachowają poufność, integralność i dostępność informacji przetwarzanych, przechowywanych lub przekazywanych przez te systemy w pełnym zakresie zagrożeń.

Systemy informatyczne godne zaufania to systemy, które zostały uznane za posiadające poziom wiarygodności niezbędny do działania w ramach określonych poziomów *ryzyka* pomimo zakłóceń środowiskowych, błędów ludzkich i celowych ataków, które zgodnie z oczekiwaniami mogą wystąpić w środowiskach ich działania. Dwa czynniki wpływające na wiarygodność systemów informatycznych to:

- *funkcjonalność bezpieczeństwa* (tj. cechy/funkcje bezpieczeństwa zastosowane w systemie); oraz
- *zapewnienie (pewność) bezpieczeństwa* (tj. podstawy zaufania, że funkcja bezpieczeństwa jest skuteczna w swoim zastosowaniu)[52].

Funkcjonalność bezpieczeństwa można uzyskać poprzez zastosowanie w organizacyjnych systemach informatycznych i ich środowiskach operacyjnych kombinacji zarządzania, operacyjnych i technicznych środków bezpieczeństwa zawartych w publikacji NSC 800-53[53]. Rozwój i wdrażanie niezbędnych środków bezpieczeństwa jest ukierunkowane i oparte na architekturze korporacyjnej ustanowionej przez organizacje.

Zapewnienie bezpieczeństwa jest krytycznym aspektem w określaniu wiarygodności systemów informatycznych. Wiarygodność jest miarą pewności, że funkcje bezpieczeństwa, praktyki, procedury i architektura systemu informatycznego dokładnie odzwierciedlają i egzekwują politykę bezpieczeństwa[54]. Zapewnienie uzyskuje się poprzez podejmowanie:

[52] Wiarygodność stanowi również podstawę zaufania, że zamierzona funkcjonalność systemu informatycznego jest poprawna, zawsze wywoływana (kiedy jest wymagana) i odporna na obejście lub manipulację.

[53] Zastosowanie odpowiednich środków bezpieczeństwa systemów informatycznych i środowisk operacyjnych jest zgodne z trzema pierwszymi krokami Ram Zarządzania Ryzykiem (tj. kategoryzacja, wybór i wdrożenie).

[54] *Polityka bezpieczeństwa* jest zbiorem kryteriów świadczenia usług bezpieczeństwa.

(i) działań przez deweloperów i wykonawców[55] w odniesieniu do projektowania, rozwoju, wdrażania i działania funkcji bezpieczeństwa (tj. środków bezpieczeństwa); oraz (ii) działań przez osoby oceniające w celu określenia zakresu, w jakim funkcjonalność jest prawidłowo wdrożona, działa zgodnie z przeznaczeniem i przynosi pożądane rezultaty w odniesieniu do spełnienia wymogów bezpieczeństwa systemów informatycznych i ich środowisk działania[56]. Deweloperzy i wykonawcy mogą zwiększyć pewność działania funkcji bezpieczeństwa poprzez stosowanie dobrze zdefiniowanych polityk i modeli bezpieczeństwa, ustrukturyzowanych i rygorystycznych technik opracowywania sprzętu i oprogramowania oraz solidnych zasad inżynierii systemowej/bezpieczeństwa.

Zapewnienie bezpieczeństwa produktów i systemów informatycznych jest zwykle oparte na przeprowadzonych ocenach (i związanych z nimi dowodach oceny) w fazach inicjacji, nabycia/rozwoju, wdrożenia oraz eksploatacji/utrzymania w cyklu życia systemu. Na przykład, dowody rozwojowe mogą obejmować techniki i metody wykorzystywane do projektowania i rozwijania funkcjonalności bezpieczeństwa. Dowody operacyjne mogą obejmować raportowanie o błędach i ich usuwanie, wyniki raportowania o zdarzeniach naruszających bezpieczeństwo oraz wyniki bieżącego monitorowania środków bezpieczeństwa. Niezależne oceny dokonywane przez wykwalifikowany personel oceniający mogą obejmować analizy dowodów, a także testowanie, inspekcje i audyty wdrożenia wybranej funkcji bezpieczeństwa[57].

Pojęcia pewności i wiarygodności są ze sobą ściśle powiązane. Zapewnienie przyczynia się do określenia wiarygodności w odniesieniu do produktu technologii informacyjnej lub systemu informatycznego. Deweloperzy/wykonawcy produktów lub systemów informatycznych mogą dostarczyć dowodów wiarygodności poprzez wygenerowanie odpowiednich artefaktów (np.

[55] W tym kontekście deweloper/wykonawca to osoba lub grupa osób odpowiedzialnych za projektowanie, opracowywanie, wdrażanie lub obsługę środków bezpieczeństwa systemu informatycznego lub infrastruktury pomocniczej.

[56] W przypadku systemów innych niż krajowe systemy bezpieczeństwa, organizacje winny spełniać minimalne wymagania w zakresie zapewnienia bezpieczeństwa określone w Załączniku E publikacji NSC 800-53.

[57] Publikacja NSC 800-53A zawiera wytyczne dotyczące oceniania środków bezpieczeństwa systemów informatycznych i organizacji.

wyników niezależnych testów i oceny, dokumentacji projektowej, specyfikacji wysokiego lub niskiego poziomu, analizy kodu źródłowego). Organizacje korzystające z produktów lub systemów informatycznych mogą same przeprowadzać lub opierać się na innych prowadzonych formach oceny tych produktów lub systemów. Organizacje mogą również mieć bezpośrednie doświadczenie z produktem bądź systemem lub mogą otrzymywać informacje o działaniu produktu lub systemu od stron trzecich. Organizacje zazwyczaj oceniają wszystkie dostępne dowody pewności, często stosując różne czynniki wagowe (wskaźniki), aby określić wiarygodność produktu lub systemu w odniesieniu do okoliczności.

Oczekuje się, że produkty i systemy informatyczne charakteryzujące się wyższym stopniem wiarygodności (tj. produkty/systemy posiadające odpowiednią funkcjonalność i pewność) będą wykazywały niższy wskaźnik ukrytych wad projektowych i wykonawczych oraz wyższy stopień odporności na penetrację przed szeregiem zagrożeń, w tym wyrafinowanymi cyberatakami, klęskami żywiołowymi, wypadkami oraz zamierzonymi/niezamierzonymi błędami. Wymagany stopień wiarygodności określa podatność misji/funkcji biznesowych organizacji na znane zagrożenia, środowiska operacyjne, w których wdrażane są systemy informatyczne, oraz maksymalny dopuszczalny poziom ryzyka dla działań i aktywów organizacji, osób, innych organizacji lub Państwa.

Wiarygodność jest kluczowym czynnikiem decydującym o wyborze i właściwym wykorzystaniu produktów informatycznych stosowanych w systemach informatycznych organizacji. Niewystarczająca dbałość o wiarygodność produktów i systemów informatycznych może negatywnie wpłynąć na zdolność organizacji do skutecznego wypełniania przypisanych jej misji/funkcji biznesowych.

2.7. KULTURA ORGANIZACYJNA

Kultura organizacyjna[58] odnosi się do wartości, przekonań i norm, które wpływają na zachowania i działania liderów/kadry zarządzającej wyższego szczebla oraz poszczególnych

[58] Zwana dalej: kultura.

członków organizacji. Kultura opisuje sposób postępowania w organizacjach i może wyjaśniać, dlaczego pewne rzeczy mają miejsce. Istnieje bezpośredni związek pomiędzy kulturą organizacyjną, a sposobem, w jaki organizacje reagują na niepewność oraz potencjalne przekształcenie krótkoterminowych korzyści w źródło długoterminowych strat. Kultura organizacyjna informuje, a nawet, być może w dużym stopniu, definiuje strategię zarządzania ryzykiem tej organizacji. Jeśli wyrażona strategia zarządzania ryzykiem nie jest spójna z kulturą organizacji, to jest prawdopodobne, że jej wdrożenie będzie trudne, jeśli nie niemożliwe. Rozpoznanie i uwzględnienie istotnego wpływu kultury na decyzje związane z ryzykiem podejmowane przez liderów/kierownictwo wyższego szczebla w organizacjach może być zatem kluczowe dla osiągnięcia efektywnego zarządzania ryzykiem.

Rozpoznanie wpływu kultury organizacyjnej na wdrożenie programu zarządzania ryzykiem w całej organizacji jest niezwykle ważne, ponieważ może to oznaczać istotną zmianę organizacyjną. Zmiana ta musi być skutecznie zarządzana, a zrozumienie kultury organizacji odgrywa ważną rolę w osiągnięciu takiej zmiany w całej organizacji. Wdrożenie efektywnego programu zarządzania ryzykiem może oznaczać znaczącą zmianę w całej organizacji, polegającą na dostosowaniu ludzi, procesów i kultury w organizacji do nowych lub zmienionych celów i zadań organizacji, strategii zarządzania ryzykiem oraz mechanizmów komunikacji służących wymianie pomiędzy jednostkami informacji związanych z ryzykiem. Aby skutecznie zarządzać takimi zmianami, organizacje włączają kwestie kulturowe, jako podstawowy element procesu tworzenia strategii i podejmowania decyzji na poziomie strategicznym (np. opracowywanie strategii zarządzania ryzykiem). Jeśli liderzy wyższego szczebla/kadra kierownicza rozumieją znaczenie aspektów kulturowych, mają większe szanse na osiągnięcie strategicznych celów w drodze skutecznego zarządzania ryzykiem.

Kultura ma również wpływ na stopień ponoszonego ryzyka. Kultura jest odzwierciedlona w gotowości organizacji do przyjęcia nowych i wiodących technologii informacyjnych. Na przykład organizacje, które prowadzą działalność badawczo-rozwojową, mogą być bardziej skłonne do przesuwania granic technologicznych. Takie organizacje są nastawione na wczesne wprowadzanie nowych technologii, a zatem częściej postrzegają nowe technologie z punktu widzenia potencjalnych korzyści, jakie można osiągnąć, niż potencjalnych szkód

wynikających z ich zastosowania. Z kolei organizacje, które zajmują się działalnością związaną z bezpieczeństwem, mogą być z natury bardziej konserwatywne i mniej skłonne do zmiany granic technologicznych - są bardziej ostrożne i nieufne wobec nowych technologii, zwłaszcza, jeśli są one dostarczane przez podmiot, z którym dana organizacja nie jest zaznajomiona i któremu nie ufa. Tego typu organizacje są również mniej skłonne do wczesnego wdrażania nowych technologii i bardziej skłonne do obserwowania potencjalnych szkód spowodowanych ich wprowadzeniem. Innym tego przykładem jest fakt, że niektóre organizacje w przeszłości tworzyły własne oprogramowanie i usługi lub zamawiały oprogramowanie i usługi wyłącznie na własny użytek. Organizacje te mogą być niechętne do korzystania z oprogramowania i usług dostarczanych z zewnątrz i ta niechęć może skutkować mniejszym ryzykiem. Inne organizacje mogą z kolei dążyć do maksymalizacji korzyści osiąganych przez nowoczesne architektury sieciocentryczne (np. architektury zorientowane na usługi, przetwarzanie chmurowe), w których sprzęt, oprogramowanie i usługi są zazwyczaj dostarczane przez organizacje zewnętrzne. Ponieważ organizacje zazwyczaj nie mają bezpośredniej kontroli nad działaniami związanymi z oceną, audytem i nadzorem zewnętrznych dostawców, ryzyko z tym związane może być większe.

Oprócz wpływu kultury na perspektywy zarządzania ryzykiem w organizacji, mogą również występować problemy kulturowe pomiędzy organizacjami. W przypadku, gdy dwie lub więcej organizacji działa razem na rzecz wspólnego celu, istnieje możliwość, że różnice kulturowe w każdej z nich mogą skutkować różnymi strategiami zarządzania ryzykiem, skłonnością do ponoszenia ryzyka oraz gotowością do jego akceptacji[59]. Na przykład, załóżmy, że dwie organizacje współpracują nad stworzeniem wspólnej usługi bezpieczeństwa, której celem jest przeciwdziałanie zaawansowanym trwałym zagrożeniom. Kultura jednej z organizacji może skutkować skupieniem się na zapobieganiu nieautoryzowanemu ujawnieniu informacji, podczas gdy natura drugiej organizacji może skutkować naciskiem na ciągłość misji. Różnice w skupieniu i nacisku wynikające z kultury organizacyjnej mogą generować różne priorytety i oczekiwania dotyczące tego, jakie usługi

[59] Podobna sytuacja może zaistnieć pomiędzy podległymi elementami organizacji, gdy elementy te otrzymują sporą dozę autonomii i władzy operacyjnej.

bezpieczeństwa należy zamawiać, ponieważ organizacje inaczej postrzegają naturę zagrożenia. Takie rozbieżności związane z kulturą nie występują wyłącznie pomiędzy organizacjami, ale mogą również występować wewnątrz organizacji, gdzie różne komponenty organizacyjne (np. komponenty informatyczne, komponenty operacyjne) mają różne wartości i być może inną tolerancję ryzyko. Przykład wewnętrznego rozdźwięku można zaobserwować w szpitalu, który kładzie nacisk na różnice kulturowe pomiędzy ochroną prywatności pacjentów, a dostępnością informacji medycznych dla pracowników medycznych w celu leczenia.

Kultura zarówno kształtuje, jak i jest kształtowana przez ludzi w organizacji. Wpływy i oddziaływanie kultury mogą być odczuwalne na wszystkich trzech Poziomach w wielopoziomowym podejściu do zarządzania ryzykiem. Liderzy/kierownictwo wyższego szczebla, zarówno bezpośrednio, jak i pośrednio, w strukturach zarządzania Poziomu 1 określają sposób, w jaki organizacje reagują na różne podejścia do zarządzania ryzykiem. Liderzy/kadra zarządzająca wyższego szczebla ustalają tolerancję ryzyka organizacji zarówno w sposób formalny (np. poprzez publikację strategii i dokumentów zawierających wytyczne), jak i nieformalny (np. poprzez działania dyscyplinujące, poziom spójności w działaniach oraz stopień egzekwowanej odpowiedzialności). Kierunek wyznaczony przez liderów/kierownictwo wyższego szczebla oraz zrozumienie istniejących wartości i priorytetów organizacyjnych są głównymi czynnikami determinującymi sposób zarządzania ryzykiem w organizacji.

2.8. ZWIĄZEK MIĘDZY KLUCZOWYMI KONCEPCJAMI RYZYKA

Jak wynika z powyższych rozważań, istnieje wiele różnych koncepcji związanych z ryzykiem (np. tolerancja ryzyka, zaufanie i kultura), z których wszystkie mają wpływ na zarządzanie ryzykiem. Koncepcje te nie funkcjonują w oderwaniu, zazwyczaj występuje silna interakcja między nimi (np. kultura organizacji wraz z jej strukturami i procesami zarządzania często wpływa na tempo zmian i realizację strategii zarządzania ryzykiem). Z tego powodu funkcja wykonawcza ds. ryzyka (RE) oraz inne strony zaangażowane w podejmowanie decyzji opartych na ryzyku organizacyjnym muszą mieć świadomość i doceniać wszystkie te koncepcje. Poniżej przedstawiono kilka przykładów relacji pomiędzy koncepcjami

związanymi z ryzykiem. Lista relacji nie jest wyczerpująca i służy jedynie zilustrowaniu, w jaki sposób łączenie koncepcji związanych z ryzykiem może wywołać niezamierzone konsekwencje, zarówno pozytywne, jak i negatywne.

2.8.1. Zarządzanie, tolerancja ryzyka i zaufanie

W ramach wdrażania strategii zarządzania ryzykiem organizacji na Poziomie 1, funkcja wykonawcza ds. ryzyka (RE) ustala praktyki dotyczące udostępniania podmiotom zewnętrznym informacji związanych z ryzykiem. Jeśli chodzi o wykazywanie należytej staranności w zarządzaniu ryzykiem, organizacje mające niższą tolerancję ryzyka będą prawdopodobnie wymagać większej liczby dowodów uzasadniających niż organizacje mające wyższą tolerancję ryzyka. Takie organizacje mogą ufać (a więc i współpracować) tylko z tymi organizacjami, z którymi mają długotrwałe i udane relacje (patrz Załącznik G: Model historycznego zaufania bezpośredniego). Stopień centralizacji organizacji może odzwierciedlać jej tolerancję na ryzyko i/lub skłonność do zaufania organizacjom partnerskim. Niektóre organizacje wybierają zdecentralizowaną strukturę zarządzania z takich powodów, jak bardzo rozbieżne obszary misji/biznesu lub potrzeba zwiększonej separacji pomiędzy misjami/biznesami ze względu na wrażliwość pracy. Powody decentralizacji mogą odzwierciedlać i prawdopodobnie będą wpływać na tolerancję ryzyka. Na przykład, jeśli nie ma organizacji partnerskich spełniających ustalone kryteria zaufania, organizacje z niższą tolerancją ryzyka mogą wymagać znacznie więcej dowodów potwierdzających należytą staranność (np. dostęp do szacowania ryzyka, planów bezpieczeństwa, raportów z oceny bezpieczeństwa, decyzji o akceptacji ryzyka) niż jest to zwykle wymagane w takich sytuacjach (patrz Załącznik G: Model potwierdzonego zaufania).

2.8.2. Zaufanie i kultura

Istnieje również potencjalna interakcja pomiędzy pojęciami ryzyka, zaufania i kultury. Zmiany w zakresie misji lub wymagań biznesowych (np. nowa misja lub wymóg biznesowy dotyczący połączenia systemów informatycznych w celu wymiany informacji) mogą wymagać większej akceptacji ryzyka niż jest to typowe dla danej organizacji. W krótkim okresie mogą być potrzebne dodatkowe środki w celu ustanowienia i/lub zbudowania zaufania (np. zwiększenie przejrzystości między wzajemnie połączonymi organizacjami). Takie działania

ułatwiają budowanie zaufania oraz ewolucję przekonań i norm organizacyjnych w dłuższej perspektywie czasowej. Interakcje pomiędzy zaufaniem, a kulturą można zaobserwować także wtedy, gdy pomiędzy elementami organizacji występują luki i nakładanie się odpowiedzialności, co może mieć wpływ na możliwość szybkiej realizacji proponowanych działań (zwłaszcza nowych). Na przykład, wiele organizacji o zdecentralizowanej strukturze zarządzania może wolniej przyjmować zmiany, jeśli nie podjęto szeroko zakrojonych wysiłków w celu zwiększenia koordynacji i poprawy zaufania między elementami organizacji. Załóżmy, że niektóre organizacje otrzymały polecenie od nadrzędnych organów (patrz Załącznik G: Model obowiązkowego zaufania), aby swobodniej dzielić się informacjami z innymi organizacjami. Jeśli organizacje te mają doświadczenie i tradycję ścisłego kontrolowania informacji, mogą niechętnie dzielić się informacjami z podmiotami zewnętrznymi, nawet jeśli otrzymały takie polecenie. W takich sytuacjach organizacje mogą wymagać, aby przed udostępnieniem informacji, organizacje partnerskie przedstawiły konkretne dowody na to, jakie kroki podjęły w celu ochrony informacji przeznaczonych do udostępnienia.

2.8.3. Strategia inwestycyjna i tolerancja ryzyka

Strategie inwestycyjne i tolerancja ryzyka organizacyjnego również są ze sobą powiązane. Organizacje mogą uznać, że istnieje potrzeba przeciwdziałania zaawansowanym trwałym zagrożeniom, w przypadku których przeciwnicy osiągnęli pewien stopień penetracji i punkt zaczepienia w organizacyjnych systemach informatycznych i środowiskach, w których te systemy funkcjonują. Inwestycje strategiczne, które są wymagane w celu przeciwdziałania tego typu zagrożeniom, mogą być częściowo uzależnione od tolerancji ryzyka danej organizacji. Organizacje charakteryzujące się mniejszą tolerancją ryzyka mogą skupić się na inwestycjach w technologie informatyczne, które uniemożliwiają przeciwnikom uzyskanie dalszego dostępu do organizacji i/lub ograniczaniu szkód wyrządzonych organizacji, nawet jeśli odbywa się to kosztem osiągnięcia niektórych z wielu korzyści dla misji/biznesu, jakie może przynieść automatyzacja. Organizacje o większej tolerancji ryzyka mogą skoncentrować inwestycje na technologiach informatycznych, które zapewniają większe korzyści dla misji/biznesu, nawet jeśli korzyści te są osiągane kosztem uzyskania przez przeciwników

pewnych zysków lub korzyści z naruszenia systemów informatycznych i infrastruktury wspomagającej.

2.8.4. Kultura i tolerancja ryzyka

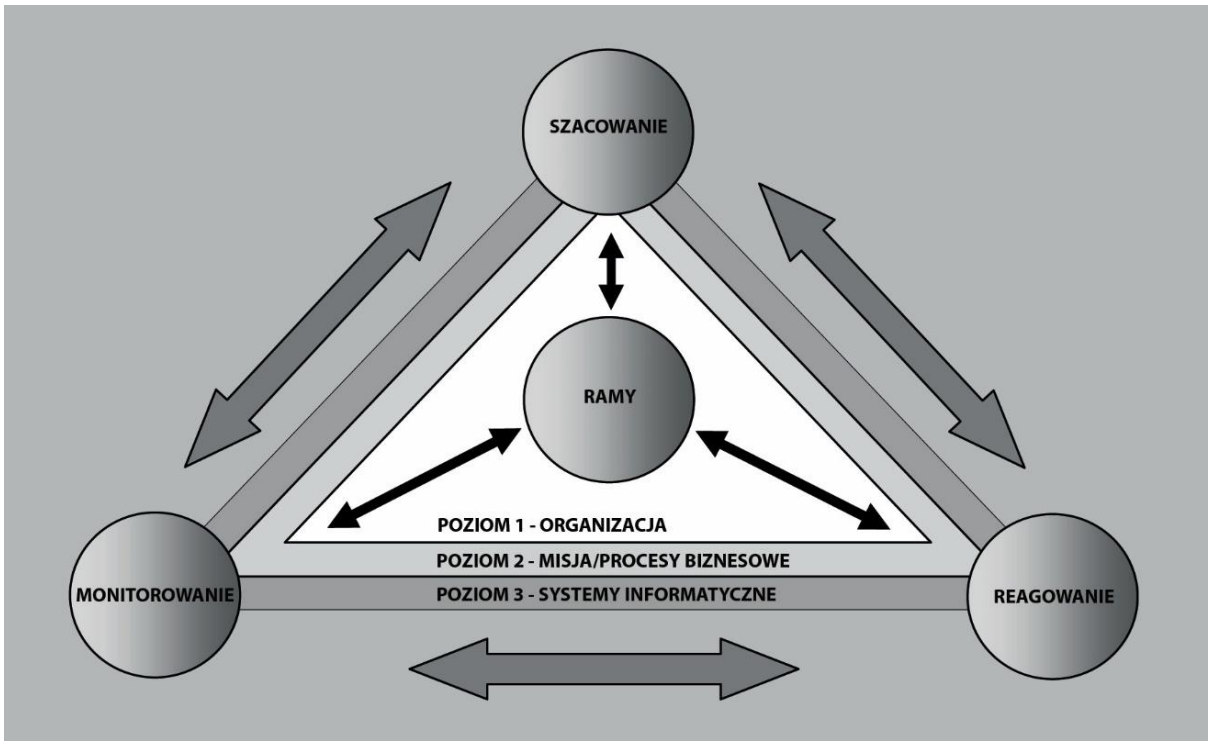
Ważnym elementem zarządzania ryzykiem w organizacji jest określenie, jaka jest tolerancja ryzyka organizacyjnego na dany rodzaj straty. Tolerancję ryzyka można opisać, jako połączenie kulturowej gotowości do akceptowania pewnych rodzajów strat w organizacji oraz subiektywnych działań związanych z ryzykiem podejmowanych przez liderów/kadrę kierowniczą wyższego szczebla. Decyzje podejmowane w organizacjach w oparciu o ryzyko często odzwierciedlają połączenie tolerancji ryzyka stosowanej przez wyższego szczebla liderów/kadrę kierowniczą oraz tolerancji ryzyka zakorzenionej w kulturze organizacji. Ustalając tolerancję ryzyka organizacyjnego, bada się wartości, przekonania i wzorce obowiązujące w organizacji, aby zrozumieć, dlaczego dokonuje się kompromisów w zakresie ryzyka. W przypadku niektórych organizacji, zwłaszcza tych, które mają do czynienia z informacjami krytycznymi i/lub wrażliwymi, informacjami umożliwiającymi identyfikację osób lub informacjami niejawnymi, nacisk kładzie się często na zapobieganie nieuprawnionemu ujawnieniu informacji. Z kolei w organizacjach, które kierują się kulturą organizacyjną oraz charakterem misji i funkcji biznesowych, nacisk kładzie się na utrzymanie dostępności systemów informatycznych w celu osiągnięcia ciągłej zdolności operacyjnej. W ramach ustalania tolerancji ryzyka organizacyjnego, szacowanie ryzyka identyfikuje rodzaje i poziomy ryzyka, na które organizacja może być narażona. Ocena ta uwzględnia zarówno prawdopodobieństwo, jak i wpływ niepożądanych zdarzeń (patrz: Rozdział trzeci, Proces zarządzania ryzykiem).

ROZDZIAŁ TRZECI PROCES

STOSOWANIE KONCEPCJI ZARZĄDZANIA RYZYKIEM W CAŁEJ ORGANIZACJI

W niniejszym rozdziale opisano proces zarządzania ryzykiem w zakresie bezpieczeństwa informacji obejmujący: (i) ogólny przegląd procesu zarządzania ryzykiem; (ii) sposób, w jaki organizacje tworzą kontekst do podejmowania decyzji opartych na ryzyku; (iii) sposób, w jaki organizacje szacują ryzyko, biorąc pod uwagę zagrożenia, podatności, prawdopodobieństwo oraz konsekwencje/wpływ; (iv) sposób, w jaki organizacje reagują na ryzyko po jego określeniu; oraz (v) sposób, w jaki organizacje monitorują ryzyko w miarę upływu czasu, przy zmieniających się potrzebach misji/biznesu, środowiskach operacyjnych i wspierających systemach informatycznych. W niniejszym rozdziale opisano przedstawiony w rozdziale drugim proces zarządzania ryzykiem, w tym możliwość jego zastosowania na trzech Poziomach zarządzania ryzykiem. Każdy z etapów procesu zarządzania ryzykiem (tj. określenie ram ryzyka, szacowanie ryzyka, reakcja na ryzyko i monitorowanie ryzyka) opisano w sposób ustrukturyzowany, koncentrując się na danych wejściowych lub warunkach wstępnych niezbędnych do rozpoczęcia danego etapu, konkretnych działaniach składających się na ten etap oraz danych wyjściowych lub warunkach końcowych wynikających z tego etapu[60]. Wpływ koncepcji ryzyka opisanych w rozdziale drugim (np. tolerancji ryzyka, zaufanie i kultura) został również omówiony w kontekście procesu zarządzania ryzykiem i jego wielopoziomowego zastosowania. Rysunek 4 ilustruje proces zarządzania ryzykiem stosowany na różnych poziomach: organizacji, misji/procesu biznesowego oraz systemu informatycznego. Dwukierunkowe strzałki na rysunku wskazują, że przepływy informacji i komunikacji pomiędzy komponentami zarządzania ryzykiem, jak również kolejność wykonywania poszczególnych komponentów, mogą być elastyczne i odpowiadać dynamicznej naturze procesu zarządzania ryzykiem, realizowanego na wszystkich trzech Poziomach.

[60] Dodatkowe wskazówki dotyczące wybranych kroków w procesie zarządzania ryzykiem (np. szacowanie ryzyka, monitorowanie ryzyka) można znaleźć w innych publikacjach wymienionych w Załączniku A.



Rysunek 4. Proces zarządzania ryzykiem stosowany na wszystkich Poziomach.

Kroki podejmowane w procesie zarządzania ryzykiem nie są z natury rzeczy sekwencyjne. Są one wykonywane w różny sposób, w zależności od poziomu, na którym dany krok jest stosowany, oraz od wcześniejszych działań związanych z każdym z tych kroków. Niezmienne jest to, że wyniki lub warunki końcowe danego etapu zarządzania ryzykiem mają bezpośredni wpływ na jeden lub więcej pozostałych etapów procesu zarządzania ryzykiem. Organizacje mają znaczną swobodę w sposobie wykonywania poszczególnych etapów zarządzania ryzykiem (np. kolejność, stopień rygorystyczności, formalność i dokładność stosowania) oraz w zakresie gromadzenia i udostępniania wyników każdego etapu - zarówno we własnym zakresie, jak i na zewnątrz. Ostatecznie, celem stosowania procesu zarządzania ryzykiem i związanych z nim koncepcji dotyczących ryzyka jest lepsze zrozumienie ryzyka związanego z bezpieczeństwem informacji w kontekście szerszych działań i decyzji organizacji, a w szczególności w odniesieniu do operacji i aktywów organizacji, osób, innych organizacji i Państwa.

3.1. RYZYKO RAMOWE

Podstawowym rezultatem opracowywania ram ryzyka jest strategia zarządzania ryzykiem, która określa, w jaki sposób organizacje zamierzają szacować ryzyko, reagować na ryzyko i monitorować je. Strategia zarządzania ryzykiem określa konkretne założenia, ograniczenia, tolerancję ryzyka oraz priorytety i kompromisy, które są wykorzystywane w organizacjach przy podejmowaniu decyzji inwestycyjnych i operacyjnych. Strategia zarządzania ryzykiem obejmuje również wszelkie decyzje i rozważania na poziomie strategicznym dotyczące sposobu zarządzania przez kierownictwo wyższego szczebla ryzykiem związanym z operacjami i aktywami organizacji, osobami, innymi organizacjami oraz Państwem.

Na Poziomie 1 liderzy/kadra kierownicza wyższego szczebla, w porozumieniu i we współpracy z funkcją wykonawczą ds. ryzyka (RE), definiują ramy ryzyka organizacyjnego, w tym rodzaje wspieranych decyzji dotyczących ryzyka (np. reakcji na ryzyko), sposób i warunki szacowania ryzyka w celu wsparcia tych decyzji dotyczących ryzyka oraz sposób monitorowania ryzyka (np. jaki poziom szczegółowości, w jakim kształcie i z jaką częstotliwością).

Na Poziomie 2 właściciele misji/biznesu stosują zrozumienie ram ryzyka organizacyjnego w celu rozwiązania problemów specyficznych dla misji/biznesu danej organizacji (np. dodatkowe założenia, ograniczenia, priorytety i kompromisy).

Na Poziomie 3 menedżerowie programów, właściciele systemów informatycznych i dostawcy zabezpieczeń wspólnych stosują swoje zrozumienie ram ryzyka organizacyjnego w oparciu o to, jak decydenci na Poziomach 1 i 2 postanowili zarządzać ryzykiem.

Ramy zarządzania ryzykiem[61] są podstawowym sposobem rozwiązywania problemów wynikających z ryzyka występującego na Poziomie 3. RMF odnosi się do kwestii związanych z projektowaniem, rozwojem, wdrażaniem, obsługą i utylizacją systemów informatycznych organizacji oraz środowisk, w których te systemy funkcjonują. Ramy ryzyka można

[61] Ramy zarządzania ryzykiem (*ang. Risk Management Framework - RMF*), które funkcjonują głównie na Poziomie 3, zostały opisane w publikacji NSC 800-37.

dostosować na Poziomie 3 w oparciu o aktualną fazę cyklu życia systemu, co dodatkowo ogranicza potencjalne reakcje na ryzyko. Początkowo ramy ryzyka organizacyjnego mogą nie być jednoznaczne lub mogą nie być zdefiniowane w kategoriach odpowiadających poziomom zarządzania ryzykiem. W przypadku braku wyraźnych ram ryzyka (opisujących założenia, ograniczenia, tolerancję ryzyka oraz priorytety/kompromisy), właściciele misji/biznesu mogą mieć rozbieżne poglądy na ryzyko lub sposób zarządzania nim. Utrudnia to wspólne zrozumienie na Poziomie 1, w jaki sposób ryzyko związane z bezpieczeństwem informacji przyczynia się do ryzyka organizacyjnego; na Poziomie 2 - sposobu, w jaki ryzyko akceptowane dla jednej misji lub funkcji biznesowej potencjalnie wpływa na ryzyko w przypadku innych misji lub funkcji biznesowych. Różnice w tolerancji ryzyka oraz leżące u ich podstaw założenia, ograniczenia i priorytety/kompromisy wynikają z uwarunkowań operacyjnych i/lub architektonicznych i powinny być rozumiane i akceptowane przez liderów/kierowników wyższego szczebla w poszczególnych organizacjach.

KROK 1: OKREŚLANIE RAM RYZYKA

Dane wejściowe i warunki wstępne

Ramy ryzyka to zbiór założeń, ograniczeń, tolerancji ryzyka oraz priorytetów i kompromisów, które kształtują podejście organizacji do zarządzania ryzykiem. Określanie ram ryzyka opiera się na strukturze zarządzania organizacją, sytuacji finansowej, środowisku prawnym/regulacyjnym, strategii inwestycyjnej, kulturze oraz relacjach zaufania wewnątrz i pomiędzy organizacjami. Dane wejściowe do etapu określania ryzyka obejmują na przykład przepisy prawa, polityki, dyrektywy, regulacje, stosunki umowne oraz uwarunkowania finansowe, które nakładają ograniczenia na potencjalne decyzje organizacji dotyczące ryzyka. Inne dane wejściowe do tworzenia ram ryzyka mogą obejmować na przykład określone informacje uzyskane od organizacji w celu jednoznacznego określenia: (i) identyfikacji relacji zaufania i modeli zaufania (patrz Załącznik G), które wynikają z istniejących protokołów ustaleń lub porozumień (MOU lub MOA); oraz (ii) identyfikacji struktur i procesów zarządzania, które wskazują zakres lub ograniczenia uprawnień w zakresie podejmowania decyzji dotyczących ryzyka, które mogą być delegowane do właścicieli misji lub biznesu. Kluczowym warunkiem wstępnym opracowania ram ryzyka jest zobowiązanie kierownictwa

wyższego szczebla do zdefiniowania wyraźnej strategii zarządzania ryzykiem oraz uznanie właścicieli misji/biznesu za odpowiedzialnych i rozliczalnych za realizację tej strategii.

Wytyczne opracowane na etapie określania ram ryzyka oraz założenia, ograniczenia, tolerancja ryzyka oraz priorytety/kompromisy wykorzystane do opracowania tych wytycznych mogą być nieodpowiednie dla celów jednej lub kilku misji organizacyjnych lub funkcji biznesowych. Ponadto, środowisko ryzyka może się zmieniać w czasie. Dlatego też proces zarządzania ryzykiem pozwala na przekazywanie informacji zwrotnych do etapu określania ryzyka z innych etapów procesu, w następujący sposób:

- *Szacowanie ryzyka:* informacje uzyskane podczas oceny ryzyka mogą wpłynąć na pierwotne założenia, zmienić ograniczenia dotyczące odpowiednich reakcji na ryzyko, określić dodatkowe kompromisy lub zmienić priorytety. Na przykład charakterystyka przeciwników (w tym reprezentatywnych taktyk, technik i procedur) lub źródła informacji o podatnościach mogą nie być zgodne z tym, jak niektóre organizacje realizują swoje misje/funkcje biznesowe; źródło informacji o zagrożeniach/podatnościach, które jest przydatne dla jednej misji/funkcji biznesowej, może być w rzeczywistości przydatne dla innych; lub wytyczne organizacyjne dotyczące oceny ryzyka w warunkach niepewności mogą być zbyt uciążliwe lub niewystarczająco zdefiniowane, aby były przydatne dla jednej lub więcej misji/funkcji biznesowych.
- *Reakcja na ryzyko:* Informacje ujawnione podczas opracowywania alternatywnych kierunków działania mogą świadczyć o tym, że określanie ryzyka spowodowało usunięcie lub nieuwzględnienie niektórych potencjalnie opłacalnych alternatyw. Taka sytuacja może stanowić dla organizacji wyzwanie do ponownego przeanalizowania pierwotnych założeń lub zbadania sposobów zmiany ustalonych ograniczeń.
- *Monitorowanie ryzyka:* Monitorowanie środków bezpieczeństwa przez organizacje może wykazać, że dana klasa zabezpieczeń lub implementacja konkretnego zabezpieczenia jest stosunkowo nieefektywna, biorąc pod uwagę inwestycje w ludzi, procesy lub technologię. Taka sytuacja może prowadzić do zmian w założeniach dotyczących tego, jakie rodzaje reakcji na ryzyko są preferowane przez organizacje.

Monitorowanie środowiska operacyjnego może ujawnić zmiany w obszarze zagrożeń (np. zmiany w taktykach, technikach i procedurach odnotowanych we wszystkich systemach informatycznych organizacji; rosnącą częstotliwość i/lub intensywność ataków na określone misje/funkcje biznesowe), które powodują, że organizacje muszą zrewidować pierwotne założenia dotyczące zagrożeń i/lub poszukać innych źródeł informacji o zagrożeniach. Znaczący postęp w zakresie defensywnych lub proaktywnych rozwiązań operacyjnych i technicznych może spowodować potrzebę zrewidowania strategii inwestycyjnej określonej podczas etapu tworzenia ram ryzyka. Monitorowanie otoczenia prawnego/regulacyjnego może również wpłynąć na zmiany w założeniach lub ograniczeniach. Ponadto, monitorowanie ponoszonego ryzyka może skutkować potrzebą ponownego rozważenia organizacyjnej tolerancji ryzyka, jeśli istniejąca deklaracja tolerancji ryzyka nie wydaje się odpowiadać realiom operacyjnym.

Funkcjonowanie

ZAŁOŻENIA DOTYCZĄCE RYZYKA

ZADANIE 1-1: Określenie założeń, które mają wpływ na sposób szacowania, reagowania i monitorowania ryzyka w organizacji.

Wskazówki uzupełniające: Organizacje, które identyfikują, charakteryzują i dostarczają reprezentatywnych przykładów źródeł zagrożeń, podatności, konsekwencji/skutków i prawdopodobieństw, promują wspólną terminologię i ramy odniesienia dla porównywania i zajmowania się ryzykiem w różnych obszarach misji/biznesu. Organizacje mogą również wybrać odpowiednie metodologie oceny ryzyka, w zależności od zarządzania organizacją, kultury i stopnia rozbieżności misji/funkcji biznesowych w ramach poszczególnych organizacji. Na przykład, organizacje o wysoce scentralizowanych strukturach zarządzania mogą zdecydować się na stosowanie jednej metodologii oceny ryzyka. Organizacje o hybrydowych strukturach zarządzania mogą wybrać wiele metodologii oceny ryzyka dla Poziomu 2 oraz dodatkową metodologię oceny ryzyka dla Poziomu 1, która asymiluje i harmonizuje ustalenia, wyniki i obserwacje z ocen ryzyka Poziomu 2. Alternatywnie, gdy autonomia i różnorodność są kluczowe dla kultury organizacyjnej, organizacje mogą

zdefiniować wymagania dotyczące stopnia rygoryzmu i formy wyników, pozostawiając wybór konkretnych metodologii oceny ryzyka właścicielom misji/biznesu.

Źródła zagrożeń

Źródła zagrożeń powodują zdarzenia mające niepożądane konsekwencje lub niekorzystny wpływ na działania i aktywa organizacji, jednostki, inne organizacje oraz Państwo. Źródła zagrożeń obejmują: (i) wrogie cyber/fizyczne ataki; (ii) ludzkie błędy zaniechania lub popełnienia; lub (iii) katastrofy naturalne i spowodowane przez człowieka. W przypadku zagrożeń spowodowanych wrogimi cyberatakami lub atakami fizycznymi, organizacje przedstawiają zwięzłą charakterystykę typów taktyk, technik i procedur stosowanych przez przeciwników, które mają być objęte środkami ochrony i przeciwdziałania (tj. środkami bezpieczeństwa) wdrożonymi na Poziomie 1 (poziom organizacji), Poziomie 2 (poziom misji/procesu biznesowego) i Poziomie 3 (poziom systemu informatycznego) - z wyraźnym wskazaniem typów źródeł zagrożeń, które mają być objęte środkami bezpieczeństwa, jak również z wyraźnym wskazaniem tych, które nie są objęte zabezpieczeniami. Przeciwnicy mogą być charakteryzowani w kategoriach poziomów zagrożenia (na podstawie zdolności, zamiarów i celów) lub z dodatkowymi szczegółami. Organizacje ujawniają wszelkie założenia dotyczące celów, zamiarów i zdolności źródła zagrożenia. Następnie organizacje identyfikują zestaw reprezentatywnych zdarzeń związanych z zagrożeniami. Ten zestaw zdarzeń stanowi wytyczne dotyczące poziomu szczegółowości, z jakim zdarzenia są opisywane. Organizacje określają również warunki, kiedy należy uwzględniać zdarzenia zagrożeń w ocenach ryzyka. Na przykład, organizacje mogą ograniczyć szacowanie ryzyka do tych zdarzeń zagrożeń, które zostały faktycznie zaobserwowane (wewnętrznie lub zewnętrznie przez partnerów lub inne organizacje) lub alternatywnie określić, że można również brać pod uwagę zdarzenia zagrożeń opisane przez wiarygodnych badaczy. Wreszcie, organizacje określają źródła informacji o zagrożeniach, które zostały uznane za wiarygodne i użyteczne (np. sektorowe Centra Wymiany i Analizy Informacji [ISAC]). Relacje zaufania określają, od których partnerów, dostawców i klientów pozyskiwane są informacje o zagrożeniach, a także oczekiwania wobec tych partnerów, dostawców i klientów w kolejnych etapach procesu zarządzania ryzykiem. Ustanawiając wspólne punkty wyjścia do identyfikacji źródeł zagrożeń

na Poziomie 1, organizacje zapewniają podstawę do agregacji i konsolidacji wyników szacowania ryzyka na Poziomie 2 (w tym szacowania ryzyka przeprowadzonego dla koalicji misji i obszarów biznesowych lub dla dostawców zabezpieczeń wspólnych) w ogólną ocenę ryzyka dla organizacji, jako całości. Na Poziomie 2, właściciele misji/biznesu mogą zidentyfikować dodatkowe źródła informacji o zagrożeniach specyficznych dla misji organizacyjnych lub funkcji biznesowych. Źródła te są zazwyczaj oparte na: (i) konkretnym sektorze biznesowym lub sektorze infrastruktury krytycznej (np. sektorowy ISAC); (ii) środowiskach operacyjnych specyficznych dla misji lub linii biznesowych (np. morskie, przestrzeń powietrzna); oraz (iii) zewnętrznych zależnościach (np. GPS lub komunikacja satelitarna). Charakterystyki źródeł zagrożeń są dopracowywane pod kątem misji/funkcji biznesowych ustanowionych przez organizacje - w rezultacie niektóre źródła zagrożeń mogą nie stanowić problemu, podczas gdy inne można opisać bardziej szczegółowo. Na Poziomie 3 menedżerowie programów, właściciele systemów informatycznych i dostawcy zabezpieczeń wspólnych biorą pod uwagę fazę cyklu życia systemu, aby określić poziom szczegółowości, z jakim można rozpatrywać zagrożenia. Większa szczegółowość zagrożeń jest zazwyczaj dostępna w późniejszej fazie cyklu życia.

Podatności

Organizacje określają metody stosowane do charakteryzowania podatności, spójne z charakteryzowaniem źródeł zagrożeń i zdarzeń. Podatności mogą być związane z możliwymi do wykorzystania słabościami lub niedociągnięciami w: (i) komponentach sprzętu, aplikacjach, lub oprogramowania układowego, z których składają się systemy informatyczne organizacji (lub środki bezpieczeństwa stosowane w ramach tych systemów lub dziedziczone przez nie); (ii) procesach misji/biznesu i architekturach korporacyjnych (w tym wbudowanych architekturach bezpieczeństwa informacji) wdrożonych przez organizacje; lub (iii) strukturach lub procesach zarządzania organizacją. Podatności mogą być również związane z wrażliwością organizacji na niekorzystny wpływ, konsekwencje lub szkody pochodzące ze źródeł zewnętrznych (np. fizyczne zniszczenie infrastruktury sieci energetycznej niebędącej własnością organizacji). Organizacje dostarczają wskazówek, w jaki sposób traktować zależności od organizacji zewnętrznych, jako podatności

w przeprowadzanych szacunkach ryzyka. Wytyczne te mogą być oparte na typach relacji zaufania, jakie organizacje nawiązały z zewnętrznymi dostawcami. Organizacje określają stopień szczegółowości, z jaką podatności są opisywane (np. ogólne terminy, identyfikatory Com on Vulnerability Enumeration [CVE], identyfikacja słabych/niedoskonałych środków bezpieczeństwa), podając kilka reprezentatywnych przykładów odpowiadających reprezentatywnym zagrożeniom. Struktury i procesy zarządzania organizacyjnego określają, w jaki sposób informacje o podatnościach są współdzielone pomiędzy organizacjami. Organizacje mogą również zidentyfikować źródła informacji o podatnościach, które zostały uznane za wiarygodne i użyteczne. Na Poziomie 2, właściciele misji/biznesu mogą zdecydować się na zidentyfikowanie dodatkowych źródeł informacji o podatnościach (np. sektorowy ISAC dla informacji o podatnościach specyficznych dla danego sektora). Na Poziomie 3, kierownicy programów, właściciele systemów informatycznych i dostawcy zabezpieczeń wspólnych biorą pod uwagę fazę cyklu życia systemu - a w szczególności technologie wchodzące w skład systemu - w celu określenia poziomu szczegółowości, z jakim podatności mogą być rozpatrywane. Organizacje jasno określają wszelkie założenia dotyczące stopnia podatności organizacji lub systemu informatycznego na konkretne źródła zagrożeń (z nazwy lub typu).

Wpływ i konsekwencje

Organizacje określają wskazówki dotyczące sposobu szacowania wpływu zdarzeń niepożądanych na działalność organizacji (tj. misję, funkcje, wizerunek i reputację), aktywa organizacji, osoby, inne organizacje i Państwo (np. przy użyciu standardu NSC 199, lub bardziej rozbudowanego podejścia). Organizacje mogą doświadczać konsekwencji/skutków zdarzeń niepożądanych na poziomie systemu informatycznego (np. niewykonanie wymaganych zadań), na poziomie misji/procesu biznesowego (np. niezrealizowanie w pełni celów misji/procesu biznesowego) oraz na poziomie organizacyjnym (np. niespełnienie wymogów prawnych lub regulacyjnych, narażenie na szwank reputacji lub relacji z innymi podmiotami albo podważenie długoterminowej rentowności). Organizacje określają na Poziomie 1 konsekwencje i rodzaje wpływu, które mają być uwzględnione na Poziomie 2, czyli na poziomie misji/procesu biznesowego. Zdarzenie niepożądane może mieć wiele

konsekwencji i różne rodzaje wpływu, na różnych poziomach i w różnych ramach czasowych. Na przykład ujawnienie informacji wrażliwych (np. informacji umożliwiających identyfikację osób) przez konkretny obszar misji/biznesu (np. zasoby ludzkie) może mieć konsekwencje dla całej organizacji i niekorzystny wpływ na reputację; wpływ na system informatyczny w kontekście wielu systemów, polegający na tym, że atakujący z większą łatwością pokonuje środki bezpieczeństwa związane z identyfikacją i uwierzytelnianiem; oraz wpływ na misję/proces biznesowy (w jednym lub kilku obszarach misji/biznesu), polegający na tym, że atakujący fałszuje informacje, na których opierają się przyszłe decyzje. Aby zapewnić spójność, organizacje określają na Poziomie 1, jak należy oceniać konsekwencje/skutki doświadczane w różnych przedziałach czasowych. Na Poziomie 2 właściciele misji/biznesu mogą w razie potrzeby wzmocnić wytyczne organizacyjne. Rodzaje konsekwencji i skutków uwzględnianych w określaniu ryzyka są identyfikowane, aby zapewnić podstawę do określania, agregowania i/lub konsolidowania wyników szacowania ryzyka oraz ułatwić komunikację dotyczącą ryzyka. Organizacje zapewniają również wytyczne dla Poziomu 2 i Poziomu 3 w odniesieniu do zakresu, w jakim oszacowania ryzyka mają uwzględniać ryzyko ponoszone przez inne organizacje i Państwo. Organizacje wyraźnie określają wszelkie założenia dotyczące stopnia wpływu/konsekwencji związanych z konkretnymi źródłami zagrożeń (z nazwy lub według typu) lub z konkretnymi podatnościami (indywidualnie lub według typu).

Prawdopodobieństwo

Organizacje mogą stosować różne podejścia do określania prawdopodobieństwa wystąpienia zdarzenia zagrożenia. Niektóre organizacje traktują prawdopodobieństwo wystąpienia zdarzenia zagrożenia oraz prawdopodobieństwo, że w przypadku jego wystąpienia spowoduje ono niekorzystne skutki, jako odrębne czynniki, podczas gdy inne organizacje oceniają prawdopodobieństwo wystąpienia zagrożenia, jako kombinację tych czynników. Ponadto niektóre organizacje preferują ilościowe szacowanie ryzyka, podczas gdy inne, zwłaszcza, gdy szacowanie wiąże się z wysokim stopniem niepewności, wolą jakościowe szacowanie ryzyka. Określenie prawdopodobieństwa może być oparte na założeniach dotyczących zagrożeń lub na rzeczywistych danych o zagrożeniach (np. danych historycznych

dotyczących cyberataków, trzęsień ziemi lub konkretnych informacji o możliwościach, zamiarach i celach przeciwnika). Jeśli dostępne są konkretne i wiarygodne dane dotyczące zagrożeń (np. rodzaje cyberataków, trendy w zakresie cyberataków, częstotliwość ataków), organizacje mogą wykorzystać dane empiryczne i analizy statystyczne do określenia bardziej szczegółowych prawdopodobieństw wystąpienia zdarzeń związanych z zagrożeniami. Organizacje wybierają metodę zgodną z kulturą organizacyjną i tolerancją ryzyka. Organizacje mogą również przyjąć jednoznaczne założenia dotyczące prawdopodobieństwa, że zdarzenie związane z zagrożeniem będzie miało następujące negatywne skutki: (i) najgorszy przypadek (tzn. atak się powiedzie, chyba, że istnieją mocne, obiektywne przesłanki, aby przypuszczać inaczej); (ii) najlepszy przypadek (tzn. atak się nie powiedzie, chyba, że istnieją konkretne, wiarygodne informacje, które temu przeczą); lub (iii) coś pomiędzy najlepszym, a najgorszym przypadkiem (np. przypadek najbardziej prawdopodobny). Organizacje dokumentują wszelkie przyjęte założenia. Organizacje mogą korzystać z danych empirycznych i analiz statystycznych w celu określenia prawdopodobieństwa wystąpienia zagrożeń. Organizacje wybierają metodę zgodną z kulturą organizacyjną, rozumieniem środowiska operacyjnego i tolerancją ryzyka.

OGRANICZANIE RYZYKA

ZADANIE 1-2: Identyfikacja ograniczeń w prowadzeniu działań związanych z szacowaniem ryzyka, reagowaniem na ryzyko i monitorowaniem ryzyka w organizacji.

Wskazówki uzupełniające: Realizacja procesu zarządzania ryzykiem może być ograniczana na różne sposoby, z których niektóre są bezpośrednie i oczywiste, a inne pośrednie. Ograniczenia finansowe mogą ograniczać zestaw działań związanych z zarządzaniem ryzykiem w sposób bezpośredni (np. poprzez ograniczenie całkowitych zasobów dostępnych na inwestycje w ocenę ryzyka, zabezpieczenia lub środki zaradcze) lub pośredni (np. poprzez eliminację działań, które - choć wiążą się ze stosunkowo niewielkimi inwestycjami w reakcję na ryzyko - pociągają za sobą ograniczenie lub rezygnację z inwestycji w dotychczasowe systemy informatyczne lub technologie informatyczne). Organizacje mogą również stwierdzić, że konieczność dalszego korzystania z dotychczasowych systemach informatycznych może ograniczyć dostępne dla organizacji opcje zarządzania ryzykiem.

Ograniczenia mogą również obejmować wymogi prawne, regulacyjne i/lub umowne. Takie ograniczenia mogą być odzwierciedlone w polityce organizacji (np. ograniczenia dotyczące outsourcingu, ograniczenia i/lub wymagania dotyczące informacji, które mają być gromadzone w ramach monitorowania ryzyka). Kultura organizacyjna może nakładać pośrednie ograniczenia na zmiany w zarządzaniu (np. uniemożliwiając przejście od zdecentralizowanych do hybrydowych struktur zarządzania) oraz na to, które środki bezpieczeństwa są uważane przez organizacje za potencjalne zabezpieczenia wspólne. W szczególności postawa organizacji wobec ryzyka związanego z technologiami informatycznymi, która na przykład sprzyja szerokiej automatyzacji i wczesnemu przyjmowaniu nowych technologii, może hamować stopień zapobiegania ryzyka, a być może także jego ograniczania. Wszelkie ograniczenia kulturowe, które ograniczają wgląd wyższego szczebla kierowniczego/wykonawczego (np. CIO) w systemy informatyczne organizacji, które są poza jego formalnymi uprawnieniami (np. systemy powiązane z misją), mogą utrudniać ogólne zrozumienie złożoności środowiska systemów informatycznych i związanego z nim ryzyka ponoszonego przez organizację. Na Poziomie 2 właściciele misji/biznesu interpretują ograniczenia w świetle misji/funkcji biznesowych organizacji. Niektóre ograniczenia prawne mogą nie mieć zastosowania do poszczególnych misji/funkcji biznesowych (np. przepisy dotyczące operacji międzynarodowych, gdy obszary misji/biznesu są ograniczone do kraju lub Unii Europejskiej). Ewentualnie mogą mieć zastosowanie dodatkowe wymagania (np. procesy misji/biznesu realizowane wspólnie z inną organizacją, co nakłada ograniczenia umowne). Na Poziomie 3 właściciele systemów informatycznych, dostawcy zabezpieczeń wspólnych i/lub menedżerowie programów interpretują ograniczenia dotyczące całej organizacji oraz specyficzne dla misji/biznesu w odniesieniu do swoich systemów i środowisk działania (np. spełnianie wymagań dotyczących zapewnienia specyficznych środków bezpieczeństwa z wykorzystaniem zabezpieczeń wspólnych).

TOLERANCJA RYZYKA

ZADANIE 1-3: Określenie poziomu tolerancji ryzyka organizacji.

Wytyczne uzupełniające: Tolerancja ryzyka to poziom ryzyka, który organizacja jest skłonna zaakceptować w dążeniu do osiągnięcia strategicznych celów i zadań. Organizacje określają

tolerancję ryzyka związanego z bezpieczeństwem informacji w skali całej organizacji, biorąc pod uwagę wszystkie misje/funkcje biznesowe. Organizacje mogą stosować różne techniki określania tolerancji ryzyka związanego z bezpieczeństwem informacji (np. poprzez wyznaczanie granic prawdopodobieństwa wpływu na ryzyko lub poprzez wykorzystanie zestawu reprezentatywnych scenariuszy). Organizacje określają również tolerancję na inne rodzaje ryzyka organizacyjnego i operacyjnego (np. ryzyko finansowe, ryzyko bezpieczeństwa, ryzyko naruszenia zgodności lub ryzyko utraty reputacji). Na Poziomie 2 właściciele misji/biznesu mogą wykazywać odmienną tolerancję ryzyka niż organizacja jako całość. Funkcja wykonawcza ds. ryzyka (RE) zapewnia organizacjom sposoby rozwiązywania takich różnic w tolerancji ryzyka na poziomie 2. Poziom ryzyka szczątkowego akceptowany przez osoby autoryzujące systemy informatyczne lub odziedziczone zabezpieczenia wspólne mieści się w ramach organizacyjnej tolerancji ryzyka, a nie w ramach indywidualnej tolerancji ryzyka osób autoryzujących. Ponadto organizacje dostarczają na Poziomie 2 i Poziomie 3 wytyczne dotyczące oceny ryzyka w odniesieniu do poszczególnych procesów lub systemów informatycznych związanych z misją/biznesem oraz koncentrują się na krótkoterminowej efektywności misji/biznesu z uwzględnieniem długoterminowej, strategicznej tolerancji ryzyka organizacyjnego. Dodatkowe informacje na temat tolerancji ryzyka znajdują się w sekcji 2.3.3.

PRIORYTETY I KOMPROMISY

ZADANIE 1-4: Ustalenie priorytetów i kompromisów w zarządzaniu ryzykiem.

Wskazówki uzupełniające: Ryzyko jest postrzegane na różnych płaszczyznach, w różnych formach i w różnych ramach czasowych. Na Poziomie 1 organizacje dokonują kompromisowych rozwiązań i ustalają priorytety reagowania na takie ryzyko. Organizacje mają zazwyczaj wiele priorytetów, które czasami są ze sobą sprzeczne, co generuje potencjalne ryzyko. Podejścia stosowane przez organizacje do zarządzania portfelem ryzyk odzwierciedlają kulturę organizacyjną, tolerancję ryzyka, a także założenia i ograniczenia związane z ryzykiem. Podejścia te są zazwyczaj zawarte w planach strategicznych, politykach i mapach drogowych organizacji, które mogą wskazywać na preferencje dotyczące różnych form reagowania na ryzyko. Na przykład, organizacje mogą być skłonne zaakceptować

krótkoterminowe ryzyko nieznacznego pogorszenia działania w celu osiągnięcia długoterminowego zmniejszenia ryzyka związanego z bezpieczeństwem informacji. Taki kompromis może być jednak nie do przyjęcia w przypadku szczególnie krytycznej misji/funkcji biznesowej (np. wymagania czasu rzeczywistego w przypadku wielu systemów sterowania przemysłowego i procesowego). W przypadku tego priorytetowego obszaru może być wymagane inne podejście do poprawy bezpieczeństwa, w tym zastosowanie kompensacyjnych środków bezpieczeństwa.

Dane wyjściowe i warunki końcowe

Wynikiem etapu określania ram dla ryzyka jest *strategia zarządzania ryzykiem*, która określa, w jaki sposób organizacja zamierza oceniać, reagować i monitorować ryzyko w czasie. W wyniku tego etapu powstaje również zestaw polityk, procedur, standardów, wytycznych i zasobów organizacyjnych obejmujących następujące zagadnienia: (i) zakres procesu zarządzania ryzykiem organizacyjnym (np. objęte jednostki organizacyjne; funkcje misji/biznesu, na które ma wpływ; sposób stosowania działań z zakresu zarządzania ryzykiem w ramach poziomów zarządzania ryzykiem); (ii) wytyczne dotyczące oceny ryzyka, w tym na przykład charakterystyka źródeł zagrożeń, źródła informacji o zagrożeniach, reprezentatywne zdarzenia związane z zagrożeniami (w szczególności taktyki, techniki i procedury przeciwnika), moment uwzględnienia i sposób oceny zagrożeń, źródła informacji o podatności na zagrożenia, stosowane metodologie oceny ryzyka oraz założenia dotyczące ryzyka; (iii) wytyczne dotyczące reagowania na ryzyko, w tym na przykład tolerancje na ryzyko, koncepcje reagowania na ryzyko, które należy zastosować, koszty alternatywne, kompromisy, konsekwencje reakcji, hierarchia kompetencji i priorytety; (iv) wytyczne dotyczące monitorowania ryzyka, w tym na przykład wytyczne dotyczące analizy monitorowanych czynników ryzyka w celu określenia zmian w ryzyku oraz częstotliwość, metody i sprawozdawczość w zakresie monitorowania; (v) inne związane z ryzykiem ograniczenia dotyczące realizacji działań w zakresie zarządzania ryzykiem; oraz (vi) priorytety i kompromisy organizacyjne. Dane wyjściowe z etapu opracowywania ram ryzyka służą, jako dane wejściowe do etapów szacowania ryzyka, reagowania na ryzyko i monitorowania ryzyka.

3.2. OCENIANIE RYZYKA

Szacowanie ryzyka identyfikuje, hierarchizuje i wycenia ryzyko dla operacji organizacyjnych (tj. misji, funkcji, wizerunku i reputacji), aktywów organizacyjnych, osób, innych organizacji i Państwa, wynikające z działania i użytkowania systemów informatycznych[62]. Szacowanie ryzyka wykorzystuje wyniki oceny zagrożeń i podatności do identyfikacji i oceny ryzyka pod względem prawdopodobieństwa wystąpienia i potencjalnego negatywnego wpływu (tj. wielkości szkody) na organizacje, aktywa i osoby. Szacowanie ryzyka można przeprowadzić na każdym z poziomów zarządzania ryzykiem, przy czym cele i przydatność uzyskanych informacji mogą być różne. Na przykład, szacowanie ryzyka przeprowadzane na Poziomie 1 lub Poziomie 2 koncentruje się na operacjach organizacyjnych, aktywach i osobach - niezależnie od tego, czy jest ono kompleksowe dla całej misji/biznesu, czy też tylko na tych szacunkach, które są przekrojowe dla danej misji/biznesu. Ogólnoorganizacyjne szacowanie ryzyka może opierać się wyłącznie na założeniach, ograniczeniach, tolerancji ryzyka, priorytetach i kompromisach ustalonych na etapie określania ryzyka (wynikających głównie z działań na Poziomie 1) lub może opierać się na szacowaniu ryzyka przeprowadzanym na wielu misjach/liniach biznesowych (wynikających głównie z działań na Poziomie 2). Szacowanie ryzyka przeprowadzone na jednym poziomie może być wykorzystane do udoskonalenia/ulepszenia informacji o zagrożeniach, podatnościach, prawdopodobieństwie i wpływie, które są wykorzystywane w szacunkach przeprowadzanych na innych poziomach. Stopień, w jakim informacje z szacowania ryzyka mogą być ponownie wykorzystane, zależy od podobieństwa misji/funkcji biznesowych oraz stopnia autonomii jednostek organizacyjnych lub subkomponentów w stosunku do organizacji macierzystych. Organizacje zdecentralizowane mogą spodziewać się, że będą przeprowadzać więcej działań związanych z szacowaniem ryzyka na Poziomie 2 i w rezultacie mogą odczuwać większą potrzebę komunikacji w ramach Poziomu 2 w celu identyfikacji przekrojowych zagrożeń i podatności. Zdecentralizowane organizacje mogą nadal czerpać korzyści z przeprowadzania szacunków

[62] NSC 800-30, zawiera wytyczne dotyczące szacowania ryzyka na wszystkich trzech poziomach w ramach wielopoziomowego podejścia do zarządzania ryzykiem.

ryzyka na Poziomie 1, a w szczególności z identyfikacji wstępnego zestawu źródeł zagrożeń i podatności. Szacowanie ryzyka w całej organizacji zapewnia wstępną priorytetyzację ryzyka, którą decydenci mogą uwzględnić, przystępując do etapu reagowania na ryzyko.

Przeprowadzanie szacowania ryzyka, jako części procesu zarządzania ryzykiem w całej organizacji, przynosi organizacjom znaczne korzyści. Jednakże, gdy szacowanie ryzyka jest już zakończone, rozsądne jest, aby organizacje poświęciły odpowiednią ilość czasu na utrzymanie aktualności tych szacunków. Utrzymanie aktualności oszacowań ryzyka wymaga wsparcia ze strony etapu monitorowania ryzyka (np. obserwowania zmian w organizacyjnych systemach informatycznych i środowiskach działania lub analizowania wyników monitorowania w celu utrzymania świadomości ryzyka). Aktualizowanie szacunków ryzyka przynosi wiele potencjalnych korzyści, takich jak aktualne, istotne informacje, które umożliwiają liderom wyższego szczebla/kadrze kierowniczej zarządzanie ryzykiem w czasie zbliżonym do rzeczywistego. Aktualizowanie wyników szacowania ryzyka zmniejsza również przyszłe koszty szacowania i wspiera bieżące monitorowanie ryzyka. Organizacje mogą uznać, że przeprowadzanie kompleksowych szacunków ryzyka, jako sposób na utrzymanie bieżących szacunków ryzyka, nie zapewnia wystarczającej wartości. W takich sytuacjach organizacje rozważają przeprowadzenie przyrostowych i/lub różnicowych szacunków ryzyka. Przyrostowe szacowanie ryzyka uwzględnia tylko nowe informacje (np. wpływ zastosowania nowego systemu informatycznego na ryzyko związane z misją/biznesem), natomiast różnicowe szacowanie ryzyka uwzględnia wpływ zmian na całościowe określenie ryzyka. Przyrostowe lub różnicowe szacowanie ryzyka jest przydatne, gdy organizacje wymagają bardziej ukierunkowanego przeglądu ryzyka, poszukują szerszego zrozumienia ryzyka lub chcą lepiej zrozumieć ryzyko wynikające z misji/funkcji przedsiębiorstwa.

KROK 2: SZACOWANIE RYZYKA

Dane wejściowe i warunki wstępne

Dane wejściowe pochodzące z etapu opracowywania ram ryzyka przeznaczone do etapu szacowania ryzyka obejmują na przykład: (i) akceptowalne metodologie oceny ryzyka; (ii) zakres i szczegółowość analizy stosowanej podczas szacowania ryzyka; (iii) poziom ziarnistości wymagany do opisywania zagrożeń; (iv) kwestię, czy/jak oceniać zewnętrznych

dostawców usług; oraz (v) kwestię, czy/jak agregować uzyskane wyniki szacowania ryzyka z różnych jednostek organizacyjnych lub misji/funkcji biznesowych do organizacji, jako całości. Oczekiwania organizacyjne dotyczące metodologii, technik i/lub procedur szacowania ryzyka są w dużym stopniu kształtowane przez struktury zarządzania, tolerancję ryzyka, kulturę, zaufanie oraz procesy cyklu życia. Przed przeprowadzeniem szacowania ryzyka organizacje powinny poznać podstawowe powody, dla których przeprowadzają szacowanie, oraz zrozumieć, co stanowi odpowiednią szczegółowość i zakres tego szacowania. Założenia dotyczące ryzyka, ograniczenia ryzyka, tolerancja ryzyka oraz ustalone podczas etapu określania ryzyka priorytety/kompromisy kształtują sposób, w jaki organizacje wykorzystują szacunki ryzyka - na przykład lokalne zastosowania szacunków ryzyka w ramach każdego z poziomów zarządzania ryzykiem (tj. zarządzanie, misja/proces biznesowy, systemy informatyczne) lub globalne zastosowania szacunków ryzyka w całej organizacji. Szacowanie ryzyka może być przeprowadzane przez organizacje nawet wtedy, gdy niektóre dane wejściowe z etapu określania ryzyka nie zostały otrzymane lub nie zostały ustalone warunki wstępne. Jednak w takich sytuacjach może to mieć wpływ na jakość wyników szacowania ryzyka. Oprócz etapu określania ram ryzyka, etap szacowania ryzyka może uzyskiwać dane wejściowe z etapu monitorowania ryzyka, zwłaszcza w trakcie realizacji misji oraz w fazie eksploatacji/utrzymania cyklu życia systemu (np. gdy organizacje odkrywają nowe zagrożenia lub podatności na zagrożenia, które wymagają natychmiastowego ponownego oszacowania ryzyka). Etap szacowania ryzyka może również korzystać z danych wejściowych z etapu reagowania na ryzyko (np. gdy organizacje rozważają ryzyko zastosowania nowych rozwiązań technologicznych, jako alternatywy dla środków redukcji ryzyka). W miarę opracowywania kierunków działania na etapie reagowania na ryzyko, konieczne może być przeprowadzenie szacowania ryzyka różnicowego, aby ocenić różnice, jakie każdy kierunek działania wnosi do ogólnego określenia ryzyka.

Działania

IDENTYFIKACJA ZAGROŻEŃ I PODATNOŚCI NA ZAGROŻENIA

ZADANIE 2-1: Identyfikacja zagrożeń i podatności w systemach informatycznych organizacji oraz w środowiskach, w których te systemy funkcjonują.

Wskazówki uzupełniające: Identyfikacja zagrożeń wymaga zbadania źródeł i zdarzeń związanych z zagrożeniami. Badając źródła i zdarzenia zagrożeń, organizacje identyfikują możliwości, zamiary i informacje o celach zagrożeń ze wszystkich dostępnych źródeł. Organizacje mogą korzystać z wielu źródeł informacji o zagrożeniach na poziomie strategicznym lub taktycznym. Informacje o zagrożeniach wygenerowane na dowolnym poziomie mogą być wykorzystane do informowania lub udoskonalania działań związanych z ryzykiem na dowolnym innym poziomie. Na przykład konkretne zagrożenia (tj. taktyki, techniki i procedury) zidentyfikowane podczas oceny zagrożeń na Poziomie 1 mogą bezpośrednio wpływać na decyzje dotyczące misji/procesu biznesowego i projektu architektonicznego na Poziomie 2. Konkretne informacje o zagrożeniach wygenerowane na Poziomach 2 i 3 mogą być wykorzystywane przez organizacje do udoskonalania informacji o zagrożeniach wygenerowanych podczas wstępnych szacowań zagrożeń przeprowadzonych na Poziomie 1.

Identyfikacja podatności występuje na wszystkich poziomach. Podatności związane z zarządzaniem organizacyjnym (np. niespójne decyzje dotyczące względnych priorytetów misji/procesów biznesowych, wybór niekompatybilnych implementacji środków bezpieczeństwa), jak również podatności związane z zależnościami zewnętrznymi (np. energia elektryczna, łańcuch dostaw, telekomunikacja), są najskuteczniej identyfikowane na Poziomie 1. Jednakże, większość identyfikacji podatności ma miejsce na Poziomie 2 i 3. Na Poziomie 2, bardziej prawdopodobne jest zidentyfikowanie podatności związanych z procesami i architekturą (np. możliwe do wykorzystania słabości lub braki w procesach misji/biznesu, architekturach bezpieczeństwa korporacyjnego/informatycznego, w tym wbudowanych architekturach bezpieczeństwa informacji). Na Poziomie 3, głównym celem są podatności w systemach informatycznych. Luki te są powszechnie znajdowane w sprzęcie, oprogramowaniu i komponentach firmowych systemów informatycznych lub w środowiskach, w których systemy te działają. Inne obszary potencjalnych słabych punktów obejmują podatności związane z definiowaniem, stosowaniem/wdrażaniem i monitorowaniem procesów, procedur i usług związanych z zarządzaniem, operacyjnymi i technicznymi aspektami bezpieczeństwa informacji. Podatności związane z projektem

architektonicznym i procesami misji/biznesu mogą mieć większy wpływ na zdolność organizacji do skutecznego realizowania misji i funkcji biznesowych ze względu na potencjalny wpływ na wiele systemów informatycznych i środowisk misji. Dopracowane oceny podatności przeprowadzone na Poziomie 2 i 3 są udostępniane personelowi organizacyjnemu odpowiedzialnemu za strategiczne ocenianie ryzyka. Szacowanie podatności przeprowadzone na Poziomie 2 i Poziomie 3 mają możliwość oceny dodatkowych powiązanych zmiennych, takich jak lokalizacja, bliskość innych aktywów wysokiego ryzyka (fizycznych lub logicznych) oraz względy dotyczące zasobów związanych ze środowiskami operacyjnymi. Informacje specyficzne dla środowisk operacyjnych pozwalają na uzyskanie bardziej użytecznych i możliwych do wykorzystania wyników szacowania. Identyfikacja podatności może być przeprowadzona na poziomie indywidualnych słabości/braków lub na poziomie przyczyny źródłowej. Wybierając jedno z podejść, organizacje rozważają, czy ogólnym celem jest identyfikacja każdego konkretnego przypadku lub symptomu problemu, czy też zrozumienie podstawowych przyczyn problemów. Zrozumienie konkretnych możliwych do wykorzystania słabości lub niedociągnięć jest pomocne, gdy problemy są identyfikowane po raz pierwszy lub gdy wymagane są szybkie rozwiązania. To konkretne zrozumienie dostarcza również organizacjom niezbędnych źródeł informacji do ostatecznego zdiagnozowania potencjalnych pierwotnych przyczyn problemów, zwłaszcza tych problemów, które mają charakter systemowy.

Organizacje o bardziej ugruntowanych architekturach korporacyjnych (w tym wbudowanych architekturach bezpieczeństwa informacji) i rozwiniętych procesach cyklu życia mają wyniki, które mogą być wykorzystane w procesach szacowania ryzyka. Założenia dotyczące ryzyka, ograniczenia, tolerancje, priorytety i kompromisy stosowane przy opracowywaniu architektur korporacyjnych i wbudowanych architektur bezpieczeństwa informacji mogą być użytecznym źródłem informacji dla wstępnych działań związanych z szacowaniem ryzyka. Szacowanie ryzyka przeprowadzone w celu wsparcia rozwoju architektur segmentowych lub architektur rozwiązań może również służyć, jako źródło informacji do identyfikacji zagrożeń i podatności. Innym czynnikiem wpływającym na identyfikację zagrożeń i podatności jest kultura organizacyjna. Organizacje, które promują swobodną i otwartą komunikację oraz

brak odpłatności za dzielenie się informacjami o zagrożeniach, zazwyczaj wspierają otwartość ze strony osób pracujących w tych organizacjach. Często personel organizacyjny działający na Poziomie 2 i 3 posiada cenne informacje i może wnieść znaczący wkład w obszar identyfikacji zagrożeń i podatności. Kultura organizacji ma wpływ na gotowość personelu do przekazywania informacji o potencjalnych zagrożeniach i podatnościach, co ostatecznie wpływa na jakość i ilość zidentyfikowanych zagrożeń/podatności.

OKREŚLANIE RYZYKA

ZADANIE 2-2: Określenie ryzyka zagrażającego operacjom i aktywom organizacji, osobom, innym organizacjom i Państwu, jeśli rozpoznane zagrożenia wykorzystają rozpoznane podatności.

Wskazówki uzupełniające: Organizacje określają ryzyko, biorąc pod uwagę prawdopodobieństwo, że znane zagrożenia wykorzystają znane podatności oraz wynikające z tego konsekwencje lub negatywny wpływ (tj. wielkość szkody), jeśli takie wykorzystanie wystąpi. Organizacje wykorzystują informacje o zagrożeniach i podatnościach wraz z informacjami o prawdopodobieństwie i konsekwencjach/wpływach w celu jakościowego lub ilościowego określenia ryzyka. Organizacje mogą stosować różne podejścia do określania prawdopodobieństwa wystąpienia zagrożeń wykorzystujących podatności. Określenie prawdopodobieństwa może być oparte na założeniach dotyczących zagrożeń lub na informacjach o rzeczywistych zagrożeniach (np. dane historyczne dotyczące cyberataków, dane historyczne dotyczące trzęsień ziemi lub specyficzne informacje dotyczące możliwości, zamiarów i celów przeciwnika). Jeśli dostępne są precyzyjne i wiarygodne informacje o zagrożeniach (np. rodzaje cyberataków, trendy w zakresie cyberataków, częstotliwość ataków), organizacje mogą wykorzystać dane empiryczne i analizy statystyczne do określenia bardziej szczegółowych prawdopodobieństw wystąpienia zagrożeń. Na ocenę prawdopodobieństwa może mieć również wpływ to, czy identyfikacja podatności miała miejsce na poziomie pojedynczych słabości lub niedociągnięć, czy też na poziomie przyczyny źródłowej. Względna łatwość/trudność wykorzystania podatności, wyrafinowanie przeciwników oraz charakter środowisk operacyjnych mają wpływ na prawdopodobieństwo wykorzystania podatności przez zagrożenia. Organizacje mogą scharakteryzować negatywne

skutki według celów bezpieczeństwa (np. utrata poufności, integralności lub dostępności). Jednak, aby zmaksymalizować użyteczność, negatywny wpływ jest wyrażany lub przekładany na misje organizacji, funkcje biznesowe i interesariuszy.

Określanie ryzyka i niepewność

Określenie ryzyka wymaga analizy informacji związanych z zagrożeniem, podatnością, prawdopodobieństwem i wpływem. Organizacje muszą również zbadać podatności misji/biznesu oraz zagrożenia, w przypadku których nie istnieją zabezpieczenia i/lub środki zaradcze. Charakter danych wejściowych dostarczonych do tego etapu (np. ogólne, szczegółowe, strategiczne, taktyczne) bezpośrednio wpływa na rodzaj danych wyjściowych lub określanie ryzyka. Wiarygodność i dokładność określenia ryzyka zależy od aktualności, dokładności, kompletności i integralności informacji zebranych w celu wsparcia procesu szacowania ryzyka. Ponadto, składniki wyników szacowania ryzyka, które wpływają na wiarygodność i dokładność określania ryzyka, wpływają również na poziom niepewności związanej z tymi określeniami ryzyka i kolejnymi określeniami. Organizacje biorą również pod uwagę dodatkowe spostrzeżenia związane z przewidywanymi ramami czasowymi związanymi z poszczególnymi ryzykami. Horyzonty czasowe związane z potencjalnymi zagrożeniami mogą kształtować przyszłe reakcje na ryzyko (np. ryzyko może nie stanowić problemu, jeśli horyzont czasowy ryzyka jest w odległej przyszłości).

Wytyczne organizacyjne dotyczące określania ryzyka w warunkach istnienia niepewności wskazują, w jaki sposób kombinacje prawdopodobieństwa i wpływu są łączone w celu określenia poziomu ryzyka lub wyniku/oceny ryzyka. Organizacje muszą rozumieć rodzaj i wielkość niepewności towarzyszącej decyzjom dotyczącym ryzyka, aby określenie ryzyka było zrozumiałe. Podczas etapu określania ram ryzyka organizacje mogły dostarczyć wskazówek, jak analizować ryzyko i jak określać ryzyko, gdy istnieje wysoki stopień niepewności. Niepewność jest szczególnie istotna, gdy w szacowaniu ryzyka bierze się pod uwagę zaawansowane trwałe zagrożenia, w przypadku których może być potrzebna analiza współdziałających podatności, powszechna wiedza jest niewystarczająca, a wcześniejsze zachowania mogą nie być przewidywalne.

Chociaż określanie zagrożeń i podatności na zagrożenia ma często zastosowanie do misji i funkcji biznesowych, specyficzne wymogi związane z misjami/funkcjami biznesowymi, w tym środowiska działania, mogą prowadzić do różnych wyników szacowania. Różne misje, funkcje biznesowe i środowiska działania mogą prowadzić do różnic w możliwości zastosowania określonych informacji o zagrożeniach oraz prawdopodobieństwie wystąpienia zagrożeń powodujących potencjalne szkody. Zrozumienie elementu szacowania ryzyka związanego z zagrożeniami wymaga znajomości konkretnych zagrożeń, przed którymi stoją poszczególne misje lub funkcje biznesowe. Taka wiedza o zagrożeniach obejmuje zrozumienie możliwości, zamiarów i celów poszczególnych przeciwników. Tolerancja ryzyka organizacji oraz podstawowe przekonania związane z kształtowaniem się tolerancji ryzyka (w tym kultura wewnątrz organizacji) mogą wpływać na postrzeganie wpływu i prawdopodobieństwa w kontekście zidentyfikowanych zagrożeń i podatności.

Nawet po ustaleniu jednoznacznych kryteriów, szacowanie ryzyka jest uzależnione od kultury organizacyjnej oraz osobistych doświadczeń i zgromadzonej wiedzy osób przeprowadzających ocenę. W rezultacie osoby oceniające ryzyko mogą dojść do różnych wniosków na podstawie tych samych informacji. Ta różnorodność poglądów może prowadzić do udoskonalenia procesu szacowania ryzyka i zapewnić decydentom większy zakres informacji oraz potencjalnie mniejszą liczbę błędów. Jednakże takie zróżnicowanie może również prowadzić do niespójnych oszacowań ryzyka. Zdefiniowane i stosowane w organizacji procesy zapewniają środki do identyfikowania niespójnych praktyk oraz obejmują procesy identyfikowania i rozwiązywania takich niespójności.

Dane wyjściowe i warunki końcowe

Wynikiem etapu szacowania ryzyka jest określenie ryzyka dla operacji organizacyjnych (tj. misji, funkcji, wizerunku i reputacji), aktywów organizacyjnych, osób, innych organizacji oraz Państwa. W zależności od podejścia przyjętego przez organizacje, decydentom odpowiedzialnym za reakcję na ryzyko może być przekazywane albo ogólne ryzyko dla organizacji, albo dane wejściowe użyte do określenia ryzyka. W niektórych sytuacjach występują powtarzające się cykle pomiędzy etapem szacowania ryzyka, a etapem reakcji na ryzyko, aż do osiągnięcia określonych celów. W zależności od sposobu postępowania

wybranego na etapie reagowania na ryzyko, może wystąpić ryzyko szczątkowe. W pewnych okolicznościach poziom ryzyka szczątkowego może spowodować konieczność ponownego oszacowania ryzyka. Powtórne szacowanie ma zazwyczaj charakter przyrostowy (ocena tylko nowych informacji) i różnicowy (ocena, w jaki sposób nowe informacje zmieniają całościowe określenie ryzyka).

Agregacja wyników szacowania ryzyka ze wszystkich trzech poziomów stanowi podstawę zarządzania portfolio ryzyk podejmowanych przez organizacje. Zidentyfikowane ryzyka wspólne dla więcej niż jednej misji/funkcji biznesowej w organizacji mogą być również źródłem przyszłych działań szacunkowych na Poziomie 1, takich jak analiza przyczyn źródłowych. Lepsze zrozumienie powodów, dla których pewne rodzaje ryzyka są bardziej powszechne lub częstsze, pomaga osobom podejmującym decyzje w wyborze takich reakcji na ryzyko, które rozwiązują problemy leżące u podstaw (lub będące przyczyną źródłową), zamiast skupiać się wyłącznie na kwestiach powierzchniowych związanych z istnieniem ryzyka. Wyniki szacowania ryzyka mogą również wpływać na przyszłe decyzje projektowe i rozwojowe związane z architekturą korporacyjną (w tym wbudowaną architekturą bezpieczeństwa informacji) oraz organizacyjnymi systemami informatycznymi. Zakres, w jakim misje/funkcje biznesowe są podatne na szereg zidentyfikowanych zagrożeń oraz względna łatwość, z jaką te podatności mogą zostać wykorzystane, przyczyniają się do przekazywanych kierownictwu wyższego szczebla informacji związanych z ryzykiem.

Dane wyjściowe z etapu szacowania ryzyka mogą być użytecznymi danymi wejściowymi do etapów określania ram ryzyka i monitorowania ryzyka. Na przykład, określenie ryzyka może spowodować ponowne przeanalizowanie tolerancji organizacyjnej na ryzyko, ustalonej podczas etapu określania ryzyka. Organizacje mogą również zdecydować się na wykorzystanie informacji z etapu oceny ryzyka do wykorzystania w etapie monitorowania ryzyka. Na przykład, szacowanie ryzyka może zawierać zalecenia dotyczące monitorowania określonych elementów ryzyka (np. źródeł zagrożeń), tak, aby w przypadku przekroczenia określonych progów można było dokonać przeglądu i aktualizacji wcześniejszych wyników szacowania ryzyka, stosownie do sytuacji. Poszczególne progi ustalone w ramach programów monitorowania ryzyka mogą również służyć, jako podstawa do ponownego oszacowania

ryzyka. Jeśli w ramach etapu określania ram ryzyka organizacje ustanowią kryteria określające, kiedy wyniki szacowania ryzyka nie uzasadniają reakcji na ryzyko, wówczas wyniki szacowania mogą być przekazywane bezpośrednio do etapu monitorowania ryzyka, jako źródło danych wejściowych.

3.3. REAGOWANIE NA RYZYKO

Reagowanie na ryzyko identyfikuje, ocenia, decyduje i wdraża odpowiednie kierunki działania w celu zaakceptowania, uniknięcia, złagodzenia, dzielenia lub przeniesienia ryzyka dotyczącego operacji i aktywów organizacji, osób, innych organizacji i Państwa, wynikającego z działania i użytkowania systemów informatycznych. Identyfikacja i analiza alternatywnych kierunków działania[63] występuje zazwyczaj na Poziomie 1 lub Poziomie 2. Wynika to z faktu, że alternatywne kierunki działania (tj. potencjalne reakcje na ryzyko) są oceniane pod kątem przewidywanych skutków dla całej organizacji oraz zdolności organizacji do kontynuowania skutecznego wykonywania misji i funkcji biznesowych. Decyzje o zastosowaniu środków reagowania na ryzyko w całej organizacji są zazwyczaj podejmowane na Poziomie 1, chociaż decyzje te są oparte na informacjach związanych z ryzykiem pochodzących z innych poziomów. Na Poziomie 2 alternatywne kierunki działania są oceniane pod kątem przewidywanego wpływu na misje/funkcje biznesowe organizacji, związane z nimi misje/procesy biznesowe wspierające misje/funkcje biznesowe oraz wymagania dotyczące zasobów. Na Poziomie 3 alternatywne kierunki działania są zazwyczaj oceniane pod kątem cyklu życia systemu lub maksymalnego czasu dostępnego na wdrożenie wybranego kierunku (kierunków) działania. Zakres potencjalnych reakcji na ryzyko jest głównym czynnikiem decydującym o tym, czy dana czynność jest wykonywana na Poziomie 1, Poziomie 2 czy Poziomie 3. Na decyzje dotyczące ryzyka ma wpływ organizacyjna tolerancja ryzyka, opracowana w ramach działań związanych z określaniem ryzyka na Poziomie 1. Organizacje

[63] *Kierunek działania* jest rozłożoną w czasie lub zależną od sytuacji kombinacją środków reakcji na ryzyko. *Środek reakcji na ryzyko* to konkretne działanie podjęte w odpowiedzi na zidentyfikowane ryzyko. Środki reakcji na ryzyko mogą być zarządzane oddzielnie i mogą obejmować na przykład wdrożenie środków bezpieczeństwa w celu ograniczenia ryzyka, ogłoszenie polityk bezpieczeństwa w celu uniknięcia ryzyka lub zaakceptowania ryzyka w określonych okolicznościach oraz umowy organizacyjne w celu podziału lub przeniesienia ryzyka.

mogą wdrażać decyzje dotyczące ryzyka na każdym z poziomów zarządzania ryzykiem, kierując się różnymi celami i użytecznością uzyskanych informacji.

KROK 3: REAKCJA NA RYZYKO

Dane wejściowe i warunki wstępne

Dane wejściowe z etapów szacowania ryzyka i tworzenia ram ryzyka obejmują: (i) identyfikację źródeł zagrożeń i zdarzeń związanych z zagrożeniami; (ii) identyfikację podatności, które podlegają wykorzystaniu; (iii) szacunki potencjalnych konsekwencji i/lub wpływu, jeśli zagrożenia wykorzystują podatności; (iv) szacunki prawdopodobieństwa, że zagrożenia wykorzystują podatności; (v) określenie ryzyka dla operacji organizacyjnych (tj. misji, funkcji, wizerunku i reputacji), aktywów organizacyjnych, osób, innych organizacji i Państwa; (vi) wytyczne zawarte w strategii zarządzania ryzykiem organizacyjnym dotyczące reagowania na ryzyko (patrz Załącznik H); oraz (vii) ogólne kierunki i wytyczne organizacyjne dotyczące odpowiedniego reagowania na ryzyko. Oprócz etapów szacowania ryzyka i określania ram ryzyka, etap reagowania na ryzyko może otrzymywać dane wejściowe z etapu monitorowania ryzyka (np. gdy organizacje doświadczają naruszenia lub narażenia na szwank swoich systemów informatycznych lub środowisk operacyjnych, które wymagają natychmiastowej reakcji w celu rozwiązania problemu i ograniczenia dodatkowego ryzyka wynikającego z tego zdarzenia). Etap reagowania na ryzyko może również otrzymywać dane wejściowe z etapu określania ram ryzyka (np. gdy organizacje są zobowiązane do wdrożenia nowych zabezpieczeń i środków zaradczych w swoich systemach informatycznych na podstawie wymogów bezpieczeństwa zawartych w przepisach lub politykach organizacyjnych). Etap określania ram ryzyka bezpośrednio kształtuje również ograniczenia zasobów związane z wyborem odpowiedniego sposobu działania. Dodatkowe warunki wstępne ustalone na etapie określania ram ryzyka mogą obejmować: (i) ograniczenia oparte na architekturze i wcześniejszych inwestycjach; (ii) preferencje i tolerancje organizacyjne; (iii) oczekiwaną skuteczność w ograniczaniu ryzyka (w tym sposób pomiaru i monitorowania skuteczności); oraz (iv) horyzont czasowy ryzyka (np. ryzyko bieżące, ryzyko przewidywane - czyli ryzyko, którego pojawienia oczekuje się w przyszłości na podstawie wyników szacowania zagrożeń lub planowanych zmian w misjach/funkcjach biznesowych,

architekturze przedsiębiorstwa (w tym architekturze bezpieczeństwa informacji) lub aspektach zgodności prawnej lub regulacyjnej).

Działania

IDENTYFIKACJA REAKCJI NA RYZYKO

ZADANIE 3-1: Określenie alternatywnych sposobów działania w odpowiedzi na ryzyko określone podczas szacowania ryzyka.

Wskazówki uzupełniające: Organizacje mogą reagować na ryzyko na różne sposoby. Obejmują one: (i) akceptację ryzyka; (ii) unikanie ryzyka; (iii) ograniczanie ryzyka; (iv) współdzielenie ryzyka; (v) transfer ryzyka; lub (vi) kombinację powyższych. Przebieg działania to rozłożona w czasie lub zależna od sytuacji kombinacja środków reagowania na ryzyko. Na przykład, w sytuacji awaryjnej organizacja może zaakceptować ryzyko związane z niefiltrowanym połączeniem z zewnętrznym dostawcą usług komunikacyjnych przez określony czas; następnie uniknąć ryzyka poprzez przerwanie połączenia; ograniczyć ryzyko w najbliższym czasie poprzez zastosowanie środków bezpieczeństwa w celu wyszukania złośliwego oprogramowania lub dowodów nieautoryzowanego dostępu do informacji, które miały miejsce w okresie niefiltrowanego połączenia; i wreszcie ograniczyć ryzyko w dłuższym czasie poprzez zastosowanie zabezpieczeń, które zapewnią większe bezpieczeństwo takich połączeń.

Akceptacja ryzyka

Akceptacja ryzyka jest właściwą reakcją na ryzyko, gdy zidentyfikowane ryzyko mieści się w granicach organizacyjnej tolerancji ryzyka. Organizacje mogą zaakceptować ryzyko uznane za niskie, umiarkowane lub wysokie w zależności od konkretnych sytuacji lub warunków. Na przykład, organizacje posiadające centra danych w obszarach asejsmicznych mogą zaakceptować ryzyko trzęsienia ziemi na podstawie znanego prawdopodobieństwa wystąpienia trzęsienia ziemi i podatności centrum danych na uszkodzenia spowodowane trzęsieniem ziemi. Organizacje akceptują fakt, że trzęsienia ziemi są możliwe, ale biorąc pod uwagę rzadkość występowania dużych trzęsień ziemi w tym regionie kraju, uważają, że przeciwdziałanie takiemu ryzyku jest nieopłacalne - czyli organizacje uznały, że ryzyko

związane z trzęsieniami ziemi jest niskie. Z drugiej strony, organizacje mogą zaakceptować znacznie większe ryzyko (w zakresie umiarkowanym/wysokim) ze względu na istotne potrzeby misyjne, biznesowe lub operacyjne. Na przykład, organizacje mogą zdecydować się na udostępnienie bardzo wrażliwych informacji osobom udzielającym pierwszej pomocy, które zazwyczaj nie mają dostępu do takich informacji ze względu na konieczność powstrzymania zbliżających się ataków terrorystycznych w odpowiednim czasie, nawet, jeśli informacje te same w sobie nie są nietrwałe pod względem ryzyka utraty poufności. Organizacje zazwyczaj określają ogólny poziom dopuszczalnego ryzyka i rodzaje dopuszczalnego ryzyka z uwzględnieniem priorytetów organizacyjnych i kompromisów między (i) krótkoterminowymi potrzebami misji/biznesu i potencjalnymi długoterminowymi skutkami misji/biznesu; oraz (ii) interesami organizacyjnymi i potencjalnymi skutkami dla jednostek, innych organizacji i Państwa.

Unikanie ryzyka

Unikanie ryzyka może być właściwą reakcją na ryzyko, gdy zidentyfikowane ryzyko przekracza tolerancję organizacji na ryzyko. Organizacje mogą prowadzić pewne rodzaje działań lub stosować pewne rodzaje technologii informatycznych, które powodują powstanie ryzyka, które jest nie do zaakceptowania. W takich sytuacjach unikanie ryzyka polega na podejmowaniu określonych działań w celu wyeliminowania działań lub technologii, które są podstawą ryzyka, lub na zmianie lub umiejscowieniu tych działań lub technologii w misji organizacji/procesach biznesowych w celu uniknięcia potencjału nieakceptowalnego ryzyka. Na przykład, organizacje planujące wykorzystanie połączeń sieciowych pomiędzy dwoma obszarami mogą ustalić poprzez szacowanie ryzyka, że istnieje nieakceptowalne ryzyko związane z ustanowieniem takich połączeń. Organizacje mogą również stwierdzić, że wdrożenie skutecznych zabezpieczeń i środków zaradczych (np. rozwiązań międzydomenowych) nie jest praktyczne w danych okolicznościach. W związku z tym organizacje decydują się na uniknięcie ryzyka poprzez wyeliminowanie połączeń elektronicznych lub sieciowych i zastosowanie "luki powietrznej" z ręcznymi procesami łączenia (np. transfery danych za pomocą dodatkowych urządzeń pamięci masowej).

Ograniczanie ryzyka

Ograniczanie ryzyka lub jego redukcja to odpowiednia reakcja na ryzyko dla tej części ryzyka, której nie można zaakceptować, uniknąć, współdzielić lub przenieść. Alternatywne rozwiązania w zakresie ograniczania ryzyka zależą od: (i) szczebla zarządzania ryzykiem oraz zakresu decyzji dotyczących reakcji na ryzyko przypisanych lub delegowanych do personelu organizacyjnego na tym szczeblu (określonego przez struktury zarządzania organizacją); oraz (ii) strategii zarządzania ryzykiem organizacyjnym i powiązanych strategii reakcji na ryzyko. Środki stosowane przez organizacje w celu ograniczania ryzyka mogą obejmować kombinację środków reagowania na ryzyko na wszystkich trzech poziomach. Na przykład ograniczanie ryzyka może obejmować wspólne środki bezpieczeństwa na Poziomie 1, przeprojektowanie procesów na Poziomie 2 i/lub nowe lub udoskonalone zabezpieczenia lub środki zaradcze o charakterze zarządczym, operacyjnym lub technicznym (lub kombinację wszystkich trzech) na Poziomie 3. Inny przykład potencjalnego ryzyka wymagającego ograniczenia można zilustrować, gdy przeciwnicy uzyskują dostęp do urządzeń przenośnych (np. laptopów lub osobistych asystentów cyfrowych) podczas podróży użytkowników. Możliwe środki ograniczania ryzyka obejmują na przykład zasady organizacyjne zabraniające przewożenia urządzeń przenośnych do określonych obszarów świata lub procedury umożliwiające użytkownikom uzyskanie „czystego" urządzenia przenośnego, które nigdy nie będzie mogło łączyć się z sieciami organizacyjnymi.

Współdzielenie lub transfer ryzyka

Dzielenie się ryzykiem lub transfer ryzyka jest właściwą reakcją na ryzyko, gdy organizacje chcą i mają środki, aby przenieść odpowiedzialność za ryzyko na inne organizacje. Transfer ryzyka przenosi całą odpowiedzialność za ryzyko z jednej organizacji na inną (np. wykorzystanie ubezpieczenia do przeniesienia ryzyka z danej organizacji na firmę ubezpieczeniową). Podział ryzyka przenosi część odpowiedzialności za ryzyko na inne organizacje (zazwyczaj organizacje, które mają większe kwalifikacje do zajęcia się ryzykiem). Należy zauważyć, że transfer ryzyka nie zmniejsza ani prawdopodobieństwa wystąpienia szkodliwych zdarzeń, ani ich konsekwencji w postaci szkód dla działań i aktywów organizacji, osób, innych organizacji lub Państwa. Współdzielenie ryzyka może polegać na podziale

zobowiązań lub podziale odpowiedzialności za inne, adekwatne reakcje na ryzyko, takie jak łagodzenie skutków. Z tego względu koncepcja transferu ryzyka ma mniejsze zastosowanie w sektorze publicznym, niż w sektorze prywatnym, ponieważ odpowiedzialność organizacji jest zazwyczaj ustalana na podstawie przepisów lub polityki. W związku z tym samoczynne przeniesienie ryzyka przez organizacje sektora publicznego (np. poprzez zakup polisy ubezpieczenia) nie jest zazwyczaj możliwe. Podział ryzyka często ma miejsce, gdy organizacje stwierdzają, że zajęcie się ryzykiem wymaga wiedzy specjalistycznej lub zasobów, które są lepiej zabezpieczone przez inne organizacje. Na przykład, zidentyfikowane ryzyko może dotyczyć fizycznej penetracji granic i ataków kinetycznych ze strony grup terrorystycznych. Organizacja decyduje się na partnerstwo z inną organizacją dzielącą fizyczny obiekt, aby wziąć wspólną odpowiedzialność za przeciwdziałanie ryzyku związanemu z atakami kinetycznymi.

OCENA ROZWIĄZAŃ ALTERNATYWNYCH

ZADANIE 3-2: Ocenianie alternatywnych sposobów reagowania na ryzyko.

Wskazówki uzupełniające: Ocena alternatywnych kierunków działania może obejmować: (i) oczekiwaną skuteczność w osiąganiu pożądanej reakcji na ryzyko (oraz sposób mierzenia i monitorowania skuteczności); oraz (ii) przewidywaną wykonalność wdrożenia, w tym np. wpływ na misję/biznes, względy polityczne, prawne, społeczne, finansowe, techniczne i ekonomiczne. Względy ekonomiczne obejmują koszty ponoszone przez cały przewidywany okres realizacji danego sposobu działania (np. koszty zamówień, integracji z procesami organizacyjnymi na Poziomie 1 i/lub Poziomie 2, systemów informatycznych na Poziomie 3, szkoleń i utrzymania). Podczas oceny alternatywnych kierunków działania można dokonać wyraźnego kompromisu między krótkoterminowym zyskiem w zakresie skuteczności lub wydajności misji/biznesu, a długoterminowym ryzykiem wyrządzenia szkód misji/biznesowi w wyniku narażenia na kompromitację informacji lub systemów informatycznych, które zapewniają te krótkoterminowe korzyści. Na przykład, organizacje zaniepokojone możliwością narażenia na kompromitację urządzeń przenośnych (np. laptopów) podczas podróży pracowników mogą ocenić kilka sposobów działania, w tym (i) zapewnienie użytkownikom podróżującym do obszarów wysokiego ryzyka wyczyszczonych laptopów;

(ii) wymontowanie dysków twardych z laptopów i prowadzenie operacji z płyt CD lub DVD; lub (iii) poddanie laptopów szczegółowej ocenie przed zezwoleniem na połączenie z sieciami organizacyjnymi. Pierwsza opcja jest bardzo skuteczna, ponieważ laptopy zwrócone nigdy nie są podłączane do sieci organizacyjnych. Druga opcja zapewnia, że dyski twarde nie mogą zostać uszkodzone, ale nie jest tak skuteczna, ponieważ nadal istnieje możliwość, że urządzenia sprzętowe (np. płyty główne) mogły zostać naruszone. Skuteczność trzeciej opcji jest ograniczona przez zdolność organizacji do wykrywania potencjalnego wprowadzenia złośliwego oprogramowania do sprzętu, oprogramowania układowego lub aplikacji. W związku z tym jest to najmniej skuteczna z trzech opcji. Z punktu widzenia kosztów, pierwsza opcja jest potencjalnie najdroższa, w zależności od liczby osób podróżujących (a więc liczby wymaganych laptopów służbowych). Warianty drugi i trzeci są znacznie tańsze. Z punktu widzenia misji i działalności operacyjnej trzecia opcja jest najlepszym rozwiązaniem, ponieważ użytkownicy mają dostęp do standardowych konfiguracji laptopów, w tym wszystkich aplikacji i danych pomocniczych potrzebnych do wykonywania zadań wspierających misje i funkcje biznesowe. Takie aplikacje i dane nie byłyby dostępne w przypadku wyboru pierwszej lub drugiej opcji. Ostatecznie, oceny kierunków działania dokonuje się na podstawie wymogów operacyjnych, w tym wymogów bezpieczeństwa informacji, niezbędnych dla powodzenia misji/biznesu w krótkim i długim okresie. Ograniczenia budżetowe, spójność ze strategiami zarządzania inwestycjami, prawa obywatelskie i ochrona prywatności to niektóre z ważnych elementów, które organizacje biorą pod uwagę przy wyborze odpowiednich sposobów działania. W przypadkach, gdy organizacja określa tylko jeden kierunek działania, ocena koncentruje się na tym, czy kierunek ten jest odpowiedni. Jeśli sposób działania zostanie uznany za nieodpowiedni, wówczas organizacja musi udoskonalić zidentyfikowany sposób działania, aby wyeliminować niedociągnięcia, lub opracować inny sposób działania (patrz Zadanie 3-1). Podsumowując, dla każdego sposobu działania przeprowadzany jest bilans ryzyka i reakcji na ryzyko w celu dostarczenia informacji niezbędnych do: (i) wyboru między kierunkami działań; oraz (ii) oceny kierunków działań pod względem skuteczności reagowania, kosztów, wpływu na misję/biznes oraz wszelkich innych czynników uznanych za istotne dla organizacji. Część kompromisu między ryzykiem a reakcją na ryzyko uwzględnia kwestię konkurujących ze sobą

zasobów. Z perspektywy organizacyjnej oznacza to, że organizacje rozważają, czy koszt (np. środki finansowe, personel, czas) wdrożenia danego sposobu działania może potencjalnie negatywnie wpłynąć na inne misje lub funkcje biznesowe, a jeśli tak, to w jakim stopniu. Jest to konieczne, ponieważ organizacje mają ograniczone zasoby do wykorzystania i wiele konkurujących ze sobą misji/funkcji biznesowych w wielu elementach organizacyjnych. Dlatego też organizacje oceniają ogólną wartość alternatywnych kierunków działania w odniesieniu do misji/funkcji biznesowych oraz potencjalne ryzyko dla każdego elementu organizacyjnego. Organizacje mogą stwierdzić, że niezależnie od konkretnej misji/funkcji biznesowej i zasadności związanego z nią ryzyka, istnieją ważniejsze misje/funkcje biznesowe, które są narażone na większe ryzyko, a tym samym mają większe zapotrzebowanie na wykorzystanie ograniczonych zasobów.

REAKCJA NA RYZYKO

ZADANIE 3-3: Podjęcie decyzji w zakresie odpowiedniego sposobu reagowania na ryzyko.

Wskazówki uzupełniające: Decyzje dotyczące najwłaściwszego sposobu postępowania obejmują pewną formę ustalania priorytetów. Niektóre rodzaje ryzyka mogą budzić większe obawy niż inne. W takim przypadku konieczne może być przeznaczenie większych zasobów na zajęcie się ryzykami o wyższym priorytecie niż na inne ryzyka o niższym priorytecie. Nie musi to oznaczać, że ryzyka o niższym priorytecie nie zostaną uwzględnione. Może to raczej oznaczać, że na ryzyko o niższym priorytecie można przeznaczyć mniej zasobów (przynajmniej na początku) lub, że ryzyko o niższym priorytecie zostanie uwzględnione w późniejszym czasie. Kluczową częścią procesu podejmowania decyzji dotyczących ryzyka jest uznanie, że niezależnie od podjętych kroków, nadal istnieje pewien stopień ryzyka szczątkowego, którym należy się zająć. Organizacje określają akceptowalne stopnie ryzyka szczątkowego w oparciu o tolerancję ryzyka organizacyjnego oraz specyficzną tolerancję ryzyka poszczególnych osób podejmujących decyzje. Na proces decyzyjny mają wpływ niektóre z bardziej niewymiernych koncepcji związanych z ryzykiem (np. tolerancja ryzyka, zaufanie i kultura). Specyficzne poglądy i podejście, jakie organizacje przyjmują w odniesieniu do tych koncepcji związanych z ryzykiem, wpływają na kierunek działań wybranych przez osoby podejmujące decyzje.

WDROŻENIE OBSŁUGI RYZYKA

ZADANIE 3-4: Wdrożenie wybranego sposobu działania w odpowiedzi na ryzyko.

Wskazówki uzupełniające: Po wybraniu sposobu działania, organizacje wdrażają związaną z nim reakcję na ryzyko. Ze względu na wielkość i złożoność niektórych organizacji, faktyczne wdrożenie środków reagowania na ryzyko może stanowić wyzwanie. Niektóre środki reagowania na ryzyko mają charakter taktyczny (np. stosowanie łat na zidentyfikowane luki w systemach informatycznych organizacji) i mogą zostać wdrożone dość szybko. Inne środki reagowania na ryzyko mogą mieć charakter bardziej strategiczny i odzwierciedlać rozwiązania, których wdrożenie wymaga znacznie więcej czasu. Dlatego też organizacje stosują i dostosowują do konkretnego sposobu reagowania na ryzyko rozważania dotyczące wdrażania reakcji na ryzyko zawarte w strategiach reagowania na ryzyko (część strategii zarządzania ryzykiem opracowanej podczas etapu określania ryzyka). Patrz Załącznik H, Strategie reagowania na ryzyko.

Dane wyjściowe i warunki końcowe

Rezultatem etapu reagowania na ryzyko jest wdrożenie wybranych kierunków działania z uwzględnieniem: (i) osób lub elementów organizacyjnych odpowiedzialnych za wybrane środki reagowania na ryzyko oraz specyfikacji kryteriów skuteczności (tj. wyartykułowania wskaźników i progów, względem których można oceniać skuteczność środków reagowania na ryzyko); (ii) zależności każdego wybranego środka reagowania na ryzyko od innych środków reagowania na ryzyko; (iii) zależności wybranych środków reagowania na ryzyko od innych czynników (np. wdrożenie innych planowanych środków informatycznych); (iv) harmonogram wdrożenia środków reagowania na ryzyko; (v) plany monitorowania skuteczności środków reagowania na ryzyko; (vi) określenie wartości progowych monitorowania ryzyka; oraz (vii) implementacja, w stosownych przypadkach, doraźnych środków reagowania na ryzyko. Prowadzona jest również bieżąca komunikacja i współdzielenie się informacjami związanymi z ryzykiem z osobami lub elementami organizacyjnymi, na które reakcje na ryzyko mają wpływ (w tym potencjalne działania, które mogą być konieczne do podjęcia przez te osoby lub elementy organizacyjne).

W uzupełnieniu do etapu monitorowania ryzyka, dane wyjściowe z etapu reakcji na ryzyko mogą być użytecznym wkładem do etapów określania i szacowania ryzyka. Na przykład, możliwe jest, że analiza przeprowadzona podczas oceny alternatywnych kierunków działania może poddać w wątpliwość niektóre aspekty strategii reagowania na ryzyko, będącej częścią strategii zarządzania ryzykiem opracowanej podczas etapu określania ryzyka. W takich przypadkach organizacje wykorzystują te informacje, aby poinformować o etapie określania ram ryzyka i podjąć odpowiednie działania w celu ponownego przeanalizowania strategii zarządzania ryzykiem i związanej z nią strategii reagowania na ryzyko. Podczas oceny alternatywnych sposobów działania w odpowiedzi na ryzyko, organizacje mogą również stwierdzić, że niektóre aspekty szacowania ryzyka są niekompletne lub nieprawidłowe. Informacje te można wykorzystać w celu udoskonalenia etapu szacowania ryzyka, co może skutkować dalszą analizą lub ponownym oszacowaniem ryzyka.

3.4. MONITOROWANIE RYZYKA

Monitorowanie ryzyka zapewnia organizacjom środki do: (i) weryfikacji *zgodności*[64]; (ii) określania bieżącej *skuteczności środków* reagowania na ryzyko; oraz (iii) identyfikacji *zmian* wpływających na ryzyko w organizacyjnych systemach informatycznych i środowiskach działania. Analiza wyników monitorowania daje organizacjom możliwość utrzymania świadomości ponoszonego ryzyka, podkreślenia potrzeby ponownego przeanalizowania innych kroków w procesie zarządzania ryzykiem oraz jeśli zajdzie taka potrzeba, zainicjowania działań usprawniających proces[65]. Organizacje stosują narzędzia, techniki i procedury monitorowania ryzyka w celu zwiększenia świadomości ryzyka, pomagając liderom wyższego szczebla/kadrze kierowniczej w lepszym zrozumieniu bieżącego ryzyka dla operacji i aktywów organizacji, osób, innych organizacji oraz Państwa. Organizacje mogą wdrożyć monitorowanie ryzyka na każdym z poziomów zarządzania ryzykiem, kierując

[64] Weryfikacja zgodności zapewnia, że organizacje wdrożyły wymagane środki reagowania na ryzyko oraz, że spełnione zostały wymagania dotyczące bezpieczeństwa informacji wynikające z misji/funkcji biznesowych organizacji, ustawodawstwa, dyrektyw, rozporządzeń, polityk i norm/wytycznych.

[65] Publikacja NIST Special Publication 800-137 zawiera wytyczne dotyczące monitorowania organizacyjnych systemów informatycznych i środowisk działania.

się różnymi celami i użytecznością uzyskanych informacji. Na przykład, działania monitorujące na Poziomie 1 mogą obejmować bieżące oceny zagrożeń oraz to, jak zmiany w przestrzeni zagrożeń mogą wpływać na działania na Poziomie 2 i 3, w tym na architektury korporacyjne (z wbudowanymi architekturami bezpieczeństwa informacji) i organizacyjne systemy informatyczne. Działania monitorujące na Poziomie 2 mogą obejmować np. analizy nowych lub obecnych technologii, które są używane lub których użycie jest rozważane w przyszłości przez organizacje, w celu zidentyfikowania możliwych do wykorzystania słabości i/lub niedociągnięć w tych technologiach, które mogą wpłynąć na powodzenie misji/biznesu. Działania monitorujące Poziomu 3 koncentrują się na systemach informatycznych i mogą obejmować np. automatyczne monitorowanie standardowych ustawień konfiguracyjnych produktów informatycznych, skanowanie podatności oraz bieżące ocenianie środków bezpieczeństwa. Poza podjęciem decyzji o wyborze odpowiednich działań monitorujących na różnych poziomach zarządzania ryzykiem, organizacje decydują również o sposobie prowadzenia monitoringu (np. podejście automatyczne lub ręczne) oraz o częstotliwości działań monitorujących w oparciu np. o częstotliwość zmian wdrażania środków bezpieczeństwa, krytyczne pozycje w planach działania i etapach oraz tolerancję ryzyka.

KROK 4: MONITOROWANIE RYZYKA

Dane wejściowe i warunki wstępne

Dane wejściowe tego etapu obejmują strategie wdrażania wybranych kierunków działań w odpowiedzi na ryzyko oraz faktyczne wdrażanie wybranych kierunków działań. Oprócz etapu reagowania na ryzyko, etap monitorowania ryzyka może otrzymywać dane wejściowe z etapu określania ram ryzyka (np. gdy organizacje uzyskają informacje o zaawansowanym trwałym zagrożeniu odzwierciedlającym zmianę założeń dotyczących zagrożenia, może to spowodować zmianę częstotliwości dalszych działań monitorujących). Etap określania ram ryzyka bezpośrednio kształtuje również ograniczenia zasobów związane z ustanowieniem i wdrożeniem strategii monitorowania w całej organizacji. W niektórych przypadkach dane wyjściowe z etapu oceny ryzyka mogą być użytecznymi danymi wejściowymi do etapu monitorowania ryzyka. Na przykład, warunki progowe oszacowania ryzyka (np. prawdopodobieństwo wystąpienia zagrożeń wykorzystujących luki w zabezpieczeniach)

mogą zostać wprowadzone do etapu monitorowania ryzyka. Z kolei organizacje mogą prowadzić monitorowanie w celu określenia, czy takie warunki progowe są spełnione. Jeśli warunki progowe są spełnione, takie informacje mogą być wykorzystane w etapie oceny ryzyka, gdzie mogą służyć, jako podstawa do przyrostowej, różnicowej oceny ryzyka lub ogólnej ponownej oceny ryzyka organizacji.

Działania

STRATEGIA MONITOROWANIA RYZYKA

ZADANIE 4-1: Opracowanie strategii monitorowania ryzyka organizacji obejmuje cel, rodzaj i częstotliwość działań monitorujących.

Wytyczne uzupełniające: Organizacje wdrażają programy monitorowania ryzyka: (i) w celu sprawdzenia, czy wymagane środki reakcji na ryzyko są wdrażane oraz czy spełnione są wymogi bezpieczeństwa informacji wynikające z misji/funkcji biznesowych organizacji, ustawodawstwa, dyrektyw, rozporządzeń, polityk oraz norm/wytycznych i możliwe do prześledzenia (monitorowanie *zgodności)*; (ii) w celu określenia bieżącej skuteczności środków reakcji na ryzyko po ich wdrożeniu (*monitorowanie skuteczności*); oraz (iii) w celu zidentyfikowania zmian w organizacyjnych systemach informatycznych i środowiskach, w których systemy te działają, które mogą mieć wpływ na ryzyko (*monitorowanie zmian),* w tym zmian w zakresie wykonalności bieżącego wdrażania środków reakcji na ryzyko). Określenie celu programów monitorowania ryzyka ma bezpośredni wpływ na środki wykorzystywane przez organizacje do prowadzenia działań monitorujących oraz na to, gdzie odbywa się monitorowanie (tj. na których poziomach zarządzania ryzykiem). Organizacje określają również rodzaj stosowanego monitorowania, w tym podejścia, które opierają się na automatyzacji lub podejścia, które opierają się na działaniach proceduralnych/ręcznych z udziałem człowieka. Wreszcie, organizacje określają częstotliwość prowadzenia działań monitorujących, równoważąc wartość uzyskaną z częstego monitorowania z potencjalnymi zakłóceniami operacyjnymi wynikającymi np. z przerwania misji/procesów biznesowych, zmniejszenia przepustowości operacyjnej podczas monitorowania oraz przesunięcia zasobów z operacji na monitorowanie. Strategie monitorowania opracowane na Poziomie 1 wpływają i nadają kierunek podobnym strategiom opracowanym na Poziomie 2 i 3, w tym działaniom

monitorującym związanym z ramowymi zasadami zarządzania ryzykiem na poziomie systemu informatycznego.

Monitorowanie zgodności

Monitorowanie zgodności jest stosowane w celu zapewnienia, że organizacje wdrażają potrzebne środki reakcji na ryzyko. Obejmuje to zapewnienie, że środki reakcji na ryzyko wybrane i wdrożone przez organizacje, w odpowiedzi na ustalenia dotyczące ryzyka wynikające z szacowania ryzyka, są wdrożone prawidłowo i działają zgodnie z przeznaczeniem. Niewdrożenie wybranych przez organizacje środków reagowania na ryzyko może spowodować, że organizacje nadal będą podlegać zidentyfikowanemu ryzyku. Monitorowanie zgodności obejmuje również zapewnienie, że środki reakcji na ryzyko wynikające z ustawodawstwa, dyrektyw, polityk, regulacji, standardów lub zaleceń organizacyjnych (np. lokalne polityki, procedury, wymagania misji/biznesu) są wdrożone. Monitorowanie zgodności jest najłatwiejszym do przeprowadzenia rodzajem monitorowania, ponieważ zazwyczaj istnieje skończony zestaw środków reagowania na ryzyko, stosowanych przez organizacje zazwyczaj w formie zabezpieczeń. Takie środki są zazwyczaj dobrze zdefiniowane i wyrażone jako wynik etapu reakcji na ryzyko. Znacznie trudniejszą częścią monitorowania zgodności jest ocenienie, czy środki reagowania na ryzyko są wdrażane prawidłowo (a w niektórych przypadkach są wdrażane w sposób nieprzerwany). Monitorowanie zgodności obejmuje także, jeśli jest to wykonalne, analizę przyczyn braku zgodności. Przyczyny braku zgodności mogą być różne - począwszy od tego, że osoby nie wykonują prawidłowo swoich zadań, a skończywszy na tym, że środek reagowania na ryzyko nie działa zgodnie z przeznaczeniem. Jeśli monitorowanie wykaże brak zgodności, należy ponownie przeanalizować etap reagowania w procesie zarządzania ryzykiem. Kluczowym elementem informacji zwrotnej dla etapu reagowania, są ustalenia z monitoringu zgodności wskazujące na przyczynę braku zgodności. W niektórych przypadkach brak zgodności może być skorygowany poprzez ponowne wdrożenie tych samych środków reagowania na ryzyko z niewielkimi zmianami lub bez zmian. W innych jednak przypadkach błędy zgodności są bardziej skomplikowane (np. wybrane środki reagowania na ryzyko są zbyt trudne do wdrożenia lub nie działają zgodnie z oczekiwaniami). W takich przypadkach może być

konieczne, aby organizacje powróciły do części ewaluacyjnej i decyzyjnej etapu reagowania na ryzyko w celu opracowania innych środków reagowania na ryzyko.

Monitorowanie efektywności

Monitorowanie skuteczności jest stosowane przez organizacje w celu określenia, czy wdrożone środki reagowania na ryzyko rzeczywiście są skutecznym narzędziem redukcji zidentyfikowanego ryzyka do pożądanego poziomu. Mimo, że monitorowanie skuteczności różni się od monitorowania zgodności, nieosiągnięcie pożądanych poziomów skuteczności może wskazywać, że środki reagowania na ryzyko zostały wdrożone nieprawidłowo lub nie działają zgodnie z założeniami. Określenie skuteczności środków reagowania na ryzyko jest na ogół trudniejsze niż określenie, czy środki te zostały wdrożone prawidłowo i czy działają zgodnie z założeniami (tj. czy spełniają określone wymogi zgodności). Środki reagowania na ryzyko wdrożone prawidłowo i działające zgodnie z założeniami nie gwarantują skutecznego zmniejszenia ryzyka. Jest to spowodowane przede wszystkim przez: (i) złożoności środowisk operacyjnych, które mogą generować niezamierzone konsekwencje; (ii) późniejszych zmian poziomów ryzyka lub powiązanych czynników ryzyka (np. zagrożeń, podatności, wpływu lub prawdopodobieństwa); (iii) nieodpowiednich lub niekompletnych kryteriów ustanowionych jako wynik etapu reakcji na ryzyko; oraz (iv) zmian w systemach informatycznych i środowiskach operacyjnych po wdrożeniu środków reakcji na ryzyko. Jest to szczególnie istotne, gdy organizacje próbują określić, czy osiągnięto bardziej strategiczne wyniki oraz w przypadku bardziej dynamicznych środowisk operacyjnych. Na przykład, jeśli pożądanym rezultatem dla organizacji jest mniejsza podatność na zaawansowane trwałe zagrożenia, może to być trudne do zmierzenia, ponieważ tego typu zagrożenia są z definicji bardzo trudne do wykrycia. Nawet jeśli organizacje są w stanie określić kryteria skuteczności, często trudno jest uzyskać kryteria, które są wymierne. Dlatego ocena, czy wdrożone środki reagowania na ryzyko są ostatecznie skuteczne, może stać się kwestią subiektywnej oceny. Ponadto, nawet jeśli zostaną przedstawione wymierne kryteria skuteczności, może wystąpić trudność w ustaleniu, czy dostarczone informacje spełniają te kryteria. Jeśli organizacje stwierdzą, że środki reagowania na ryzyko nie są skuteczne, może być konieczne powrócenie do etapu reagowania na ryzyko. Ogólnie rzecz biorąc, w przypadku stwierdzenia braku

skuteczności organizacje nie mogą po prostu powrócić do części wdrożeniowej etapu reagowania na ryzyko. Dlatego też, w zależności od przyczyny braku skuteczności, organizacje ponownie analizują wszystkie części etapu reagowania na ryzyko (tj. rozwój, ocenę, decyzję i wdrożenie) oraz potencjalnie etap oceny ryzyka. W wyniku tych działań organizacje mogą opracować i wdrożyć zupełnie nowe reakcje na ryzyko.

Monitorowanie zmian

Oprócz monitorowania zgodności i skuteczności, organizacje monitorują zmiany w organizacyjnych systemach informatycznych i środowiskach, w których te systemy działają. Monitorowanie zmian w systemach informatycznych i środowiskach działania nie jest bezpośrednio związane z dotychczasowymi środkami reagowania na ryzyko, niemniej jednak jest ważne dla wykrywania zmian, które mogą wpływać na ryzyko dla działań i aktywów organizacji, osób, innych organizacji i Państwa. Ogólnie rzecz biorąc, monitorowanie takie pozwala wykryć zmiany warunków, które mogą podważyć założenia dotyczące ryzyka (sformułowane w etapie określania ryzyka) w:

- *Systemach informatycznych*. W systemach informatycznych organizacji (w tym w sprzęcie, oprogramowaniu i oprogramowaniu układowym) mogą wystąpić zmiany, które mogą wprowadzić nowe ryzyko lub zmienić istniejące. Na przykład, aktualizacje oprogramowania systemu operacyjnego mogą wyeliminować funkcje bezpieczeństwa, które istniały we wcześniejszych wersjach, wprowadzając w ten sposób nowe podatności na zagrożenia w organizacyjnych systemach informatycznych. Innym przykładem jest odkrycie nowych podatności systemu, które wykraczają poza zakres narzędzi i procesów dostępnych w celu ich wyeliminowania (np. podatności, dla których nie istnieją ustalone środki zaradcze).
- *Środowiskach operacyjnych*. Środowiska, w których działają systemy informatyczne, mogą również zmieniać się w sposób, który wprowadza nowe lub zmienia istniejące ryzyko. Do czynników środowiskowych i operacyjnych należą między innymi: misje/funkcje biznesowe, zagrożenia, podatności, procesy misyjne/biznesowe, obiekty, polityka, przepisy i technologie. Na przykład, mogą zostać wprowadzone nowe przepisy lub regulacje nakładające na organizacje dodatkowe wymagania.

Zmiana ta może wpłynąć na założenia dotyczące ryzyka ustalone przez organizacje. Innym przykładem jest zmiana w środowisku zagrożeń, która informuje o nowych taktykach, technikach, procedurach lub zwiększeniu możliwości technicznych przeciwników. Organizacje mogą doświadczyć zmniejszenia dostępnych zasobów (np. personelu lub funduszy), co z kolei może spowodować zmianę priorytetów. Organizacje mogą również doświadczyć zmian w strukturze własności dostawców zewnętrznych, co może wpłynąć na ryzyko związane z łańcuchem dostaw. Zmiany misji mogą wymagać od organizacji weryfikacji podstawowych założeń dotyczących ryzyka. Na przykład organizacja, której misją jest gromadzenie informacji o zagrożeniach związanych z możliwymi atakami terrorystycznymi na terenie kraju i przekazywanie tych informacji odpowiednim organom ścigania i służbom wywiadowczym, może zmienić zakres swojej działalności tak, aby stała się odpowiedzialna również za udostępnianie części informacji lokalnym służbom pierwszego kontaktu. Taka zmiana mogłaby wpłynąć na założenia dotyczące zasobów bezpieczeństwa, jakimi mogą dysponować tacy użytkownicy. Zmiany w technologii mogą również wpłynąć na założenia dotyczące ryzyka, które organizacje przyjęły za podstawę swoich działań. W przeciwieństwie do innych rodzajów zmian, zmiany technologiczne mogą być całkowicie niezależne od organizacji, ale mimo to wpływać na ryzyko, którym organizacje muszą się zająć. Na przykład, wzrost mocy obliczeniowej może podważyć założenia dotyczące tego, co stanowi wystarczająco silny sposób uwierzytelniania (np. liczba czynników uwierzytelniających) lub mechanizm kryptograficzny.

Monitorowanie automatyczne vs. ręczne

Ogólnie rzecz biorąc, organizacje mogą prowadzić monitorowanie zarówno metodami automatycznymi, jak i ręcznymi. Tam, gdzie jest to możliwe, należy stosować monitorowanie automatyczne, ponieważ jest ono szybsze, skuteczniejsze i bardziej opłacalne niż ręczne. Monitorowanie automatyczne jest też mniej podatne na błędy ludzkie. Nie we wszystkich rodzajach monitorowania można jednak korzystać z automatyzacji. Monitorowanie prowadzone na Poziomie 3 generalnie nadaje się do automatyzacji, gdy monitorowane

aktywności mają charakter informatyczny. Takie działania można zwykle wykrywać, śledzić i monitorować poprzez instalację odpowiednich aplikacji, sprzętu komputerowego i/lub oprogramowania układowego. W celu zapewnienia, że zautomatyzowane procesy, procedury i/lub mechanizmy wspierające działania monitorujące dostarczają potrzebnych informacji, takie procesy, procedury i mechanizmy powinny być odpowiednio weryfikowane, aktualizowane i monitorowane. Monitorowanie zgodności może być wspierane przez automatyzację, gdy środki ograniczania ryzyka poddawane weryfikacji są oparte na technologii informacyjnej (np. instalacja zapór ogniowych lub testowanie ustawień konfiguracyjnych na komputerach stacjonarnych). Taka zautomatyzowana weryfikacja może często obejmować sprawdzenie, czy środki ograniczające ryzyko zostały zainstalowane i czy instalacje te są prawidłowe. Również monitorowanie skuteczności może być wspomagane przez automatyzację. Jeśli warunki progowe dla określenia skuteczności środków reagowania na ryzyko są z góry określone, to automatyzacja może wspierać takie monitorowanie skuteczności. Choć automatyzacja może stanowić wsparcie dla Poziomu 1 i 2, na ogół nie zapewnia ona istotnego wglądu w działania nieoparte na technologiach informacyjnych, które są bardziej rozpowszechnione na wyższych poziomach. Czynności, które prawdopodobnie nie wykorzystają automatyzacji, to na przykład korzystanie z usług wielu dostawców w ramach łańcucha dostaw, zmieniające się środowiska operacyjne lub ocena możliwości nowych technologii wspierających misje/funkcje biznesowe. Tam, gdzie zautomatyzowane monitorowanie nie jest dostępne, organizacje stosują ręczne monitorowanie i/lub analizę.

Częstotliwość monitorowania

Częstotliwość monitorowania ryzyka (automatycznego lub ręcznego) jest uzależniona od misji/funkcji biznesowych organizacji oraz od zdolności organizacji do wykorzystania wyników monitorowania w celu zwiększenia świadomości sytuacyjnej. Zwiększony poziom świadomości sytuacyjnej w zakresie stanu bezpieczeństwa systemów informatycznych i środowisk działania pomaga organizacjom lepiej zrozumieć ryzyko. Częstotliwość monitorowania zależy również od innych czynników, na przykład: (i) przewidywanej częstotliwości zmian w organizacyjnych systemach informatycznych i środowiskach działania;

(ii) potencjalnego wpływu ryzyka, jeśli nie zostanie ono właściwie zaadresowane poprzez odpowiednie środki reagowania; oraz (iii) stopnia, w jakim zmienia się przestrzeń zagrożeń. Na częstotliwość monitorowania może mieć również wpływ rodzaj prowadzonego monitorowania (tj. podejście zautomatyzowane versus proceduralne). W zależności od częstotliwości wymaganego przez organizację monitorowania, w większości sytuacji najbardziej efektywne i opłacalne jest stosowanie automatyzacji. Monitorowanie może przynieść znaczące korzyści, szczególnie w sytuacjach, gdy ogranicza ono możliwości zdobycia przez przeciwników dostępu do organizacji (poprzez systemy informatyczne lub środowiska, w których te systemy działają). Jeżeli organizacja stosuje ręczne monitorowanie, na ogół nie jest efektywne wykonywanie go z taką częstotliwością, na jaką pozwala automatyzacja. W niektórych przypadkach, rzadkie monitorowanie nie stanowi istotnego problemu. Na przykład, misje/funkcje biznesowe, obiekty, przepisy prawne, polityka i technologie zmieniają się stopniowo i jako takie nie wymagają częstego monitorowania. Zamiast tego, zmiany tego typu lepiej nadają się do monitorowania opartego na warunkach/zdarzeniach (np. jeśli misje i/lub funkcje biznesowe ulegają zmianie, należy monitorować takie zmiany, aby określić, czy mają one wpływ na ryzyko).

MONITOROWANIE RYZYKA

ZADANIE 4-2: Monitorowanie na bieżąco systemów informatycznych i środowisk działania organizacji w celu weryfikacji zgodności, określenia skuteczności środków reagowania na ryzyko oraz identyfikacji zmian.

Wskazówki uzupełniające: Opracowane przez organizację strategie monitorowania są wdrażane w całej organizacji. Ponieważ istnieje tak wiele różnych aspektów monitorowania, nie wszystkie z nich mogą być wykonywane lub mogą być wykonywane w różnym czasie. Poszczególne aspekty monitoringu, które są wykonywane, zależą w dużej mierze od założeń, ograniczeń, tolerancji ryzyka i priorytetów/wyborów ustalonych przez organizacje na etapie określania ryzyka. Na przykład, podczas gdy organizacje mogą chcieć prowadzić wszystkie formy monitorowania (tj. zgodności, skuteczności i zmiany), narzucone im ograniczenia mogą pozwalać tylko na monitorowanie zgodności, które można łatwo zautomatyzować na Poziomie 3. Jeśli można wspierać wiele aspektów monitorowania, dane wyjściowe z etapu

tworzenia ram ryzyka pomagają organizacjom określić stopień ważności i poziom wysiłku, jaki należy włożyć w różne działania monitorujące.

Jak zauważono powyżej, nie wszystkie działania monitorujące są prowadzone na tych samych poziomach, w tym samym celu, w tym samym czasie lub przy użyciu tych samych technik. Ważne jest jednak, by organizacje starały się koordynować różne działania monitorujące. Koordynacja działań monitorujących ułatwia dzielenie się informacjami związanymi z ryzykiem, które mogą być użyteczne dla organizacji w zakresie wczesnego ostrzegania, opracowywania informacji o trendach oraz terminowego i skutecznego przydzielania środków reagowania na ryzyko. Jeśli monitorowanie nie jest skoordynowane, korzyści z niego płynące mogą być mniejsze, co może osłabić całościowe wysiłki na rzecz identyfikacji i przeciwdziałania ryzyku. Jeśli to możliwe, organizacje wdrażają różne działania monitorujące w taki sposób, aby zmaksymalizować ogólny cel monitorowania, wychodząc poza ograniczone cele poszczególnych działań monitorujących. Wyniki monitorowania ryzyka są wykorzystywane podczas przeprowadzania przyrostowych ocen ryzyka w celu utrzymania świadomości ponoszonego ryzyka, podkreślenia zmian w ryzyku oraz wskazania potrzeby ponownego przeanalizowania kolejnych etapów procesu zarządzania ryzykiem, jeśli jest to właściwe.

Dane wyjściowe i warunki końcowe

Wynikiem etapu monitorowania ryzyka są informacje uzyskiwane poprzez: (i) weryfikację, czy wymagane środki reagowania na ryzyko są wdrażane oraz czy spełnione i możliwe do prześledzenia są wymagania dotyczące bezpieczeństwa informacji wynikające z misji/funkcji biznesowych organizacji, przepisów prawnych, dyrektyw, rozporządzeń, polityk oraz norm/wytycznych; (ii) określanie bieżącej skuteczności środków reagowania na ryzyko; oraz (iii) identyfikowanie zmian w organizacyjnych systemach informatycznych i środowiskach działania. Dane wyjściowe z etapu monitorowania ryzyka mogą być użytecznymi danymi wejściowymi do etapów określania ryzyka, szacowania ryzyka i reagowania na ryzyko. Na przykład, wyniki monitorowania zgodności mogą wymagać od organizacji ponownego przeanalizowania części wdrożeniowej kroku reagowania na ryzyko, natomiast wyniki monitorowania skuteczności mogą wymagać od organizacji ponownego przeanalizowania

całego kroku reagowania na ryzyko. Wyniki monitorowania zmian w systemach informatycznych i środowiskach działania mogą wymagać od organizacji ponownego przeanalizowania etapu oceny ryzyka. Wyniki etapu monitorowania ryzyka mogą również posłużyć do określenia ram ryzyka (np. gdy organizacje odkryją nowe zagrożenia lub podatności na zagrożenia, które wpływają na zmianę założeń organizacyjnych dotyczących ryzyka, tolerancji ryzyka i/lub priorytetów/wyborów).

ZAŁĄCZNIK A REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych – na podstawie FIPS 200
NSC 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych – na podstawie NIST SP 800- 18
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53B

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informatycznego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61

LAWS, POLICIES, DIRECTIVES, INSTRUCTIONS, STANDARDS, AND GUIDELINES

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

POLICIES, DIRECTIVES, INSTRUCTIONS

1. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance (IA) Glossary*, April 2010.
2. Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, October 2009.
3. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

STANDARDS

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
3. ISO/IEC 15408:2005, *Common Criteria for Information Technology Security Evaluation*, 2005.

GUIDELINES

1. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
2. Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, (Projected Publication Spring 2011).

3. National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.
4. National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.
5. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010.
6. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
7. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
8. National Institute of Standards and Technology Special Publication 800-70, Revision 1, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, September 2009.
9. National Institute of Standards and Technology Special Publication 800-137, Initial Public Draft, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, December 2010.

ZAŁĄCZNIK B SŁOWNIK

PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA

ZAŁĄCZNIK C AKRONIMY

PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA

ZAŁĄCZNIK D ROLE I OBOWIĄZKI

KLUCZOWI UCZESTNICY PROCESU ZARZĄDZANIA RYZYKIEM

Role i obowiązki kluczowych uczestników zaangażowanych w proces zarządzania ryzykiem w organizacji wynikają z Ram Zarządzania Ryzykiem zawartymi w publikacji NSC 800-37[66, 67]. Biorąc pod uwagę, że organizacje mają bardzo różne misje i struktury organizacyjne, mogą występować różnice w nazewnictwie ról związanych z zarządzaniem ryzykiem oraz w sposobie przydzielania konkretnych obowiązków pracownikom organizacji (np. wiele osób pełniących jedną rolę lub jedna osoba pełniąca wiele ról)[68]. Podstawowe funkcje pozostają jednak niezmienne. Zastosowanie procesu zarządzania ryzykiem na trzech poziomach zarządzania ryzykiem opisanych w niniejszej publikacji jest elastyczne, co pozwala organizacjom skutecznie realizować cele poszczególnych zadań w ramach ich struktur organizacyjnych, aby jak najlepiej zarządzać ryzykiem.

[66] Opis ról i obowiązków – patrz publikacje: NSC 800-37, *Załącznik D*; oraz NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.*

[67] Organizacje mogą zdefiniować inne role (np. kierownik obiektów, kierownik ds. zasobów ludzkich, administrator systemów) w celu wsparcia procesu zarządzania ryzykiem.

[68] Należy zachować szczególną ostrożność, gdy jedna osoba pełni wiele ról w procesie zarządzania ryzykiem, aby zapewnić, że osoba ta zachowa odpowiedni poziom niezależności i pozostanie wolna od konfliktu interesów.

ZAŁĄCZNIK E ZADANIA PROCESU ZARZĄDZANIA RYZYKIEM

ZESTAWIENIE ZADAŃ W POSZCZEGÓLNYCH ETAPACH PROCESU ZARZĄDZANIA RYZYKIEM

ZADANIE	OPIS ZADANIA
Krok 1: Określenie ram ryzyka	
ZADANIE 1-1 ZAŁOŻENIA DOTYCZĄCE RYZYKA	Określenie założeń, które mają wpływ na sposób szacowania, reagowania i monitorowania ryzyka w organizacji.
ZADANIE 1-2 OGRANICZANIE RYZYKA	Identyfikacja ograniczeń w prowadzeniu działań związanych z szacowaniem ryzyka, reagowaniem na ryzyko i monitorowaniem ryzyka w organizacji.
ZADANIE 1-3 TOLERANCJA RYZYKA	Określenie poziomu tolerancji ryzyka organizacji.
ZADANIE 1-4 PRIORYTETY I KOMPROMISY	Ustalenie priorytetów i kompromisów w zarządzaniu ryzykiem.
Krok 2: Szacowanie ryzyka	
ZADANIE 2-1 IDENTYFIKACJA ZAGROŻEŃ I PODATNOŚCI	Identyfikacja zagrożeń i podatności w systemach informatycznych organizacji oraz w środowiskach, w których te systemy funkcjonują.

ZADANIE	OPIS ZADANIA
ZADANIE 2-2 OKREŚLANIE RYZYKA	Określenie ryzyka zagrażającego operacjom i aktywom organizacji, osobom, innym organizacjom i Państwu, jeśli rozpoznane zagrożenia wykorzystają rozpoznane podatności.
Krok 3: Reakcja na ryzyko	
ZADANIE 3-1 IDENTYFIKACJA REAKCJI NA RYZYKO	Określenie alternatywnych sposobów działania w odpowiedzi na ryzyko określone podczas szacowania ryzyka.
ZADANIE 3-2 OCENA ROZWIĄZAŃ ALTERNATYWNYCH	Ocenianie alternatywnych sposobów reagowania na ryzyko.
ZADANIE 3-3 REAKCJA NA RYZYKO	Podjęcie decyzji w zakresie odpowiedniego sposobu reagowania na ryzyko.
ZADANIE 3-4 WDROŻENIE OBSŁUGI RYZYKA	Wdrożenie wybranego sposobu działania w odpowiedzi na ryzyko.
Krok 4: Monitorowanie ryzyka	
ZADANIE 4-1	Opracowanie strategii monitorowania ryzyka organizacji obejmującej cel, rodzaj i częstotliwość działań monitorujących.

ZADANIE	OPIS ZADANIA
STRATEGIA MONITOROWANIA RYZYKA	
ZADANIE 4-2 MONITOROWANIE RYZYKA	Monitorowanie na bieżąco systemów informatycznych i środowisk działania organizacji w celu weryfikacji zgodności, określenia skuteczności środków reagowania na ryzyko oraz identyfikacji zmian.

ZAŁĄCZNIK F MODELE ZARZĄDZANIA

PODEJŚCIA DO ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

W celu zaspokojenia potrzeb organizacji można zastosować trzy podejścia do zarządzania bezpieczeństwem informacji: (i) *scentralizowane*; (ii) *zdecentralizowane*; lub (iii) podejście *hybrydowe*.

Uprawnienia, odpowiedzialność i kompetencje decyzyjne związane z bezpieczeństwem informacji i zarządzaniem ryzykiem różnią się w każdym podejściu do zarządzania. Odpowiednia dla danej organizacji struktura zarządzania zależy od wielu czynników (np. od misji/potrzeb biznesowych, kultury i wielkości organizacji, geograficznego rozproszenia operacji organizacyjnych, aktywów i osób oraz tolerancji ryzyka). Struktura zarządzania bezpieczeństwem informacji jest dostosowywana do innych struktur zarządzania (np. zarządzania technologią informacyjną) w celu zapewnienia zgodności z ustalonymi praktykami zarządzania w organizacji oraz zwiększenia jej ogólnej skuteczności.

Zarządzanie scentralizowane

W scentralizowanych strukturach zarządzania uprawnienia, odpowiedzialność i moc decyzyjna spoczywają wyłącznie na organach centralnych. Te scentralizowane organy ustanawiają odpowiednie polityki, procedury i procesy zapewniające zaangażowanie całej organizacji w rozwój i wdrażanie strategii zarządzania ryzykiem i bezpieczeństwem informacji, podejmowanie decyzji dotyczących ryzyka i bezpieczeństwa informacji oraz tworzenie mechanizmów komunikacji międzyorganizacyjnej i wewnątrzorganizacyjnej. Scentralizowane podejście do zarządzania wymaga sprawnego, dobrze przygotowanego i kompetentnego kierownictwa na szczeblu centralnym oraz zapewnia spójność w całej organizacji. Scentralizowane struktury zarządzania zapewniają także mniejszą autonomię podległych organizacji, będących częścią organizacji macierzystej.

Zarządzanie zdecentralizowane

W zdecentralizowanych strukturach zarządzania bezpieczeństwem informacji uprawnienia, odpowiedzialność i moc decyzyjna są nadawane i przekazywane poszczególnym organizacjom podległym w ramach organizacji macierzystej (np. biurom/komórkom

w ramach departamentu lub jednostkom biznesowym w ramach korporacji). Podległe organizacje ustalają własne zasady, procedury i procesy zapewniające zaangażowanie w rozwój i wdrażanie strategii zarządzania ryzykiem i bezpieczeństwem informacji, podejmowanie decyzji dotyczących ryzyka i bezpieczeństwa informacji oraz tworzenie mechanizmów komunikacji wewnątrz organizacji. Zdecentralizowane podejście do zarządzania bezpieczeństwem informacji uwzględnia podległe organizacje o rozbieżnych misjach/potrzebach biznesowych i środowiskach operacyjnych w kosztach utrzymania spójności w całej organizacji. Skuteczność tego podejścia znacznie zwiększa dzielenie się informacjami związanymi z ryzykiem pomiędzy podległymi organizacjami tak, aby żadna z nich nie mogła przenieść ryzyka na inną bez świadomej zgody tej ostatniej. Ważne jest także dzielenie się informacjami o ryzyku z organizacjami macierzystymi, ponieważ decyzje dotyczące ryzyka podejmowane przez podległe organizacje mogą mieć wpływ na całą organizację.

Zarządzanie hybrydowe

W hybrydowych strukturach zarządzania bezpieczeństwem informacji uprawnienia, odpowiedzialność i moc decyzyjna są rozdzielone między organ centralny i poszczególne podległe organizacje. Organ centralny ustanawia zasady, procedury i procesy zapewniające zaangażowanie całej organizacji w część strategii zarządzania ryzykiem i bezpieczeństwem informacji oraz w decyzje dotyczące całej organizacji (np. decyzje związane ze wspólną infrastrukturą lub wspólnymi usługami bezpieczeństwa). Organizacje podległe, w podobny sposób, ustanawiają odpowiednie polityki, procedury i procesy zapewniające ich zaangażowanie w tę część strategii i decyzji dotyczących zarządzania ryzykiem i bezpieczeństwem informacji, które są specyficzne dla ich misji/potrzeb biznesowych i środowiska działania. Hybrydowe podejście do zarządzania wymaga silnego, dobrze poinformowanego kierowania organizacją jako całością oraz organizacjami podległymi, a także zapewnia spójność w całej organizacji w zakresie tych aspektów ryzyka i bezpieczeństwa informacji, które dotyczą całej organizacji.

ZAŁĄCZNIK G MODELE ZAUFANIA

JAK NAWIĄZAĆ RELACJE OPARTE NA ZAUFANIU

Poniższe modele zaufania opisują sposoby, za pomocą których organizacje mogą uzyskać poziom zaufania niezbędny do tworzenia partnerstw, współpracy z innymi organizacjami, wymiany informacji lub korzystania z usług systemów informatycznych/usług bezpieczeństwa. Żaden pojedynczy model zaufania nie jest z natury lepszy od innego. Przeciwnie, każdy model dostarcza organizacjom pewnych zalet i wad w zależności od okoliczności (np. struktury zarządzania, tolerancji ryzyka oraz krytyczności/wrażliwości misji organizacji i procesów biznesowych).

Model potwierdzonego zaufania

W modelu potwierdzonego zaufania (*ang. validated trust model*) jedna organizacja uzyskuje dowody dotyczące działań innej organizacji (np. jej polityki bezpieczeństwa informacji, działań i decyzji związanych z ryzykiem) i wykorzystuje te dowody do ustanowienia poziomu zaufania do tej drugiej organizacji. Przykładem potwierdzonego zaufania jest sytuacja, w której jedna organizacja opracowuje aplikację lub system informatyczny i dostarcza drugiej organizacji dowody (np. plan bezpieczeństwa, wyniki szacowania), które potwierdzają twierdzenia pierwszej organizacji, że aplikacja/system spełnia określone wymagania dotyczące bezpieczeństwa i/lub uwzględnia odpowiednie środki bezpieczeństwa określone w standardzie NSC 800-53. Potwierdzone zaufanie może nie być wystarczające - to znaczy, dowody oferowane przez pierwszą organizację drugiej organizacji mogą nie spełniać w pełni wymagań lub oczekiwań zaufania drugiej organizacji. Im więcej dowodów dostarczonych pomiędzy organizacjami, jak również jakość tych dowodów, tym większy stopień zaufania można osiągnąć. Zaufanie jest powiązane ze stopniem przejrzystości pomiędzy dwoma organizacjami w odniesieniu do działań i decyzji związanych z ryzykiem i bezpieczeństwem informacji.

Model historycznego zaufania bezpośredniego

W modelu historycznego zaufania bezpośredniego (*ang. direct historical trust model*) osiągnięcia organizacji w przeszłości, w szczególności w zakresie działań i decyzji związanych

z ryzykiem i bezpieczeństwem informacji, mogą przyczynić się do ustanowienia poziomu zaufania w stosunku do innych organizacji i pomóc w jego ustanowieniu. Podczas, gdy modele potwierdzonego zaufania zakładają, że organizacja dostarcza wymagany poziom dowodów potrzebnych do ustanowienia zaufania, uzyskanie takich dowodów nie zawsze jest możliwe. W takich przypadkach zaufanie może być oparte na innych czynnikach decyzyjnych, w tym na historycznych relacjach organizacji z inną organizacją lub na jej niedawnym doświadczeniu we współpracy z tą organizacją. Na przykład, jeśli jedna organizacja od lat współpracuje z drugą organizacją przy realizacji jakiegoś działania i nie miała żadnych negatywnych doświadczeń, pierwsza organizacja może być skłonna zaufać drugiej organizacji przy pracy nad innym działaniem, nawet, jeśli organizacje nie mają wspólnych doświadczeń w tym konkretnym działaniu. Bezpośrednie zaufanie historyczne ma tendencję do zwiększania się w czasie, a pozytywne doświadczenia przyczyniają się do wzrostu poziomu zaufania między organizacjami. I odwrotnie, negatywne doświadczenia mogą powodować spadek poziomu zaufania między organizacjami.

Model zaufania mediacyjnego

W modelu zaufania mediacyjnego (*ang. mediated trust model*) organizacja ustanawia poziom zaufania z inną organizacją na podstawie zapewnień dostarczonych przez wzajemnie zaufaną stronę trzecią. Istnieje kilka rodzajów modeli zaufania mediacyjnego, które mogą być zastosowane. Na przykład, dwie organizacje próbujące nawiązać relację zaufania mogą nie mieć bezpośredniej historii zaufania pomiędzy tymi dwiema organizacjami, ale mają relację zaufania z trzecią organizacją. Ta trzecia strona, która posiada zaufanie obu organizacji, pośredniczy w relacji zaufania pomiędzy dwoma organizacjami, pomagając w ten sposób w ustanowieniu wymaganego poziomu zaufania. Innym rodzajem zaufania mediacyjnego jest koncepcja przechodniości zaufania. Inny rodzaj zaufania mediacyjnego wiąże się z pojęciem przechodniości zaufania. W tym przykładzie, pierwsza organizacja nawiązuje relację zaufania z drugą organizacją. Niezależnie od tej relacji zaufania, druga organizacja nawiązuje relację zaufania z trzecią organizacją. Ponieważ pierwsza organizacja ufa drugiej organizacji, a druga

organizacja ufa trzeciej organizacji, relacja zaufania została nawiązana między pierwszą, a trzecią organizacją (ilustruje to koncepcję przechodniości zaufania między organizacjami)[69].

Model zaufania mandatowego

W modelu zaufania mandatowego (*ang. mandated trust model*), organizacja ustanawia poziom zaufania z inną organizacją w oparciu o konkretny mandat wydany przez osobę trzecią posiadającą stosowne uprawnienia[70]. Mandat ten może być ustanowiony przez odpowiednie władze za pomocą rozporządzeń wykonawczych, dyrektyw, regulacji lub polityk (np. memorandum kierownika jednostki organizacyjnej nakazujące wszystkim podległym organizacjom zaakceptowanie wyników ocen bezpieczeństwa przeprowadzonych przez dowolną podległą jednostkę w ramach danej organizacji). Zaufanie mandatowe może być również ustanowione, gdy jakaś jednostka organizacyjna zostanie uznana za wiarygodne źródło dostarczania zasobów informacyjnych, w tym produktów, systemów i usług informatycznych. Na przykład organizacja może uzyskać uprawnienia i odpowiedzialność za wydawanie certyfikatów infrastruktury klucza publicznego (PKI) dla grupy organizacji.

Model zaufania hybrydowego

Ogólnie rzecz biorąc, opisane powyżej modele zaufania nie wykluczają się wzajemnie. Każdy z modeli zaufania może być stosowany niezależnie, jako samodzielny model lub w połączeniu z innym modelem. W organizacji może być wykorzystywanych kilka modeli zaufania (np. w różnych fazach cyklu życia systemu). Ponadto, ponieważ organizacje są często duże i zróżnicowane, możliwe jest, że podległe jednostki w ramach organizacji macierzystej mogą niezależnie stosować różne modele zaufania podczas tworzenia relacji zaufania z potencjalnymi organizacjami partnerskimi (w tym podległymi). Struktura zarządzania organizacją może określać specyficzne warunki i zasady, w jaki sposób różne modele zaufania są stosowane w organizacji w sposób wzajemnie uzupełniający.

[69] W modelu zaufania mediacyjnego pierwsza organizacja zazwyczaj nie ma wglądu w naturę relacji zaufania pomiędzy drugą i trzecią organizacją.

[70] Organizacja posiadająca uprawnienia jednoznacznie akceptuje ryzyko, które ma być ponoszone przez wszystkie organizacje objęte mandatem i jest odpowiedzialna za decyzje związane z ryzykiem narzucone przez organizację.

Zastosowanie modeli zaufania

Modele zaufania mogą być stosowane na różnych poziomach w podejściu do zarządzania ryzykiem opisanym w niniejszej publikacji. Żaden z modeli zaufania nie jest z natury lepszy lub gorszy od pozostałych. Niektóre modele mogą być jednak lepiej dostosowane do pewnych sytuacji niż inne. Na przykład, model potwierdzonego zaufania, jako że wymaga dowodów o charakterze technicznym (np. pomyślnie zakończonych testów), prawdopodobnie najlepiej nadaje się do stosowania na Poziomie 3. Z kolei model historycznego zaufania bezpośredniego, w którym znaczny nacisk kładzie się na doświadczenia z przeszłości, jest bardziej odpowiedni do stosowania na Poziomie 1 lub 2. Mediacyjne i mandatowe modele zaufania są zazwyczaj bardziej zorientowane na zarządzanie i w związku z tym najlepiej nadają się do zastosowania na Poziomie 1. Jednak niektóre wdrożenia modelu zaufania wymagającego mandatu, na przykład wymóg zaufania do źródła certyfikatu PKI, są bardziej ukierunkowane na Poziom 3. Podobnie, chociaż model zaufania mediacyjnego jest przede wszystkim zorientowany na Poziom 1, mogą istnieć jego implementacje, które są bardziej zorientowane na system informatyczny Poziomu 3. Przykładem takiego zastosowania może być wykorzystanie usług uwierzytelniania, które potwierdzają autentyczność lub tożsamość komponentu systemu informatycznego lub usługi.

Charakter danej usługi informatycznej może również wpływać na przydatność i możliwość zastosowania różnych modeli zaufania. Model potwierdzonego zaufania jest bardziej tradycyjnym modelem zatwierdzania zaufania do produktu, systemu lub usługi informatycznej. Ten model zaufania sprawdza się jednak najlepiej w sytuacjach, gdy istnieje pewien stopień kontroli między stronami (np. umowa między organizacją, a zewnętrznym dostawcą usług) lub gdy jest wystarczająco dużo czasu na uzyskanie i zatwierdzenie dowodów niezbędnych do ustanowienia relacji zaufania. Potwierdzone zaufanie jest nieoptymalnym modelem w sytuacjach, gdy obie strony są równorzędne i/lub gdy decyzje dotyczące zaufania w odniesieniu do wspólnych/dostarczanych usług muszą być podejmowane szybko ze względu na bardzo dynamiczny i nagły charakter żądanej/dostarczanej usługi (np. architektury zorientowane na usługi).

ZAŁĄCZNIK H STRATEGIE REAGOWANIA NA RYZYKO

OD OCHRONY GRANIC ORGANIZACJI DO OBRONY ZWINNEJ

Organizacje opracowują *strategie zarządzania ryzykiem, jako* część etapu tworzenia ram ryzyka w procesie zarządzania ryzykiem opisanym w rozdziale trzecim. Strategie zarządzania ryzykiem określają sposoby, przy pomocy których organizacje zamierzają szacować ryzyko, reagować na nie i monitorować je - dzięki czemu postrzeganie ryzyka, które organizacje rutynowo wykorzystują przy podejmowaniu decyzji inwestycyjnych i operacyjnych, staje się jasne i przejrzyste. W ramach strategii zarządzania ryzykiem organizacyjnym, organizacje opracowują również strategie reagowania na ryzyko. Praktyczne realia, w jakich funkcjonują dzisiejsze organizacje, sprawiają, że strategie reagowania na ryzyko są niezbędne. Są to: konieczność zapewnienia skuteczności misji/biznesu dzięki technologiom informatycznym, brak wiarygodności dostępnych technologii oraz rosnąca świadomość przeciwników, że mogą oni osiągnąć swoje cele i wyrządzić szkody, narażając na szwank systemy informatyczne organizacji oraz środowiska, w których te systemy funkcjonują. Kierownictwo współczesnych organizacji stoi przed dylematem niemal nie do rozwiązania - technologie informatyczne niezbędne do osiągnięcia sukcesu w realizacji misji/biznesu mogą być tymi samymi technologiami, za pomocą których przeciwnicy doprowadzają do niepowodzenia misji/biznesu. Strategie reagowania na ryzyko, opracowane i wdrożone przez organizacje, dostarczają liderom i kadrze kierowniczej (tj. osobom podejmującym decyzje w organizacjach) praktycznych, pragmatycznych sposobów radzenia sobie z tym dylematem. Jasno zdefiniowane i wyrażone strategie reagowania na ryzyko zapewniają, że liderzy/kierownictwo wyższego szczebla przejmują odpowiedzialność za reakcje na ryzyko organizacyjne i są ostatecznie odpowiedzialni za decyzje dotyczące ryzyka - rozumiejąc, dostrzegając i jednoznacznie akceptując wynikające z tego ryzyko dla misji/biznesu.

Jak opisano w rozdziale drugim, istnieje pięć podstawowych rodzajów reakcji na ryzyko: (i) akceptacja; (ii) unikanie; (iii) ograniczanie; (iv) współdzielenie; oraz (v) transfer

(przeniesienie)[71]. Chociaż każdy typ reakcji może mieć powiązaną strategię, powinna istnieć ogólna strategia wyboru spośród podstawowych typów reakcji. Ta ogólna strategia reagowania na ryzyko oraz strategia dla każdego typu reakcji zostały omówione poniżej. Ponadto przedstawiono specyficzne strategie ograniczania ryzyka, w tym opis tego, jak takie strategie można wdrożyć w organizacjach.

H.1 OGÓLNE STRATEGIE REAGOWANIA NA RYZYKO

Strategie reagowania na ryzyko określają: (i) osoby lub subkomponenty organizacyjne, które są odpowiedzialne za wybrane środki reagowania na ryzyko oraz specyfikacje kryteriów skuteczności (tj. wyartykułowanie wskaźników i progów, według których można oceniać skuteczność środków reagowania na ryzyko); (ii) zależności wybranych środków reagowania na ryzyko od innych środków reagowania na ryzyko; (iii) zależności wybranych środków reagowania na ryzyko od innych czynników (np. wdrożenie innych planowanych środków technologii informacyjnej); (iv) harmonogram wdrażania środków reagowania na ryzyko; (v) plany monitorowania skuteczności środków reagowania na ryzyko; (vi) określenie czynników inicjujących monitorowanie ryzyka; oraz (vii) tymczasowe środki reagowania na ryzyko wybrane do wdrożenia, jeśli jest to właściwe. Strategie wdrażania środków reagowania na ryzyko mogą obejmować środki tymczasowe, które organizacje zdecydują się wdrożyć. Ogólna strategia reagowania na ryzyko przedstawia podejście organizacyjne do wyboru podstawowych reakcji na ryzyko w danej sytuacji ryzyka. Decyzja o zaakceptowaniu ryzyka musi być zgodna z określoną tolerancją organizacji na ryzyko. Nadal jednak istnieje potrzeba dobrze zdefiniowanej, ustalonej ścieżki organizacyjnej w zakresie wyboru jednej lub kombinacji reakcji na ryzyko: akceptacji, unikania, ograniczania, współdzielenia lub przeniesienia. Organizacje często znajdują się w sytuacjach, w których ryzyko jest większe niż to, które chcą zaakceptować wyznaczeni liderzy wyższego szczebla/kadra kierownicza. Prawdopodobnie konieczna będzie akceptacja niektórych rodzajów ryzyka. Możliwe jest

[71] Podstawowe reakcje na ryzyko nakładają się na siebie. Na przykład ryzyko współdzielone to takie, które jest akceptowane przez każdą ze stron w porozumieniu dotyczącym dzielenia się ryzykiem, a unikanie ryzyka może być rozumiane, jako ograniczanie go do zera. Niemniej jednak, przy takim rozumieniu zachodzących na siebie elementów, warto zająć się każdym z pięciu rodzajów reakcji na ryzyko osobno.

unikanie ryzyka, dzielenie się nim lub przenoszenie go, a pewne ograniczanie ryzyka jest prawdopodobnie wykonalne. Uniknięcie ryzyka może wymagać selektywnego przeprojektowania misji organizacji/procesów biznesowych oraz rezygnacji z niektórych korzyści wynikających z zastosowania technologii informacyjnej w całej organizacji, być może nawet z tego, co organizacje postrzegają, jako niezbędne korzyści. Ograniczanie ryzyka wymaga nakładów pewnych ograniczonych zasobów i może szybko stać się nieefektywne kosztowo ze względu na pragmatyczne realia dotyczące stopnia ograniczania ryzyka, jaki można faktycznie osiągnąć. Wreszcie, dzielenie się ryzykiem i jego transfer mają również konsekwencje, z których niektóre, jeśli nie są nie do przyjęcia, mogą być niepożądane. Strategie reagowania na ryzyko stosowane przez organizacje umożliwiają liderom/kadrze kierowniczej podejmowanie decyzji opartych na ryzyku, zgodnych z celami, zadaniami i szerszą perspektywą organizacyjną.

H.2 STRATEGIE AKCEPTACJI RYZYKA

Strategie akceptacji ryzyka organizacyjnego są niezbędnym uzupełnieniem organizacyjnych deklaracji tolerancji ryzyka. Celem ustanowienia tolerancji ryzyka organizacyjnego jest określenie w sposób jasny i jednoznaczny limitu ryzyka, tzn. jak daleko organizacja jest gotowa się posunąć, przyjmując ryzyko w odniesieniu do działalności organizacyjnej (w tym misji, funkcji, wizerunku i reputacji), majątku organizacyjnego, osób, innych organizacji oraz Państwa. Jednak działania w świecie rzeczywistym rzadko są tak proste, aby takie stwierdzenia dotyczące tolerancji ryzyka stały się ostatecznym punktem odniesienia w podejmowaniu decyzji o akceptacji ryzyka. Organizacyjne strategie akceptacji ryzyka umieszczają akceptację ryzyka w ramach organizacyjnych perspektyw radzenia sobie z praktycznymi realiami działania w warunkach ryzyka i dostarczają wskazówek niezbędnych do zapewnienia, że zakres ryzyka akceptowanego w konkretnych sytuacjach jest zgodny z kierunkiem działania organizacji.

H.3 STRATEGIE UNIKANIA RYZYKA

Spośród wszystkich strategii reagowania na ryzyko, strategie unikania ryzyka organizacyjnego mogą być kluczem do osiągnięcia odpowiedniego reagowania na ryzyko. Ze względu na pragmatyczne realia dotyczące wiarygodności technologii informacyjnych

dostępnych do wykorzystania w ramach powszechnych ograniczeń zasobów, rozważne korzystanie z tych technologii stanowi prawdopodobnie istotną, jeśli nie najważniejszą reakcję na ryzyko. Rozsądne korzystanie z technologii informacyjnych, które składają się na systemy informatyczne organizacji, jest podstawową formą unikania ryzyka, polegającą na tym, że organizacje modyfikują sposób korzystania z technologii informacyjnych w celu zmiany charakteru ponoszonego ryzyka (tj. uniknięcia ryzyka). Takie podejście może jednak stać w sprzeczności z dążeniami organizacji, a w niektórych przypadkach z nakazem pełnej automatyzacji procesów biznesowych. Organizacje proaktywnie rozwiązują ten dylemat, zapewniając, że: (i) liderzy wyższego szczebla/kadra kierownicza (oraz inny personel organizacyjny podejmujący decyzje oparte na ryzyku) byli odpowiedzialni tylko za to, na co mają wpływ; oraz (ii) osoby podejmujące decyzje mogły podejmować trudne decyzje dotyczące ryzyka, co w rzeczywistości może leżeć w najlepszym interesie organizacji.

H.4 STRATEGIE WSPÓŁDZIELENIA i TRANSFERU RYZYKA

Strategie *współdzielenia ryzyka* organizacyjnego i strategie *transferu ryzyka* są kluczowymi elementami umożliwiającymi podejmowanie decyzji dotyczących ryzyka związanego z określonymi misjami/funkcjami biznesowymi na Poziomie 2 lub organizacyjnymi systemami informatycznymi na Poziomie 3. Strategie współdzielenia i transferu ryzyka zarówno uwzględniają, jak i w pełni wykorzystują zmniejszenie ryzyka poprzez współdzielenie/transfer potencjalnego wpływu na inne wewnętrzne elementy organizacyjne lub z innymi organizacjami zewnętrznymi, co sprawia, że inne podmioty są w rzeczywistości całkowicie (transfer) lub częściowo (współdzielenie) odpowiedzialne za ryzyko. Aby współdzielenie lub transfer ryzyka były skutecznymi reakcjami na ryzyko, muszą one uwzględniać wpływ na środowisko lokalne (np. misję/procesy biznesowe lub systemy informatyczne), tzn. nacisk musi być położony na powodzenie misji/biznesu, a nie na przypisywanie winy za niepowodzenie. Ponadto działania związane ze współdzieleniem i transferem ryzyka muszą być prowadzone zgodnie z dynamiką i realiami wewnątrz- i międzyorganizacyjnymi (np. kultura organizacyjna, zarządzanie, tolerancja ryzyka). Wyjaśnia to, dlaczego strategie współdzielenia/transferu ryzyka są szczególnie ważne, aby dzielenie się ryzykiem i/lub jego przenoszenie było realną opcją reagowania na ryzyko.

H.5 STRATEGIE OGRANICZANIA RYZYKA

Organizacyjne strategie ograniczania ryzyka odzwierciedlają perspektywę organizacyjną dotyczącą tego, jakie środki ograniczające i gdzie te środki należy zastosować, aby zmniejszyć ryzyko związane z bezpieczeństwem informacji w odniesieniu do działań i aktywów organizacyjnych, osób, innych organizacji i Państwa. Strategie ograniczania ryzyka stanowią podstawowe ogniwo łączące programy zarządzania ryzykiem organizacyjnym z programami bezpieczeństwa informacji - przy czym te pierwsze obejmują wszystkie aspekty zarządzania ryzykiem, a te drugie są przede wszystkim częścią komponentu reagowania na ryzyko w procesie zarządzania ryzykiem. Skuteczne strategie ograniczania ryzyka uwzględniają ogólne umiejscowienie i podział środków ograniczających ryzyko, stopień zamierzonego ograniczenia oraz obejmują środki ograniczające na Poziomie 1 (np. zabezpieczenia wspólne), na Poziomie 2 (np. architektura korporacyjna, w tym wbudowana architektura bezpieczeństwa informacji, oraz świadome ryzyka procesy realizacji misji/biznesu) oraz na Poziomie 3 (środki bezpieczeństwa stosowane w poszczególnych systemach informatycznych). Strategie ograniczania ryzyka organizacyjnego obejmują następujące elementy:

- procesy związane z misją/biznesem, zaprojektowane z uwzględnieniem potrzeb w zakresie ochrony informacji i wymogów bezpieczeństwa informacji[72];
- architektury korporacyjne (w tym wbudowane architektury bezpieczeństwa informacji) są projektowane z uwzględnieniem realistycznie osiągalnych środków ograniczających ryzyko;
- środki ograniczające ryzyko są wdrażane w organizacyjnych systemach informatycznych i środowiskach operacyjnych przy zastosowaniu zabezpieczeń/środków zaradczych (tj. środków bezpieczeństwa) zgodnych z architekturą bezpieczeństwa informacji; oraz

[72] W uzupełnieniu potrzeb ochrony informacji wynikających z misji/biznesu, niezbędne informacje są pozyskiwane z różnych źródeł (np. z ustawodawstwa, polityk, dyrektyw, przepisów i norm).

- programy, procesy i środki ochrony/przeciwdziałania w zakresie bezpieczeństwa informacji są bardzo elastyczne i zwinne w realizacji, z uwzględnieniem różnorodności misji i funkcji biznesowych organizacji oraz dynamicznych środowisk, w których one działają[73].

Organizacje opracowują strategie ograniczania ryzyka w oparciu o cele i zadania strategiczne, wymagania misji i wymagania biznesowe oraz priorytety organizacyjne. Strategie te stanowią podstawę do podejmowania w organizacji decyzji opartych na analizie ryzyka, dotyczących rozwiązań w zakresie bezpieczeństwa informacji związanych z systemami informatycznymi i stosowanych w tych systemach. Strategie ograniczania ryzyka są niezbędne do zapewnienia, że organizacje są odpowiednio chronione przed rosnącymi zagrożeniami informacji przetwarzanych, przechowywanych i przesyłanych przez organizacyjne systemy informatyczne. Charakter zagrożeń i dynamiczne środowiska, w których działają organizacje, wymagają elastycznych i skalowalnych mechanizmów obronnych oraz rozwiązań, które można dostosować do szybko zmieniających się warunków. Warunki te obejmują na przykład pojawianie się nowych zagrożeń i podatności, rozwój nowych technologii, zmiany misji/wymagań biznesowych i/lub zmiany w środowiskach działania. Skuteczne strategie ograniczania ryzyka wspierają cele i zadania organizacji oraz ustalone cele misji/biznesu, są ściśle powiązane z architekturą korporacyjną i architekturą bezpieczeństwa informacji oraz mogą funkcjonować przez cały cykl życia systemu.

Tradycyjne strategie ograniczania ryzyka w odniesieniu do zagrożeń związanych z cyberatakami, początkowo opierały się prawie wyłącznie na monolitycznej *ochronie brzegowej*. Strategie te zakładały, że przeciwnicy znajdują się poza jakimś ustalonym obszarem obronnym, a celem organizacji jest odparcie ataku. Głównym celem statycznej ochrony brzegowej była odporność na penetrację produktów informatycznych i systemów informatycznych wykorzystywanych przez organizację, a także wszelkie dodatkowe zabezpieczenia i środki zaradcze wdrożone w środowiskach, w których te produkty i systemy

[73] Dynamiczne środowiska działania charakteryzują się, na przykład, ciągłymi zmianami w ludziach, procesach, technologiach, infrastrukturze fizycznej i zagrożeniach.

działały. Uznanie, że granice systemów informatycznych są przenikalne lub nieszczelne, doprowadziło do powstania strategii obrony w głąb (ang. defense-in-depth), jako części strategii ograniczania zagrożeń, polegającej na mechanizmach wykrywania i reagowania na zagrożenia występujące w granicach strefy ochronnej. W dzisiejszym świecie charakteryzującym się *zaawansowanymi trwałymi zagrożeniami*[74] potrzebna jest bardziej kompleksowa strategia ograniczania ryzyka - strategia, która łączy tradycyjną ochronę brzegową z *obroną zwinną*.

Obrona zwinna zakłada, że niewielki procent zagrożeń wynikających z celowych cyberataków będzie skuteczny poprzez kompromitację organizacyjnych systemów informatycznych za pośrednictwem łańcucha dostaw[75], pokonując wstępne zabezpieczenia i środki zaradcze (tj. środki bezpieczeństwa) wdrożone przez organizacje lub wykorzystując wcześniej niezidentyfikowane podatności, dla których nie wprowadzono zabezpieczeń. W tym scenariuszu przeciwnicy działają wewnątrz granic strefy obronnej ustanowionej przez organizacje i mogą mieć znaczną lub całkowitą kontrolę nad systemami informatycznymi organizacji. Obrona zwinna wykorzystuje koncepcję odporności systemów informatycznych, czyli zdolność systemów do działania podczas ataku, nawet w stanie zdegradowanym lub osłabionym, oraz do szybkiego odzyskania zdolności operacyjnych w zakresie podstawowych funkcji po udanym ataku. Koncepcję odporności systemów informatycznych można również zastosować do innych klas zagrożeń, w tym do zagrożeń wynikających z zakłóceń środowiskowych i/lub ludzkich błędów niedopełnienia/zaniechania. Najskuteczniejsze strategie ograniczania ryzyka wykorzystują połączenie ochrony brzegowej i obrony zwinnej,

[74] *Zaawansowane trwałe zagrożenie* to adwersarz, który posiada zaawansowany poziom wiedzy specjalistycznej i znaczne zasoby, co pozwala mu stwarzać okazje do osiągania swoich celów przy użyciu wielu wektorów ataku (np. cyberataku, ataku bezpośredniego i podstępu). Do celów tych należy zazwyczaj ustanowienie/rozszerzenie dostępu do infrastruktury informatycznej organizacji będących celem ataku w celu wydostania informacji, podważenia lub utrudnienia krytycznych aspektów misji, programu lub organizacji, lub też pozycjonowanie się w celu realizacji tych celów w przyszłości. Zaawansowane trwałe zagrożenie: (i) realizuje wielokrotnie swoje cele w dłuższym okresie czasu; (ii) dostosowuje się do wysiłków obrońców próbujących mu się przeciwstawić; oraz (iii) jest zdeterminowane, aby utrzymać poziom interakcji niezbędny do realizacji swoich celów.

[75] Publikacja NIST Interagency Report 7622 zawiera wytyczne dotyczące zarządzania ryzykiem w łańcuchu dostaw.

w zależności od charakterystyki zagrożenia[76]. Ta podwójna strategia ochrony ilustruje dwie ważne koncepcje bezpieczeństwa informacji, znane jako „obrona w głąb" (*ang. defense-in-depth*)[77] i „obrona wszerz" (*ang. defense-in-breadth*[78].

Informacja ma określoną wartość i musi być chroniona. Systemy informatyczne (w tym ludzie, procesy i technologie) są podstawowymi narzędziami wykorzystywanymi do przetwarzania, przechowywania i przekazywania takich informacji - dzięki nim organizacje mogą realizować swoje misje w różnych środowiskach działania i ostatecznie odnosić sukcesy.

[76] Charakterystyka zagrożeń obejmuje zdolności, zamiary i informacje o celach.

[77] „Obrona w głąb" to strategia bezpieczeństwa informacji, która integruje ludzi, technologię i możliwości operacyjne w celu ustanowienia zmiennych zabezpieczeń na wielu poziomach i w różnych misjach organizacji.

[78] „Obrona wszerz" to zaplanowany, systematyczny zestaw multidyscyplinarnych działań, których celem jest identyfikacja, zarządzanie i redukcja ryzyka wykorzystania podatności na każdym etapie cyklu życia systemu, sieci lub subkomponentu (projektowanie i rozwój systemu, sieci lub produktu, produkcja, pakowanie, montaż, integracja systemu, dystrybucja, eksploatacja, utrzymanie i wycofanie z eksploatacji).