Centralna Biblioteka Statystyczna

Zasady przeprowadzania analizy ryzyka bezpieczeństwa informacji w Centralnej Bibliotece Statystycznej (CBS)

Podpis dyrektora CBS Bożena Łazowska Zatwierdzam 27.10.2021 r.	Signed by / Podpisano przez: Bożena Dorota Łazowska Date / Data: 2021-10-27 08:54

Historia dokumentu

Nr wersji	Data wersji	Zmiany wprowadził	Opis	Uwagi
0.1	2021-03-25	Jacek Knopik (PBSG)/	*Utworzenie szablonu*	
0.2	2021-02-26	KSZBI – zespół projektowy ds. dokumentacji SZBI	*Uzupełnienie dokumentu*	
0.3	Zgodnie z datą zatwierdzenia	Bożena Łazowska- dyrektor CBS	*Nowa wersja główna, zatwierdzona/wprowadzona do użycia*	

Spis treści

I. Wprowadzenie

1. Niniejsze Zasady przeprowadzania analizy ryzyka bezpieczeństwa informacji (dalej: Zasady) stanowią procedurę wyodrębnioną w ramach Polityki Zarządzania Ryzykiem, określającej podejście do zarządzania ryzykiem.
2. Postanowienia, o których mowa w § 3 ust. 6 i 7, § 10 i § 11 ust. 5 (proces zarządzania ryzykiem), § 12 i § 13 (rejestr ryzyka), § 14 z wyłączeniem ust. 4 i § 15 z wyłączeniem ust. 1 (monitorowanie procesu) Polityki Zarządzania Ryzykiem stosuje się odpowiednio, z uwzględnieniem definicji określonych w części I ust. 4, ról i odpowiedzialności określonych w części II oraz częstotliwości określonych w części I ust. 7.
3. Do niniejszych Zasad zastosowanie mają definicje określone w § 2 Polityki zarządzania ryzykiem, z zastrzeżeniem ust. 4 zasad.
4. Użyte w Zasadach określenia oznaczają:

– **Aktywa** – wszystko co stanowi wartość dla organizacji, projektu, programu lub inicjatywy dot. zespołu utworzonego przez Prezesa GUS lub dyrektora CBS, w tym pracownicy, zasób informacyjny, infrastruktura, lokalizacja, umowy, dostawcy, dane, licencje, proces,

– **Administrator techniczny** – dział administratorów systemów informatycznych CBS, na podstawie założeń przekazanych przez Właściciela aktywa,

– **grupa aktywów** – zbiór powiązanych ze sobą aktywów, np. serwery, stacje robocze, urządzenia mobilne, powiązane aplikacje, czy sieć teleinformatyczna,

– **metodyka oceny ryzyka bezpieczeństwa informacji** – zbiór zasad i trybów postępowania dotyczących sposobów identyfikacji, analizy i oceny ryzyka bezpieczeństwa informacji, określona w części III niniejszych Zasad,

– **ryzyko bezpieczeństwa informacji** – możliwość zaistnienia zdarzenia w stosunku do aktywa lub grupy aktywów, które będzie oddziaływało na poufność, dostępność i integralność, mierzone wpływem (skutkiem) i prawdopodobieństwem wystąpienia. Może mieć charakter zagrożenia (zdarzenia szkodliwego) lub też pozytywnej możliwości/szansy (zdarzenia korzystnego – ryzyko utracenia korzyści),

– **ryzyko inherentne** – ryzyko występujące w sytuacji braku zastosowania środków kontroli,

– **ryzyko rezydualne** – ryzyko szczątkowe, pozostające po zastosowaniu środków kontroli,

– **Właściciel aktywa** – dyrektor CBS, kierownik projektu, osoba kierująca zespołem utworzonym przez Prezesa GUS lub dyrektora CBS,

– **Właściciel ryzyka bezpieczeństwa informacji** – osoba odpowiedzialna za monitorowanie i systematyczną ocenę przypisanych jej ryzyk oraz za efektywność działań ograniczających te ryzyka. Właściciel ryzyka prowadzi rejestr zidentyfikowanych ryzyk bezpieczeństwa informacji. Rolę właściciela ryzyka pełni dyrektorCBS, kierownik projektu, osoba kierująca zespołem utworzonym przez Prezesa GUS lub dyrektora CBS, administrator techniczny systemu.

5. Zasady definiują proces zarządzania ryzykiem bezpieczeństwa informacji, zgodnie z wymaganiami Polityki Bezpieczeństwa Informacji Statystyki Publicznej oraz międzynarodowej normy PN-ISO/IEC 27005 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

6. Zasady określają metodę przeprowadzania analizy ryzyka oraz zakres działań związanych z przeprowadzeniem okresowej oceny ryzyka i postępowania z ryzykiem bezpieczeństwa informacji, uwzględniając 5-cio stopniową skalę oceny prawdopodobieństwa wystąpienia danego ryzyka i wpływu (skutku) na realizację celów bezpieczeństwa informacji spójną ze skalą przyjętą w Polityce Zarządzania Ryzykiem.
7. Analiza Ryzyka bezpieczeństwa informacji realizowana jest raz na kwartał w odniesieniu do aktywów istotnych dla programu, projektu, zespołu utworzonego przez dyrektora CBS oraz przynajmniej raz w roku w odniesieniu do pozostałych aktywów.
8. Ryzyka zidentyfikowane zgodnie niniejszymi Zasadami mają swoje odzwierciedlenie w rejestrach ryzyka prowadzonych zgodnie z Polityką Zarządzania Ryzykiem przez każdego Właściciela ryzyka.

II. Struktura zarządzania i odpowiedzialności

1. Dyrektor CBS sprawuje nadzór nad wykonaniem analizy ryzyka bezpieczeństwa informacji dla aktywów, dla których jest Właścicielem aktywa oraz dla których Właścicielem aktywa jest pracownik CBS kierujący programem, projektem, lub zespołem utworzonym przez Prezesa GUS lub dyrektora Biblioteki.
2. W ramach przeprowadzania analizy ryzyka bezpieczeństwa informacji ustanawia się:
   1) Zespół ds. analizy ryzyka bezpieczeństwa informacji;
   2) Koordynatora ds. analizy ryzyka bezpieczeństwa informacji;
   3) Właścicieli ryzyka bezpieczeństwa informacji.
3. W skład Zespołu wchodzą:
   1) Paweł Olszak – Przewodniczący Zespołu, kierujący pracami Zespołu oraz posiadający decydujący głos;
   2) Agnieszka Jakubiak - Koordynator ds. analizy ryzyka bezpieczeństwa informacji;
   3) Marta Skiba - Inspektor Ochrony Danych;
   4) Konrad Rydołowski - Pełnomocnik do spraw bezpieczeństwa fizycznego;
   5) Rafał Gawarecki - Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni.
4. Za organizację prac Zespołu ds. analizy ryzyka bezpieczeństwa informacji odpowiada Koordynator ds. analizy ryzyka bezpieczeństwa informacji w CBS.
5. Do zadań Zespołu ds. analizy ryzyka bezpieczeństwa informacji należy, w szczególności:
   1) zgłaszanie uwag do wyników analizy i oceny ryzyka bezpieczeństwa informacji, proponowanych metod postępowania z ryzykiem bezpieczeństwa informacji oraz rekomendowanie ich Dyrektorowi CBS;
   2) przedkładanie Dyrektorowi CBS w celu akceptacji rekomendacji w zakresie poziomu akceptowalności ryzyka bezpieczeństwa informacji, poprzez zakwalifikowanie ryzyk ocenionych na poziomie minimalnym i umiarkowanym, do ryzyk nieakceptowalnych, dla których niezbędne jest opracowanie przez Kierownika komórki organizacyjnej odpowiedzialnej za ryzyko planu postępowania z ryzykiem;
   3) rekomendowanie Dyrektorowi CBS działań w zakresie integracji zarządzania ryzykiem bezpieczeństwa informacji z innymi procesami w ramach zarządzania i planowania.
6. Spotkania Zespołu ds. analizy ryzyka bezpieczeństwa informacji odbywają się zgodnie z częstotliwością określoną w części I ust. 7.

7. W spotkaniach Zespołu ds. analizy ryzyka bezpieczeństwa informacji mogą uczestniczyć inne osoby zaproszone przez Koordynatora ds. analizy ryzyka bezpieczeństwa informacji.

8. Do zadań i kompetencji Koordynatora ds. analizy ryzyka bezpieczeństwa informacji w CBS należy w szczególności:
   1) prowadzenie zbiorczego rejestru ryzyka bezpieczeństwa informacji;
   2) monitorowanie przebiegu procesów identyfikacji, analizy i oceny ryzyka bezpieczeństwa informacji;
   3) analiza rejestru ryzyka bezpieczeństwa informacji pod kątem kompletności aktywów i grup aktywów, dla których jest ona przeprowadzona;
   4) analizowanie informacji na temat poszczególnych rodzajów ryzyka dla aktywów, o których mowa w ust. 1;
   5) monitorowanie planowania i wdrażania działań, będących reakcją na ryzyko bezpieczeństwa informacji, dla aktywów, o których mowa w ust. 1;
   6) opracowanie po przeprowadzonej pierwszej iteracji analizy i oceny ryzyka informacji o zidentyfikowanych ryzykach nieakceptowalnych oraz planach postępowania z nimi celem przedłożenia Dyrektorowi CBS;
   7) opracowanie raportu z przeprowadzonej analizy i oceny ryzyka bezpieczeństwa informacji, którego wzór określono w załączniku nr 1 do niniejszych Zasad (począwszy od drugiej iteracji analizy i oceny ryzyka), celem przedkładania Dyrektorowi CBS;
   8) inicjowanie działań na rzecz zwiększenia świadomości i kompetencji w zakresie analizy ryzyka bezpieczeństwa informacji.

9. Do zakresu zadań i kompetencji Właścicieli ryzyka bezpieczeństwa informacji należy zarządzanie podległym ryzykiem, w tym:
   1) okresowa identyfikacja, analiza i ocena ryzyka bezpieczeństwa informacji;
   2) okresowa weryfikacja kompletności wykazywanych aktywów i grup aktywów, dla których prowadzona jest identyfikacja, analiza i ocena ryzyka bezpieczeństwa informacji;
   3) identyfikacja i ocena skuteczności środków kontroli podległego ryzyka bezpieczeństwa informacji;
   4) podejmowanie decyzji o przeciwdziałaniu ryzyku bezpieczeństwa informacji;
   5) opracowanie i wdrażanie planu postępowania z podległym nieakceptowalnym ryzykiem bezpieczeństwa informacji;
   6) okresowe monitorowanie i przegląd ryzyka oraz procesu zarządzania ryzykiem bezpieczeństwa informacji;
   7) wdrażanie działań na rzecz zwiększenia świadomości w zakresie zarządzania podległym ryzykiem bezpieczeństwa informacji.

10. Kierownicy komórek organizacyjnych CBS zarządzają, w zakresie o którym mowa w ust. 9, podległym ryzykiem bezpieczeństwa informacji zidentyfikowanych w odniesieniu do aktywów dla których Właścicielem jest Dyrektor CBS – z wyłączeniem ryzyk odnoszących się do programu, projektu, zespołu.

11. W zakresie powierzonych zadań pracownicy:
   1) uczestniczą w identyfikacji, analizie i ocenie ryzyka bezpieczeństwa informacji;
   2) informują bezpośredniego przełożonego o wszystkich zidentyfikowanych ryzykach bezpieczeństwa informacji;

3) monitorują poziom ryzyk zdefiniowanych w rejestrach ryzyka bezpieczeństwa informacji, w zakresie realizowanych zadań;
4) informują bezpośredniego przełożonego, w tym w ramach programu/projektu/zespołu, o istotnych zmianach poziomu ryzyk zidentyfikowanych w rejestrach ryzyka bezpieczeństwa informacji.

III. Metodyka oceny ryzyka bezpieczeństwa informacji

Metodyka oceny ryzyka bezpieczeństwa informacji:
1) zapewnia powtarzalność i porównywalność wyników oceny ryzyka bezpieczeństwa informacji;
2) uwzględnia przy ocenie wartości ryzyka stosowane środki kontroli (mechanizmy kontroli ryzyka), które zmniejszają prawdopodobieństwo lub skutek wystąpienia ryzyka bezpieczeństwa informacji.

III.1. Etapy identyfikacji, analizy i oceny ryzyka bezpieczeństwa informacji

1. Identyfikacja ryzyka bezpieczeństwa informacji przez Właściciela ryzyka bezpieczeństwa informacji polega na wskazaniu potencjalnych czynników ryzyka, czyli zdarzeń, które będą miały wpływ na aktywa. Ich źródłem może być zarówno działalność CBS, jak i jej otoczenie zewnętrzne.

2. Ryzyka bezpieczeństwa informacji identyfikowane są w odniesieniu do zagrożeń i szans dla aktywów, w szczególności dla ich:
   1) poufności, rozumianej jako zapewnienie, że informacja nie jest udostępniania bądź ujawniana osobom podmiotom i procesom nieuprawnionym;
   2) dostępności, rozumianej jako możliwość autoryzowanego wykorzystania danych i informacji w pożądanym czasie;
   3) integralności, rozumianej jako precyzyjność, dokładność oraz kompletność informacji.

3. Dla każdego zidentyfikowanego ryzyka bezpieczeństwa informacji należy uzupełnić rejestr ryzyka zgodnie z poniższą strukturą:
   1) opis ryzyka:
      a) Właściciel ryzyka,
      b) Kierownik komórki organizacyjnej zarządzający ryzykiem w imieniu Właściciela ryzyka,
      c) nazwa aktywa wraz z przyporządkowaniem obszaru aktywa (zgodnie z Tabelą 1 zawartą w części III.2 „Identyfikacja ryzyk w zakresie bezpieczeństwa informacji”), do których aktywo się odnosi,
      d) rodzaj ryzyka (zagrożenie/szansa) i nazwa ryzyka,
      e) potencjalne przyczyny (wewnętrzne i zewnętrzne) wystąpienia danego ryzyka;
   2) ocena skuteczności środków kontroli, z zastrzeżeniem, że w przypadku analizy szans należy pominąć lit. b:
      a) wskazanie środków kontroli, które na moment dokonywania oceny powodują, że zagrożenie jest niższe,
      b) skuteczność środków kontroli według przyjętej 4-stopniowej skali określonej w Tabeli 2 zawartej w części III.3 „Ocena ryzyka bezpieczeństwa informacji”;
   3) ocena ryzyka, z zastrzeżeniem, że w przypadku analizy szans należy pominąć lit. b i c, a w ramach scenariusza wystąpienia ryzyka dokonać opisowej oceny wpływu ryzyka:

a) ocena prawdopodobieństwa wystąpienia ryzyka, według przyjętej 5-stopniowej skali określonej w Tabeli 3 zawartej w części III.3 „Ocena ryzyka bezpieczeństwa informacji”,
b) odrębna ocena skutków wystąpienia ryzyka (wpływ ryzyka) dla dostępności i bezpieczeństwa, według przyjętej 5-stopniowej skali określonej w Tabeli 4 zawartej w części III.3 „Ocena ryzyka bezpieczeństwa informacji”,
c) scenariusz wystąpienia ryzyka,
d) istotność ryzyka inherentnego, która wyliczana jest automatycznie,
e) określenie istotności ryzyka rezydualnego, zgodnie z Tabelą 5 zawartą w części III.3 „Ocena ryzyka bezpieczeństwa informacji”;

4) Określenie planu postępowania z ryzykiem w przypadku wystąpienia ryzyka nieakceptowalnego:
a) planowane działania ograniczenia ryzyka (opis),
b) rodzaj reakcji na ryzyko (słownik),
c) kierownik komórki organizacyjnej/kierownik/przewodniczący zespołu/programu odpowiedzialna za realizację poszczególnych działań realizowanych w ramach planu postępowania z ryzykiem,
d) planowany termin podjęcia działań,
e) status realizacji działań (propozycja postępowania, w trakcie realizacji, zrealizowano, wycofano z realizacji).

III.2. Identyfikacja ryzyk w zakresie bezpieczeństwa informacji

Tabela 1. Obszary aktywów

Obszar aktywów
1) Personel
2) Informacje
3) Sprzęt i wyposażenie
4) Systemy i oprogramowanie
5) Sieć
6) Lokalizacja
7) Organizacja

III.3. Ocena ryzyka

Zidentyfikowane ryzyko należy poddać ocenie mającej na celu określenie skuteczności stosowanych środków kontroli, prawdopodobieństwa wystąpienia danego ryzyka i wpływu (skutku) na realizację celów bezpieczeństwa informacji.

Ocena skuteczności środków kontroli (mechanizmów kontroli ryzyka):

1) Przez środki kontroli ryzyka bezpieczeństwa informacji należy rozumieć m. in. polityki, procedury, zasady, techniczne środki zabezpieczeń oraz inne zaprojektowane rozwiązania, jak również rzeczywiste praktyki funkcjonujące w organizacji w celu prewencji zdarzeń lub redukcji skutków w przypadku zmaterializowania się ryzyka.
2) Skala oceny skuteczności wdrożonych mechanizmów kontroli ryzyka pozwala na ocenę działań zarządczych wdrożonych względem zidentyfikowanych ryzyk w zakresie bezpieczeństwa informacji. Skala przygotowana została w celu oceny możliwości wpłynięcia na wartość ryzyka poprzez podniesienie skuteczności aktualnie wdrożonych działań zarządczych (kontroli) względem zidentyfikowanych ryzyk w zakresie bezpieczeństwa informacji.
3) Wspólnej oceny wszystkich zastosowanych środków kontroli.
4) Skala oceny skuteczności środków kontroli przedstawia Tabela 3.

Tabela 2. Skuteczność środków kontroli

Skuteczność środków kontroli	
3	Wysoka skuteczność – środki zabezpieczają ryzyko w sposób adekwatny
2	Średnia skuteczność – środki częściowo zabezpieczają ryzyko, wymagają podjęcia działań doskonalących
1	Niska skuteczność – środki w ograniczonym zakresie zabezpieczają ryzyko, wymagają podjęcia działań naprawczych
0	Brak środków

Do przedstawienia **prawdopodobieństwa wystąpienia ryzyka bezpieczeństwa informacji** ustala się skalę punktową (Tabela 3).

Tabela 3. Prawdopodobieństwo wystąpienia ryzyka bezpieczeństwa informacji

Prawdopodobieństwo wystąpienia ryzyka		
Bardzo wysokie	**5**	Zdarzenie objęte ryzykiem z bardzo dużym prawdopodobieństwem wystąpi wcześniej czy później.
Wysokie	**4**	Zdarzenie z dużym prawdopodobieństwem wystąpi w pewnych okolicznościach. Jego wystąpienie nie powinno być zaskoczeniem.
Możliwe	**3**	Zdarzenie może wystąpić w pewnym momencie, ale może również w ogóle nie wystąpić. Materializacja ryzyka miała miejsce w podobnych komórkach/jednostkach w zbliżonych/analogicznych do występujących okolicznościach.
Niskie	**2**	Nie oczekuje się wystąpienia zdarzenia. Nie ma informacji, aby ryzyko mogło się zmaterializować.
Bardzo niskie	**1**	Zdarzenie prawie niemożliwe do wystąpienia. Może wystąpić tylko i wyłącznie w wyjątkowych okolicznościach.

Do przedstawienia **wpływu ryzyka bezpieczeństwa informacji** ustala się skalę punktową (Tabela 4). Jest to ocena dokonywana na bazie doświadczenia i posiadanej wiedzy.

Tabela 4. Wpływ ryzyka bezpieczeństwa informacji

	Skala	Przesłanki - dostępność	Przesłanki – bezpieczeństwo (poufność /integralność)
Wpływ ryzyka			
Bardzo duży	**5**	Zdarzenie objęte ryzykiem powoduje **krytyczne** zakłócenia lub opóźnienia w dostępnie do danych skutkujące opóźnieniem w realizacji zadań **powyżej 24 h**. Z wystąpieniem zdarzenia objętego ryzykiem wiąże się **długotrwały** i **trudny proces przywracania** stanu poprzedniego.	**Utrata poufności** danych (**na zewnątrz organizacji**) lub istotna utrata integralności danych wpływająca na podmioty zewnętrzne. Z wystąpieniem zdarzenia objętego ryzykiem wiąże się **długotrwały** i **trudny proces przywracania** integralności.
Duży	**4**	Zdarzenie objęte ryzykiem powoduje **krytyczne** zakłócenia lub opóźnienia w dostępnie do danych skutkujące opóźnieniem w realizacji zadań **od 8 do 24 h**. Z wystąpieniem zdarzenia objętego ryzykiem wiąże się **trudny proces przywracania** stanu poprzedniego.	**Utrata integralności** danych wpływająca na podmioty zewnętrzne. Z wystąpieniem zdarzenia objętego ryzykiem wiąże się **trudny proces przywracania** integralności.
Średni	**3**	Zdarzenie objęte ryzykiem powoduje **znaczące** zakłócenia lub opóźnienia w dostępnie do danych skutkujące opóźnieniem w realizacji zadań **od 2 do 8 h**. Skutki zdarzenia **można usunąć** (**długotrwały proces**).	**Zaburzenia poufności** danych o ograniczonym zasięgu (**wewnątrz organizacji**) lub istotne zaburzenie integralności danych (wewnątrz organizacji). Z wystąpieniem zdarzenia objętego ryzykiem wiąże się **długotrwały proces przywracania** integralności.
Mały	**2**	**Małe** zakłócenia lub opóźnienia w dostępnie do danych skutkujące opóźnieniem w realizacji zadań **do 2 h**. Skutki zdarzenia **można usunąć**.	**Zaburzenia integralności** danych o ograniczonym zasięgu (wewnątrz organizacji). Skutki zdarzenia **można usunąć**.
Bardzo mały	**1**	Nieznaczne zakłócenie lub opóźnienie w dostępie do danych, niepowodujące opóźnień w realizacji zadań Skutki zdarzenia **można łatwo usunąć**.	**Brak wpływu** na integralność i poufność danych. Skutki zdarzenia **można łatwo usunąć**.

Istotność ryzyka w przypadku szans, stanowi wartość prawdopodobieństwa jego wystąpienia. W tym przypadku nie stosuje się podziału na ryzyko inherentne i rezydualne. Obliczane jest jedynie ryzyko rezydualne.

Istotność ryzyka inherentnego bezpieczeństwa informacji stanowi kombinację (iloczyn) wyższej wartości wpływu ryzyka (Tabela 4), prawdopodobieństwa jego wystąpienia (Tabela 3) i oceny skuteczności środków kontroli powiększonej uprzednio o wartość „1". Istotność ryzyka inherentnego jest podzielona na 3 grupy oznaczone w Mapie ryzyka (Tabela 5) odrębnymi kolorami, z zastrzeżeniem, że dla nieakceptowalnych ryzyk inherentnych nie ma obowiązku opracowania planu postępowania z ryzykiem.

Takie przyjęcie wyliczenia Istotności ryzyka inherentnego uzasadnione jest z jednej strony możliwością popełnienia błędu przez osoby dokonujące eksperckiej oceny ryzyka – bardzo trudno nie uwzględnić jakichkolwiek zabezpieczeń, czego wymaga ocena ryzyka inherentnego, a z drugiej strony priorytetem, jak najbardziej rzetelnej oceny ryzyka rezydualnego, którego wartość jest najistotniejsza, ponieważ to jego wartość decyduje o konieczności wdrożenia postępowania z ryzykiem.

Istotność rezydualna ryzyka bezpieczeństwa informacji stanowi kombinację (iloczyn) wyższej wartości wpływu ryzyka (Tabela 4) i prawdopodobieństwa jego wystąpienia (Tabela 3). Istotność ryzyka rezydualnego jest podzielona na 3 grupy oznaczone w Mapie ryzyka (Tabela 5) odrębnymi kolorami.

Ryzyko poważne – nieakceptowalne – wymaga pilnej reakcji i podjęcia działań ograniczających istotność ryzyka (wartości od 15).

Ryzyko umiarkowane – należy omawiać na okresowych spotkaniach kierownictwa oraz spotkaniach wewnętrznych i monitorować (wartości od 5 do 12).

Ryzyko minimalne – to najniższe zagrożenie wymagające monitorowania (wartości do 4).

Ryzyka inherentne wspomagają ocenę poziomu skuteczności zastosowania środków kontroli przy ocenie ryzyka rezydualnego. Działania (pilna reakcja/omawianie na spotkaniach/monitorowanie) związane z postępowaniem z ryzykiem odnoszą się do ryzyk rezydualnych. W przypadku ryzyk rezydualnych sklasyfikowanych jako nieakceptowalne (poważne) należy opracować i wdrożyć plan postępowania z ryzykiem bezpieczeństwa informacji.

Tabela 5. Mapa ryzyka – matryca punktowej oceny istotności ryzyka bezpieczeństwa informacji

Wpływ	**Bardzo duży**	**5**	**10**	**15**	**20**	**25**
	Duży	**4**	**8**	**12**	**16**	**20**
	Średni	**3**	**6**	**9**	**12**	**15**
	Mały	**2**	**4**	**6**	**8**	**10**
	Bardzo mały	**1**	**2**	**3**	**4**	**5**
		Bardzo niskie	**Niskie**	**Możliwe**	**Wysokie**	**Bardzo wysokie**
		Prawdopodobieństwo				

III.4. Rejestr ryzyka

1. Wzór rejestru ryzyka bezpieczeństwa informacji stanowi załącznik nr 2 do niniejszych Zasad.
2. Prowadzenie rejestru ryzyka bezpieczeństwa informacji jest procesem ciągłym i odbywa się z zachowaniem kryteriów i skali określonych w niniejszej Metodyce oceny ryzyka bezpieczeństwa informacji.
3. Zgodnie z częstotliwością określoną w części I ust. 7 następuje przegląd ryzyk ujętych w rejestrze ryzyka bezpieczeństwa informacji, którego celem jest sprawdzenie aktualności i uzupełnienie dokonanych wpisów.
4. Wyciąg z rejestru ryzyka bezpieczeństwa informacji przekazywany jest Koordynatorowi ds. analizy ryzyka bezpieczeństwa informacji przez Właściciela ryzyka/Kierownika komórki organizacyjnej zarządzającej ryzykiem w imieniu Właściciela ryzyka bezpieczeństwa informacji za pośrednictwem poczty elektronicznej.
5. Wpisowi do wyciągu z rejestru ryzyka bezpieczeństwa informacji podlegają odpowiednio informacje określone w załączniku nr 2 do niniejszych Zasad.

III.5. Reakcja na ryzyko

1. W stosunku do każdego poważnego (nieakceptowalnego) ryzyka rezydualnego bezpieczeństwa informacji należy określić w rejestrze ryzyka sposób reakcji w postaci opisania Planu postępowania z ryzykiem, o którym mowa w części. III.1 ust. 4.

2. Wyróżnia się następujące rodzaje reakcji na ryzyko nieakceptowalne:

1) **zapobieganie ryzyka** (przeciwdziałanie) – podjęcie działań prowadzących do ograniczenia istotności ryzyka lub zapobiegających jego wystąpieniu, np. wprowadzenie dodatkowych mechanizmów kontrolnych w danym procesie;
2) **dzielenie ryzyka** (przeniesienie) – przeniesienie ryzyka na zewnątrz, np. na inną instytucję poprzez ubezpieczenie skutków lub zlecanie usług zewnętrznych;
3) **tolerowanie ryzyka** (akceptacja) – świadoma decyzja kontynuacji działań lub też nie podejmowanie działań pomimo występującego ryzyka, np. kiedy koszty przeciwdziałania ryzyku mogą przekroczyć jego potencjalne korzyści lub brak jest zdolności do skutecznego przeciwdziałania ryzyku;
4) **niwelacja ryzyka** (wycofanie się) – zakończenie działań związanych z dużym ryzykiem, gdy nie udało się obniżyć ryzyka do akceptowalnego poziomu, poprzez wycofanie z realizacji zadania w wyniku braku środków lub możliwości skutecznego przeciwdziałania, mając na uwadze, iż kontynuacja przyniosłaby większe negatywne skutki niż zaprzestanie działania.

Załącznik nr 1 do Zasad przeprowadzania analizy ryzyka bezpieczeństwa informacji

Raport z zarządzania ryzykiem za okres [kwartał/rok]

Opracował Koordynator: **Akceptował Przewodniczący Zespołu:**

Data i podpis **Data i podpis**

1. Działania rekomendowane przez Zespół ds. zarządzania ryzykiem bezpieczeństwa informacji

.....

.....

.....

.....

2. Opis zmian w stosunku do poprzedniego zbiorczego rejestru ryzyka.

2.1 Postępy w wdrożeniu planów postępowania z ryzykiem nieakceptowalnym zidentyfikowanych w poprzednich iteracjach analizy i oceny ryzyka.

Nazwa aktywa	Nazwa ryzyka	Właściciel ryzyka/Kierownik komórki organizacyjnej zarządzającej ryzykiem	Plan postępowania z ryzykiem	Stan realizacji, efekty, uzasadnienie

2.2 Ryzyka zidentyfikowane w bieżącej iteracji analizy i oceny ryzyka jako nieakceptowalne.

Nazwa aktywa	Nazwa ryzyka	Właściciel ryzyka/Kierownik komórki organizacyjnej zarządzającej ryzykiem	Wartość ryzyka	Uwagi Zespołu