Załącznik do zarządzenia
Ministra Funduszy i Polityki
Regionalnej z dnia 10 marca
2023 r. (poz. 7)

Metodyka zarządzania ryzykiem bezpieczeństwa informacji w Ministerstwie Funduszy i Polityki Regionalnej

Rozdział 1

Przepisy ogólne i definicje

§ 1. 1. Metodyka zarządzania ryzykiem bezpieczeństwa informacji w Ministerstwie Funduszy i Polityki Regionalnej, zwana dalej „Metodyką", jest elementem zarówno systemu zarządzania bezpieczeństwem informacji, jak i systemu zarządzania ryzykiem. Metodyka stanowi podstawowy dokument w zakresie szacowania ryzyka bezpieczeństwa informacji, w tym ryzyka w cyberprzestrzeni, w Ministerstwie Funduszy i Polityki Regionalnej, zwanym dalej „Ministerstwem". Metodyka nie jest podstawą do szacowania ryzyka w ramach kontroli zarządczej, ale może stanowić wsparcie podczas realizacji działań związanych z kontrolą zarządczą.

2. Metodyka określa metodę szacowania ryzyka bezpieczeństwa informacji i sposób postępowania z ryzykiem bezpieczeństwa informacji, zwanym dalej „ryzykiem".

3. Metodyka stanowi realizację § 20 ust. 2 pkt 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247) w zakresie konieczności przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko stosownie do wyników przeprowadzonej analizy.

4. Metodyka opracowana została z wykorzystaniem obowiązujących standardów i norm, w szczególności norm ISO z serii ISO/IEC 2700x i obejmuje trzy główne atrybuty bezpieczeństwa: poufności, integralności i dostępności.

5. Szacowanie ryzyka powinno być realizowane wobec wszystkich użytkowanych w Ministerstwie zasobów, o których mowa w załączniku nr 1 do Metodyki, lub które mogą

mieć wpływ na bezpieczeństwo informacji, w szczególności na bezpieczeństwo danych osobowych.

6. Metodykę stosują:

1) obowiązkowo – co najmniej raz w roku – Biuro Polityki Bezpieczeństwa, zwane dalej „BPB”, i Departament Informatyki, zwany dalej „DI”, we współpracy z Pełnomocnikiem do spraw Bezpieczeństwa Informacji w Ministerstwie, zwanym dalej „Pełnomocnikiem”;
2) fakultatywnie – w zależności od potrzeb – pozostałe komórki organizacyjne.

7. Metodyki nie stosuje się do informacji niejawnych. Ryzyko towarzyszące przetwarzaniu informacji niejawnych jest zarządzane z wykorzystaniem odrębnej, dedykowanej metodyki.

§ 2. W procesie zarządzania ryzykiem biorą udział wszyscy pracownicy Ministerstwa, w tym członkowie kierownictwa Ministerstwa i dyrektorzy komórek organizacyjnych.

§ 3. 1. Pełnomocnik nadzoruje proces zarządzania ryzykiem, w tym jego szacowanie. Szacowanie ryzyka polega na jego identyfikowaniu, analizie i ocenie.

2. Pełnomocnik inicjuje proces szacowania ryzyka, o którym mowa w ust. 1, co najmniej raz w roku, nie później niż do końca pierwszego kwartału.

3. BPB i DI przeprowadzają szacowanie ryzyka obowiązkowo do końca pierwszego półrocza każdego roku. Inne komórki organizacyjne przeprowadzają dodatkowe, fakultatywne szacowanie ryzyka w dowolnym czasie – w tym przypadku ust. 2 nie ma zastosowania.

4. Wyniki procesu szacowania ryzyka wpisuje się do tabeli szacowania i postępowania z ryzykiem, zwanej dalej „tabelą”, której wzór stanowi załącznik nr 2 do Metodyki.

§ 4. 1. W razie przeprowadzania istotnej zmiany zakresu działania lub zaistnienia istotnych okoliczności mogących wpływać na realizację celów i zadań Ministerstwa lub danej komórki organizacyjnej, należy każdorazowo oszacować ryzyko i zaktualizować tabelę.

2. W przypadku zmian, o których mowa w ust. 1 DI lub BPB występują do właściwej komórki organizacyjnej o przekazanie informacji o zmianach; komórka ta bierze udział w weryfikacji wyników analizy ryzyka. Proces weryfikacji ryzyka może zostać także zainicjowany przez komórkę lub komórki, w których nastąpiła istotna zmiana – poprzez wystąpienie z wnioskiem do DI lub BPB, przy czym weryfikacje koordynuje lub przeprowadza DI lub BPB odpowiednio.

§ 5. Za terminowe i poprawne szacowanie ryzyka w zakresie analiz obligatoryjnych na mocy niniejszej Metodyki odpowiada Pełnomocnik, a szczegółowy sposób jego

przeprowadzenia, uwzględniający zasady zawarte w Metodyce, określa dyrektor komórki organizacyjnej przeprowadzającej szacowanie ryzyka.

§ 6. Użyte w Metodyce określenia oznaczają:

1) aktywa – wszystko, co stanowi wartość dla Ministerstwa i w związku z tym wymaga ochrony, w tym aktywa informacyjne;
2) akceptacja ryzyka – decyzję uprawnionej osoby o zaniechaniu działań mających na celu zmianę poziomu ryzyka;
3) analiza ryzyka – systematyczne podejście mające na celu zidentyfikowanie w systemie źródeł ryzyka i przypisanie zidentyfikowanym ryzykom wartości;
4) członek kierownictwa Ministerstwa – Ministra, sekretarzy stanu, podsekretarzy stanu oraz Dyrektora Generalnego Ministerstwa;
5) dostępność informacji – właściwość polegającą na tym, że informacja jest możliwa do wykorzystania przez uprawniony podmiot na jego żądanie, w założonym czasie;
6) dyrektor – dyrektora departamentu, biura albo osobę kierującą komórką organizacyjną;
7) identyfikowanie ryzyka – proces znajdowania, zestawiania i charakteryzowania przyczyn ryzyka w systemie;
8) incydent – pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia funkcjonowania Ministerstwa i zagrażają bezpieczeństwu informacji;
9) integralność informacji – właściwość polegającą na tym, że informacja nie została zmodyfikowana w sposób nieuprawniony;
10) istotność ryzyka – punktową ocenę ryzyka wyliczaną jako iloczyn prawdopodobieństwa wystąpienia danego ryzyka i jego wpływu na realizację celów i zadań określonych w planie działalności Ministra lub celów i zadań komórki organizacyjnej;
11) komórka organizacyjna – departament lub biuro wchodzące w skład Ministerstwa, zgodnie ze statutem Ministerstwa;
12) końcowy poziom ryzyka – poziom ryzyka pozostający po procesie postępowania z ryzykiem;
13) materializacja zagrożenia – stan, w którym zagrożenie oddziałuje na aktywa;
14) Minister – ministra właściwego do spraw rozwoju regionalnego;

15) ocena ryzyka – proces porównywania wartości ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
16) plan działalności Ministra – plan działalności Ministra na rok następny, sporządzony zgodnie z przepisami wydanymi na podstawie art. 70 ust. 7 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2022 r. poz. 1634, z późn. zm.[1)]);
17) podatność – słabość zasobu (aktywa) lub zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie;
18) postępowanie z ryzykiem – proces wyboru i wdrażania środków sterowania ryzykiem mających na celu zmianę wartości poziomu ryzyka;
19) poziom ryzyka – produkt operacji na wartości przypisanej skutkowi i wartości związanej z prawdopodobieństwem zaistnienia zdarzenia powodującego skutek;
20) poufność informacji – właściwość polegającą na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
21) ryzyko – możliwość wystąpienia zdarzenia, które będzie miało negatywny wpływ na realizację celów i zadań określonych w planie działalności Ministra lub celów i zadań komórki organizacyjnej;
22) skutek – negatywną zmianę w odniesieniu do zaplanowanego poziomu miernika celu w wyniku oddziaływania zagrożenia;
23) szacowanie ryzyka – całościowy proces analizy i oceny ryzyka;
24) właściciel ryzyka − osoba lub komórka organizacyjna odpowiedzialna za ryzyko wobec posiadanych zasobów (aktywów);
25) właściciel zasobów – osoba lub komórka organizacyjna posiadająca aktywa stanowiące wartość informacyjną.

Rozdział 2

Proces szacowania ryzyka

§ 7. 1. Metodyka opiera się na identyfikowaniu zasobów pod kątem bezpieczeństwa informacji, które mają wpływ na cele i zadania Ministerstwa. Działania w tym zakresie prowadzą do opracowania zbiorczego dokumentu, informującego członków kierownictwa Ministerstwa o istniejących ryzykach i ich istotności.

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 1692, 1725, 1747, 1768, 1964 i 2414.

2. Szacowanie ryzyka wykonywane jest z użyciem tabeli.

3. Proces szacowania ryzyka w Ministerstwie koordynuje Pełnomocnik, a proces szacowania ryzyka w komórce organizacyjnej koordynuje dyrektor, wskazany przez niego zespół lub osoba, we współpracy z właścicielami zasobów i właścicielami ryzyka. Identyfikowanie zagrożeń i podatności może zostać dokonane w szczególności przez właścicieli ryzyka w oparciu o posiadane informacje o zagrożeniach, podatnościach i incydentach, które ich dotyczą.

§ 8. Schemat procesu zarządzania ryzykiem określony jest w załączniku nr 3 do Metodyki.

Rozdział 3

Identyfikowanie zasobów i analiza ryzyka

§ 10. 1. Podczas identyfikowania zasobów konieczne jest określenie ich właścicieli – pracowników lub komórek organizacyjnych odpowiedzialnych za każdy z nich.

2. Pierwszym krokiem w szacowaniu ryzyka jest zidentyfikowanie wszystkich istotnych zasobów pod kątem przetwarzanych informacji, należących do komórek organizacyjnych – dotyczy to wszystkich zasobów posiadających potencjał informacyjny, pod kątem poufności, integralności i dostępności.

§ 11. Wyniki identyfikowania zasobów wpisuje się do wykazu zasobów podstawowych (przykładowych) stanowiącego załącznik nr 1 do Metodyki oraz zakładki: „Zasoby” w tabeli.

§ 12. Zasoby Ministerstwa, które mogą podlegać identyfikowaniu, obejmują w szczególności:

1) dane oraz wszelkie informacje wpływające na wartość Ministerstwa, w tym informacje udokumentowane, elektroniczne oraz przetwarzane w formie tradycyjnej;
2) zasoby ludzkie;
3) wizerunek Ministerstwa;
4) usługi i licencje, procesy zlecane na zewnątrz;
5) sprzęt informatyczny mobilny i stacjonarny, sprzęt IT, infrastruktura IT;
6) dane na nośnikach danych np. pendrive’y, dyski, płyty CD;
7) aplikacje, bazy danych;
8) urządzenia dostępowe i oprogramowanie;

9) systemy teleinformatyczne i cyberprzestrzeń Ministerstwa;
10) zabezpieczenia organizacyjne, techniczne oraz fizyczne i środowiskowe;
11) siedziba i nieruchomości oraz poszczególne pomieszczenia użytkowane przez Ministerstwo.

§ 13. 1. Identyfikowania zagrożeń i prawdopodobieństw dokonuje się z użyciem katalogów zagrożeń znajdujących się w tabeli.

2. Poszczególne zasoby mogą być związane z więcej niż jednym zagrożeniem, a każde zagrożenie może mieć inny wpływ na poufność, integralność i dostępność informacji – wartości te określamy odpowiednio w kolumnach D, E, F tabeli.

3. Identyfikowanie zagrożeń i prawdopodobieństw następuje poprzez uzupełnienie arkusza „zagrożenia” w tabeli.

§ 14. Po uzupełnieniu informacji, o których mowa w § 13, uzupełnia się informację w kolejnych arkuszach dotyczących poszczególnych zasobów określonych w tabeli.

§ 15. Pierwotny poziom ryzyka obliczany jest według wzoru:

$$R_p = P*(S_d+S_i+S_p), \text{ gdzie:}$$

$R_p \in (0,48)$,

P – wartość przypisana prawdopodobieństwu materializacji zagrożenia, $P \in \{0,1,2,3,4\}$,

S_d – skutki dla dostępności informacji, $Sd \in \{0,1,2,3,4\}$,

S_i – skutki dla integralności informacji, $Si \in \{0,1,2,3,4\}$,

S_p – skutki dla poufności informacji, $Sp \in \{0,1,2,3,4\}$.

§ 16. Na analizę ryzyka składają się:
1) szacowanie następstw;
2) szacowanie prawdopodobieństwa incydentu (zmaterializowania się ryzyka);
3) określenie poziomu ryzyka.

§ 17. Do szacowania poziomu prawdopodobieństwa zaistnienia zdarzenia stosuje się metodę punktową, zgodnie z poniższą skalą:

0	zdarzenie nieprawdopodobne (zagrożenie nie występuje)	wystąpienie zagrożenia jest wysoce nieprawdopodobne w odniesieniu do analizowanej czynności lub charakter zagrożenia jest nieadekwatny do specyfiki czynności
1	zdarzenie prawie nieprawdopodobne	zagrożenie wystąpiło rzadziej niż co dziesięć lat lub brak jest informacji, by zagrożenie występowało w podobnych podmiotach
2	zdarzenie mało prawdopodobne	zagrożenie wystąpiło co kilka lat lub zagrożenie wystąpiło w podobnych podmiotach w pojedynczych przypadkach
3	zdarzenie wysoce prawdopodobne	zagrożenie wystąpiło kilka razy w roku w podobnych podmiotach
4	zdarzenie niemal pewne	wystąpiło wielokrotnie w ciągu roku w danym podmiocie lub w podobnych podmiotach

§ 18. Do szacowania poziomu skutków zdarzenia stosuje się metodę punktową, zgodnie z poniższą skalą:

0	zdarzenie nie powoduje skutku (brak podatności)	utrata poufności, dostępności lub integralności nie występuje
1	zdarzenie wywołuje niewielki skutek	utrata poufności, dostępności lub integralności powoduje niewielkie konsekwencje finansowe oraz ma niski wpływ na zobowiązania prawne, umowne lub reputację organizacji
2	zdarzenie wywołuje znaczący skutek	utrata poufności, dostępności lub integralności powoduje niewielkie konsekwencje finansowe oraz ma średni wpływ na zobowiązania prawne, umowne lub reputację organizacji
3	zdarzenie wywołuje bardzo znaczący skutek	utrata poufności, dostępności lub integralności ma znaczący i/lub natychmiastowy wpływ na przepływy pieniężne w organizacji, jej działanie, zobowiązania prawne lub umowne i/lub jej reputację

4	zdarzenie wywołuje skutek katastrofalny	utrata poufności, dostępności lub integralności ma krytyczny i natychmiastowy wpływ na przepływy pieniężne w organizacji, jej działanie, zobowiązania prawne lub umowne i jej reputację

§ 19. W celu wyznaczenia poziomu ryzyka początkowego w tabeli należy wykonać poniższe czynności:

1) w arkuszu „ZS-1” (a następnie w kolejnych arkuszach) do kolumny B (Nazwa zagrożenia) należy skopiować z arkusza „Zagrożenia” nazwę zagrożenia umieszczoną w kolumnie B (Katalog zagrożeń), co spowoduje automatyczne przekopiowanie stopnia prawdopodobieństwa wystąpienia zagrożenia do kolumny C (Prawdopodobieństwo wystąpienia zagrożenia) w arkuszu „ZS-1”;
2) w kolumnach: D, E i F w arkuszu „ZS-1” określa się odpowiednio wpływ zagrożenia na utratę dostępności, integralności i poufności informacji dla szacowanego zasobu;
3) po wykonaniu czynności, o których mowa w pkt 1 i 2, w kolumnie G (Pierwotny poziom ryzyka, w zakładce zasobów) w arkuszu „ZS-1” zostanie wyliczony pierwotny poziom ryzyka według wzoru zawartego w arkuszu „Słowniki”;
4) następnie wykonujemy czynności, o których mową w pkt 1-3, dla wszystkich arkuszy dotyczących zasobów począwszy od „ZS-2”.

§ 20. 1. Poziomy ryzyka określone są w wartościach liczbowych i procentowych, zgodnie z załącznikiem nr 4 do Metodyki.

2. W przypadku uwzględniania dodatkowych kryteriów bezpieczeństwa informacji – poza poufnością, integralnością i dostępnością – należy odpowiednio rozszerzyć wzór służący do obliczania poziomu ryzyka oraz uzupełnić opisy związane z dodatkowymi kryteriami (np. rozliczalnością lub autentycznością).

Rozdział 4

Właściciele ryzyka

§ 21. 1. W przypadku, gdy dane ryzyko wstępuje w kilku komórkach organizacyjnych właścicielem jest komórka organizacyjna, w której dane ryzyko jest największe lub która ma największy wpływ na zarządzanie tym ryzykiem.

2. W przypadku wątpliwości w określeniu właściciela ryzyka decyzję podejmuje Pełnomocnik.

3. W przypadku współdzielenia zasobów z innymi podmiotami Pełnomocnik wskazuje – w porozumieniu z podmiotem - właściciela ryzyka.

Rozdział 5

Ocena ryzyka i postępowanie z ryzykiem

§ 22. 1. Postępowanie z ryzykiem planuje się z użyciem tabeli.

2. Dla wszystkich ryzyk progowych i wysokich niezbędne jest zastosowanie środków ograniczających ryzyka. Poziomy ryzyka są określone w załączniku nr 4 do Metodyki.

3. Za postępowanie z ryzykiem odpowiada właściciel ryzyka.

§ 23. Dla każdego ryzyka oszacowanego na poziomie >40% należy wybrać od jednej do maksymalnie 3 opcji postępowania z ryzykiem:

1) sterowanie ryzykiem – ograniczanie poziomu ryzyka poprzez zastosowanie środka sterowania ryzykiem w postaci zabezpieczenia, dobranego adekwatnie do charakteru tego ryzyka;
2) transfer ryzyka do strony trzeciej – np. poprzez ubezpieczenie ryzyka lub podpisanie innych umów (z dostawcą, partnerem);
3) uniknięcie ryzyka poprzez zaprzestanie działań, które mogą to ryzyko powodować − o ile prowadzenie tych działań nie jest obligatoryjnym wymogiem prawa;
4) akceptacja ryzyka – ta opcja dopuszczalna jest jedynie wtedy, gdy wybór innej opcji postępowania z ryzykiem wiązałby się z kosztami wyższymi niż skutki finansowe incydentu związanego z tym ryzykiem.

§ 24. 1. W wyniku przeliczenia poziomów ryzyka uzyskuje się wartość końcową poziomu ryzyka.

2. Ryzyka, dla których końcowy poziom ryzyka jest niższy lub równy 20% poziomu maksymalnego ($R_k \leq 9,6$), podlegają automatycznej akceptacji, ale pozostają pod nadzorem właściciela ryzyka lub dyrektora komórki organizacyjnej przeprowadzającej szacowanie w celu ich monitorowania.

3. Ryzyka, dla których poziom zawiera się w przedziale $9,6 < R_k \leq 19,2$, podlegają akceptacji przez właściciela ryzyka lub dyrektora komórki organizacyjnej przeprowadzającej szacowanie, monitorowaniu oraz cyklicznej – nie rzadziej niż raz do roku – analizie.

4. Ryzyka, dla których poziom ryzyka jest równy i większy od 40% ($R_k >= 19,2$), przedstawiane są do akceptacji członków kierownictwa Ministerstwa reprezentowanych przez Dyrektora Generalnego Ministerstwa.

§ 25. Na etapie postępowania z ryzykiem dokonuje się ponownego estymowania poziomu ryzyka, czyli ryzyka końcowego z uwzględnieniem zabezpieczenia, zgodnie z wzorem:

$$R_k = P \times (S_d/\Sigma C_d + S_i/\Sigma C_i + S_p/\Sigma C_p), \text{ gdzie:}$$

$R_k \in (0;48)$,

C – skuteczność zabezpieczenia, $C_d, C_i, C_p \in \{1,2,3,4\}$.

§ 26. Poziomy skuteczności zabezpieczeń określone są w poniższy sposób:

1	brak możliwości zastosowania zabezpieczenia lub zastosowanie zabezpieczenia jest niecelowe
2	zabezpieczenie powoduje obniżenie skutku $S_{d,i,p}$ o jeden stopień i ogranicza poziom ryzyka
3	zabezpieczenie powoduje obniżenie skutku $S_{d,i,p}$ o dwa stopnie i w istotny sposób ogranicza poziom ryzyka
4	zabezpieczenie powoduje obniżenie skutku $S_{d,i,p}$ o trzy stopnie i w bardzo istotny sposób ogranicza poziom ryzyka

§ 27. W celu wyznaczenia poziomu ryzyka końcowego w tabeli należy wykonać poniższe czynności:

1) w kolumnach: H, L i P w zakładce dotyczących zasobów, należy wstawić po jednym z zadeklarowanych wcześniej w arkuszu „Zabezpieczenia" zastosowanych środków zabezpieczających wraz z parametrami ich skuteczności na zachowanie dostępności, integralności i poufności, które mają wpływ na ograniczenie ryzyka w zależności od wybranych zagrożeń;
2) po wykonaniu ww. czynności w kolumnie W (Końcowy poziom ryzyka) zostanie wyliczony końcowy poziom ryzyka według wzoru zawartego w arkuszu „Słowniki".

Rozdział 6

Monitorowanie i przeglądy ryzyk

§ 28. 1. BPB i DI, przy ewentualnej współpracy z właścicielami ryzyka, dokonują przeglądów istniejących ryzyk, mogą identyfikować nowe ryzyka oraz aktualizują tabelę.

2. Czynności, o których mowa w ust. 1, należy dokonywać co najmniej raz w roku np. w przypadku znaczących zmian organizacyjnych, zmian w stosowanych technologiach, celach i zadaniach Ministerstwa, otoczeniu działania Ministerstwa.

3. Niezbędne jest stałe monitorowanie ryzyk w celu wykrycia zmian.

4. Działanie, o którym mowa w ust. 3, może być wspierane przez usługi zewnętrzne, które mogą w szczególności dostarczać informacji dotyczących nowych zagrożeń lub nowych rodzajów podatności.

§ 29. Zaleca się ciągłe monitorowanie następujących czynników ryzyka:

1) nowych zasobów, które zostały włączone w zakres zarządzania ryzykiem;
2) koniecznych modyfikacji wartości zasobów (poziomu krytyczności), np. z powodu zmian organizacyjnych lub zmian celów i zadań Ministerstwa;
3) nowych zagrożeń, które mogą być aktywne zarówno na zewnątrz, jak i wewnątrz Ministerstwa, i które dotąd nie zostały oszacowane;
4) nowych podatności pod kątem możliwości ich wpływu na istniejące podatności;
5) zidentyfikowanych rodzajów podatności w celu określenia tych, które są narażone na nowe lub pojawiające się powtórnie zagrożenia;
6) większych skutków lub następstw oszacowanych zagrożeń, rodzajów podatności i typów ryzyka, które razem powodują nieakceptowalny poziom ryzyka;
7) incydentów związanych z bezpieczeństwem informacji.

Rozdział 7

Raportowanie

§ 30. 1. BPB i DI oraz inne komórki organizacyjne szacujące ryzyko dokumentują zarówno wyniki szacowania ryzyka oraz wyniki postępowania z ryzykiem, jak i wszystkie kolejne przeglądy w tabeli.

2. Dyrektorzy komórek organizacyjnych przeprowadzających szacowanie ryzyka odpowiednio monitorują postępy we wdrażaniu planów postępowania z ryzykiem oraz raportują do Pełnomocnika co najmniej raz w roku. Dyrektor komórki organizacyjnej, która przeprowadziła szacowanie ryzyka sporządza raport z szacowania oraz postępowania z ryzykiem i przesyła go wraz z tabelą Pełnomocnikowi. Raport zawiera co najmniej podsumowanie wyników szacowania ryzyka i wnioski, w szczególności w zakresie wzrostu lub spadku poziomu ryzyka i przyczyn zmian.

3. Pełnomocnik, co najmniej raz w roku, przeprowadza analizy w zakresie ryzyka, z zakresu bezpieczeństwa informacji, uwzględniając przekazane raporty, o których mowa w ust. 2, i przekazuje informację zbiorczą Dyrektorowi Generalnemu Ministerstwa. Pełnomocnik może przesłać raporty bezzwłocznie po ich otrzymaniu, jeśli wymaga tego sytuacja wynikająca z wyników zawartych w tych raportach.

Rozdział 8

Zarządzanie dokumentacją

§ 31. 1. Zarządzanie dokumentacją określa załącznik nr 5 do Metodyki.

2. Dyrektorzy BPB, DI oraz innych komórek organizacyjnych przeprowadzających szacowanie ryzyka mogą przyznawać , dostęp do tabeli, raportu, o którym mowa w § 30 ust. 2, oraz planu postępowania z ryzykiem, także pracownikom którzy nie przeprowadzali danego szacowania.

Rozdział 9

Konsultowanie ryzyka

§ 32. 1. Konsultowanie ryzyka szacowanego przez komórki organizacyjne, pozostaje w zakresie działania BPB i DI.

2. Osoby uczestniczące w zarządzaniu ryzykiem mogą na bieżąco konsultować się z Pełnomocnikiem oraz wyznaczonymi pracownikami BPB w zakresie postępowania z ryzykiem.

3. Analizę ryzyka komórki organizacyjne wykonują we współpracy z BPB i DI lub samodzielnie. Wyniki analizy komórki organizacyjne przekazują do wiadomości Pełnomocnika.

Rozdział 10

Postanowienia końcowe

§ 33. 1. Pierwszy, proces zarządzania ryzykiem zgodny z niniejszym zarządzeniem zostanie zrealizowany w pierwszym półroczu 2023 r., a kolejne nie rzadziej niż raz w roku.

2. Sposób realizacji szacowania ryzyka przez DI i BPB, a także inne komórki organizacyjne może być uzgadniany z Pełnomocnikiem.

3. Wyniki przeprowadzonych analiz powinny zostać każdorazowo zaakceptowane zgodnie z § 24. Sposób akceptacji wyników jest uzależniony od poziomu oszacowanego ryzyka i może się wiązać z koniecznością zastosowania dodatkowych zabezpieczeń – akceptacja następuje poprzez akceptację wypełnionej tabeli, w której uwzględnione zostały wyniki całego procesu, w tym oszacowane poziomy ryzyka.

Załączniki do Metodyki
zarządzania ryzykiem
bezpieczeństwa informacji
w Ministerstwie Funduszy
i Polityki Regionalnej

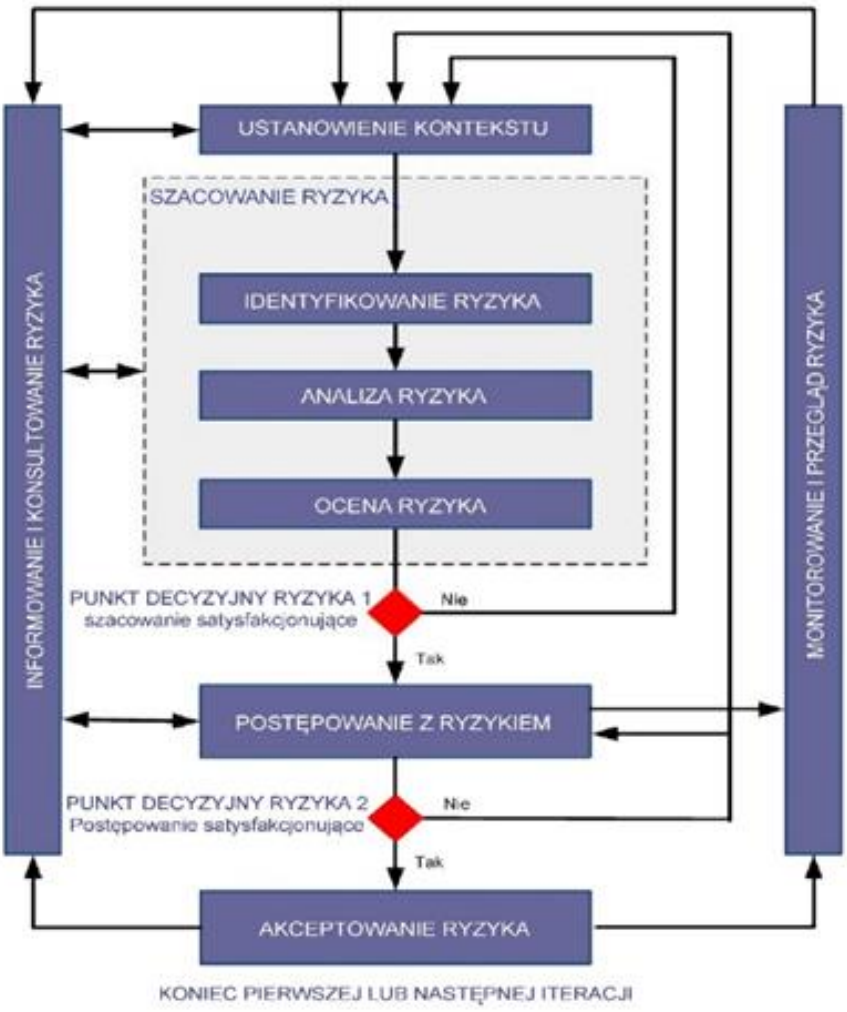
Załącznik nr 1

WYKAZ ZASOBÓW PODSTAWOWYCH (PRZYKŁADOWYCH)

Lp.	NAZWA ZASOBU
	ZS-1 SYSTEM X
	ZS-2 BAZA X
	ZS-3 SYSTEM CENTRALNEGO WYDRUKU
	ZS-4 LOTUS NOTES - APLIKACJE
	ZS-5 PORTAL X
	ZS-6 REJESTR X
	ZS-7 - PROGRAMY W JĘZYKU X
	ZS-8 ZBIÓR NAGRAŃ VIDEO Z KAMERY X
	ZS-9 CENTRALNY REJESTR X
	ZS-10 SERWEROWNIE
	ZS-11 ZASOBY LUDZKIE
	ZS-12 INFRASTRUKTURA
	ZS-13 STACJE ROBOCZE
	ZS-14 ZARZĄDZANIE PARKINGAMI
	ZS-15 BAZA PROJEKTU X
	ZS-16 DOKUMENTACJA X

Załącznik nr 3

SCHEMAT PROCESU ZARZĄDZANIA RYZYKIEM



Załącznik nr 4

Poziomy ryzyka

wysokie	50%-100% (24-48)	ryzyka wysokie nie do zaakceptowania bez zastosowania dodatkowych środków fizycznych, technicznych lub organizacyjnych
progowe	40%-50% (19,2-24)	ryzyka progowe wymagające minimalizacji poprzez zastosowanie dodatkowych środków fizycznych lub organizacyjnych
akceptowalne	20%-40% (9,6-19,2)	ryzyka akceptowalne nawet bez konieczności zastosowania dodatkowych zabezpieczeń
niskie	0%-20% (0-9,6)	ryzyka pomijalne niebrane pod uwagę, niewymagające dodatkowych zabezpieczeń

Załącznik nr 5

ZARZĄDZANIE DOKUMENTACJĄ

NAZWA	MIEJSCE PRZECHOWYWANIA	ZARZĄDZANIE BEZPIECZEŃSTWEM	OKRES PRZECHOWYWANIA
Tabela szacowania ryzyka, w tym ew. Plan postępowania z ryzykiem (którego załącznikiem jest ww. tabela)	**Komórka organizacyjna wykonująca szacowanie oraz Pełnomocnik**	Tylko komórka organizacyjna wykonująca szacowanie ryzyka ma prawo wprowadzać oraz modyfikować dane	Zgodnie z przepisami kancelaryjnymi
Raport z szacowania oraz postępowania z ryzykiem (którego załącznikiem jest ww. tabela)	**Komórka organizacyjna wykonująca szacowanie ryzyka oraz Pełnomocnik**	Tylko komórka organizacyjna wykonująca szacowanie ryzyka ma prawo wprowadzać oraz modyfikować dane	Zgodnie z przepisami kancelaryjnymi