Załącznik do Zarządzenia Nr 20/2024
Dyrektora Centrum Informatycznych Usług Wspólnych Olsztyna
z dnia 17 czerwca 2024 r. w sprawie zmiany Zarządzenia nr 32/2019
Dyrektora Centrum Informatycznych Usług Wspólnych Olsztyna
z dnia 4 grudnia 2019 r. w sprawie wprowadzenia regulaminu
zarządzania ryzykiem w Centrum Informatycznych Usług Olsztyna

REGULAMIN
ZARZĄDZANIA RYZYKIEM
W CENTRUM INFORMATYCZNYCH
USŁUG WSPÓLNYCH OLSZTYNA

Signed by / Podpisano przez:
Paweł Maciej Witkowski
Date / Data: 2024-06-17 16:01

Spis treści

Rozdział 1. Założenia ogólne

§ 1. Zarządzanie ryzykiem jest procesem ciągłym, stanowiącym jeden z elementów systemu kontroli zarządczej, obejmującej ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy.

§ 2. Funkcjonowanie systemu kontroli zarządczej w Centrum Informatycznych Usług Wspólnych Olsztyna (dalej CIUWO), o którym mowa w § 1, a także poszczególne jego elementy określone zostały w Regulaminie funkcjonowania systemu kontroli zarządczej w CIUWO.

§ 3. Regulamin zarządzania ryzykiem opisuje przyjęty dla CIUWO model zarządzania ryzykiem.

§ 4. Niniejszy dokument jest zbiorem zasad realizacji procesu zarządzania ryzykiem w kontroli zarządczej, zarządzaniu usługami IT oraz bezpieczeństwie informacji zgodnie z wytycznymi normy PN-ISO/IEC 27005, a także ochronie danych osobowych zgodnie z ogólnym rozporządzeniem o ochronie danych.

§ 5. Ilekroć w regulaminie jest mowa o:

1) Centrum lub CIUWO - należy przez to rozumieć Centrum Informatycznych Usług Wspólnych Olsztyna,

2) Dyrektorze – należy przez to rozumieć Dyrektora CIUWO,

3) Kierownictwie – należy przez to rozumieć Dyrektora, Zastępcę Dyrektora oraz Głównego Księgowego,

4) danych osobowych – należy przez to rozumieć dane w rozumieniu art. 4 pkt 1 ogólnego rozporządzenia o ochronie danych,

5) ryzyku - należy przez to rozumieć prawdopodobieństwo wystąpienia zdarzenia mającego negatywny wpływ na wykonywanie zadań bądź osiąganie celów,

6) ryzyku w bezpieczeństwie informacji – należy przez to rozumieć wartość zależną od wysokości potencjalnych strat wynikających z niewłaściwego przetwarzania informacji i od prawdopodobieństwa wystąpienia takich strat,

7) cyberbezpieczeństwie – należy przez to rozumieć odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

8) wpływie ryzyka - należy przez to rozumieć skutki dla realizowania zadań i osiągania celów spowodowane przez zdarzenie objęte ryzykiem,

9) prawdopodobieństwie wystąpienia ryzyka - należy przez to rozumieć częstotliwość występowania zdarzenia objętego ryzykiem,

10) istotności ryzyka - należy przez to rozumieć kombinację wpływu ryzyka i prawdopodobieństwa jego wystąpienia,

11) akceptowalnym poziomie ryzyka - należy przez to rozumieć ustalony poziom istotności ryzyka, przy którym nie jest wymagane podejmowanie działań przeciwdziałających ryzyku,

12) zarządzaniu ryzykiem - należy przez to rozumieć proces identyfikacji, oceny i przeciwdziałania ryzyku; proces ten obejmuje także monitorowanie ryzyka i środków podejmowanych w celu jego ograniczenia w kontroli zarządczej, zarządzaniu usługami IT oraz bezpieczeństwie informacji, a także ochronie danych osobowych,

13) mechanizmach kontroli - należy przez to rozumieć wszystkie działania i procedury podejmowane lub ustanawiane w celu zwiększenia prawdopodobieństwa realizacji zadań i osiągania celów, w tym zwłaszcza:

    a) dokumentację systemu zarządzania bezpieczeństwem informacji (w szczególności procedury, instrukcje, wytyczne),
    b) dokumentowanie poszczególnych zdarzeń,
    c) zatwierdzanie operacji,
    d) podział obowiązków,
    e) nadzór,
    f) rejestrowanie istotnych odstępstw od zasad zapisanych w procedurach, instrukcjach czy wytycznych,

14) aktywach i zasobach informacyjnych – należy przez to rozumieć wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością CIUWO lub wykorzystywane bądź administrowane,

15) właścicielu aktywa i zasobu informacyjnego – należy przez to rozumieć kierowników/ koordynatorów komórek organizacyjnych oraz pracowników na stanowiskach określonych w strukturze organizacyjnej CIUWO,

16) poufności informacji – należy przez to rozumieć atrybut bezpieczeństwa aktywa informacyjnego oznaczający, że dostęp do informacji powinny mieć jedynie osoby uprawnione,

17) integralności – należy przez to rozumieć atrybut bezpieczeństwa aktywa i zasobu informacyjnego określający jakość informacji w aspekcie kompletności, spójności i wiarygodności danych,

18) dostępności – należy przez to rozumieć atrybut bezpieczeństwa aktywa i zasobu informacyjnego oznaczający łatwość przetwarzania informacji osób uprawnionych wtedy, kiedy potrzebują ich przetwarzania,

19) podatności – należy przez to rozumieć wady, luki lub słabości w strukturze fizycznej, organizacji działania CIUWO, procedurach, personelu, zarządzaniu, administrowaniu, sprzęcie lub oprogramowaniu (zasobu lub grupy zasobów), które mogą być wykorzystane przez zagrożenie do spowodowania strat,

20) zagrożeniu informacji – należy przez to rozumieć potencjalne działanie wobec aktywa i zasobu informacyjnego lub procesu, mogące wykorzystać określoną podatność, w celu spowodowania strat,

21) incydencie - należy przez to rozumieć zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo,

22) prawdopodobieństwie wystąpienia zagrożenia – należy przez to rozumieć potencjalną możliwość lub częstość występowania zagrożenia,

23) skutku wystąpienia zagrożenia - należy przez to rozumieć rezultat zdarzenia (wystąpienie lub zmiana konkretnego zestawu okoliczności; zdarzenie może być określone również jako incydent), mający negatywny wpływ na cele,

24) ogólnym rozporządzeniu o ochronie danych - należy przez to rozumieć Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie

ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z 27 kwietnia 2016 r.,

Rozdział 2. Ogólne zasady zarządzania ryzykiem

§ 6. Celem zarządzania ryzykiem jest:
1) usprawnienie procesu planowania,
2) zwiększenie prawdopodobieństwa realizacji zadań i osiągania celów,
3) zapewnienie odpowiednich mechanizmów kontroli zarządczej,
4) zapewnienie Kierownictwu otrzymywania na czas wczesnej informacji na temat zagrożeń dla realizacji celów i zadań,
5) uzyskanie bezpieczeństwa informacji, w tym danych osobowych na adekwatnym poziomie,
6) zwiększenie poziomu cyberbezpieczeństwa,
7) podnoszenie jakości świadczonych usług IT.

§ 7. Zarządzanie ryzykiem wewnętrznym odbywa się w szczególności według zasad:
1) spójności z przepisami prawa oraz wytycznymi w zakresie standardów kontroli zarządczej w jednostkach sektora finansów publicznych,
2) powiązania z celami i zadaniami CIUWO,
3) przypisania odpowiedzialności,
4) proporcjonalności działań przeciwdziałających ryzyku do jego istotności.

Rozdział 3. Elementy systemu zarządzania ryzykiem

§ 8. Zarządzanie ryzykiem obejmuje:
1) identyfikację ryzyka,
2) ocenę ryzyka, mającą na celu określenie możliwych skutków, prawdopodobieństwa i istotności wystąpienia danego ryzyka,
3) określenie akceptowanego poziomu ryzyka,
4) określenie reakcji na ryzyko i wskazanie działań w celu zmniejszenia danego ryzyka do akceptowanego poziomu ze wskazaniem właścicieli ryzyk,
5) zapewnienie mechanizmów kontroli ryzyka,
6) wdrożenie środków zapobiegawczych i korygujących oraz monitorowanie i raportowanie.

Rozdział 4. Identyfikacja ryzyka

§ 9. Identyfikacja ryzyka polega na określeniu ryzyka, które zagraża poszczególnym celom i zadaniom, realizowanym przez CIUWO oraz ustaleniu ryzyk zagrażających utracie poufności, integralności, dostępności i rozliczalności aktywów (w tym m.in. informacji, danych osobowych, sprzętu) oraz ryzyk zagrażających bezpieczeństwu sieci i systemów informatycznych. Przy identyfikacji zagrożeń uwzględnia się też realizowane przez CIUWO programy oraz projekty.

§ 10. Identyfikując ryzyko, analizuje się wyniki wcześniej przeprowadzonych kontroli lub audytów oraz przypadki nieprawidłowości i niepowodzeń w osiąganiu celów CIUWO w przeszłości.

§ 11. Podczas identyfikacji należy przeanalizować:
1) cele i zadania CIUWO,
2) obszary działalności CIUWO,
3) zasoby/aktywa informacyjne CIUWO i zarządzane przez CIUWO,

4) zagrożenia związane z utratą poufności, integralności, rozliczalności i dostępności do informacji i danych, w tym danych osobowych,
5) zagrożenia związane z utratą bezpieczeństwa sieci i systemów informatycznych,
6) zagrożenia związane z osiąganiem celów i realizowaniem zadań, w szczególności wynikające z następujących czynników:
   a) struktury organizacyjnej,
   b) sytuacji finansowej CIUWO, w tym: liczby, rodzaju i wielkości dokonywanych operacji finansowych,
   c) liczby pracowników oraz ich kwalifikacji,
   d) przestrzegania przez pracowników zasad etyki,
   e) warunków pracy w CIUWO,
   f) wpływów/nacisków zewnętrznych na pracowników CIUWO (zwłaszcza o charakterze korupcyjnym lub innym kryminogennym),
   g) możliwości zaistnienia zmian (np. zakresu rzeczowego lub terytorialnego działania jednostki, struktury organizacyjnej, sposobu działania, fluktuacji kadr, systemów informatycznych).

Rozdział 5. Ocena ryzyka

§ 12. Ocena ryzyka odbywa się na podstawie przyjętego modelu oceny zapewniającego porównywalność wyników we wszystkich obszarach funkcjonowania jednostki oraz ułatwiającego przetwarzanie indywidualnych ocen w celu stworzenia ogólnego profilu ryzyka, z uwzględnieniem procedury identyfikacji i klasyfikacji aktywów i zasobów informacyjnych oraz zarządzania ryzykiem w bezpieczeństwie informacji, w tym danych osobowych.

§ 13. Ocena ryzyka polega na określeniu prawdopodobieństwa wystąpienia ryzyka i wpływie zagrożenia, a następnie ustaleniu jego istotności.

§ 14. Ocena zarówno prawdopodobieństwa, jak i potencjalnego wpływu zagrożenia wystąpienia ryzyka polega na nadaniu im wartości szacunkowych w przyjętych skalach jakościowo-ilościowych.

§ 15. W ocenie ryzyka uwzględnia się częstotliwość zaistnienia ryzyka (liczbę możliwych powtórzeń) jako jeden ze wskaźników prawdopodobieństwa wystąpienia ryzyka.

§ 16. Na podstawie oszacowanego prawdopodobieństwa oraz wpływu zagrożenia wystąpienia ryzyka określa się współczynnik istotności każdego zidentyfikowanego ryzyka.

§ 17. Określenie istotności ryzyka umożliwia uporządkowanie ryzyk według kryterium ich znaczenia dla realizacji celów i zadań jednostki.

§ 18. Pogrupowanie ryzyk według kryterium ich istotności przedstawia rzeczywiste zagrożenia dla realizacji celów i zadań CIUWO oraz wskazuje Dyrektorowi CIUWO kierunki priorytetowe w podejmowaniu odpowiednich działań.

§ 19. Dla poszczególnych zidentyfikowanych i oszacowanych ryzyk wskazuje się rozwiązania, które mają na celu ograniczenie prawdopodobieństwa lub wpływu zagrożenia ich wystąpienia.

§ 20. Dyrektor CIUWO wyznacza akceptowany poziom ryzyka, uwzględniając ocenę istotności ryzyka.

§ 21. Określenie poziomu istotności ryzyka może wynikać m.in. z konieczności zaakceptowania ryzyka w obszarze, w którym długofalowe korzyści przewyższają krótkoterminowe straty, z uwzględnieniem aktualnej sytuacji CIUWO oraz wysokości kosztów ograniczenia danego ryzyka.

Rozdział 6. Prawdopodobieństwo wystąpienia ryzyka

§ 22. Oceniając prawdopodobieństwo wystąpienia ryzyka, uwzględnia się możliwą częstotliwość wystąpienia zdarzenia/ incydentu (jak często dane zdarzenie może mieć miejsce). W odniesieniu do czynności powtarzalnych (spraw występujących cyklicznie lub wielokrotnie) uwzględnia się liczbę możliwych powtórzeń (ile razy względem ogólnej liczby spraw zdarzenie może mieć miejsce).

§ 23. Jakościowa ocena prawdopodobieństwa wystąpienia ryzyka opiera się na oszacowaniu stopnia prawdopodobieństwa zaistnienia ryzyka. Dla każdego zdarzenia, w wyniku którego może zrealizować się rozpatrywane ryzyko należy dobrać odpowiednie wartości prawdopodobieństwa. Podczas oceny prawdopodobieństwa wystąpienia zagrożenia wykorzystującego wskazaną podatność w celu spowodowania strat, należy uwzględniać nie tylko potencjalne zajście zdarzenia w przyszłości, lecz również sytuacje z przeszłości.

1) Dla każdego prawdopodobieństwa należy dobrać wartości zgodnie z poniższą tabelą:

Wartość	**Prawdopodobna częstotliwość wystąpienia**	**Opis prawdopodobieństwa wystąpienia**
4	prawie pewne	Ryzyko z pewnością wystąpi w ciągu najbliższego okresu. W ciągu ostatniego roku obszar /proces podlegał istotnym zmianom technologicznym, organizacyjnym i kadrowym/ podlega częstym zmianom technologicznym, organizacyjnym i kadrowym / jest w trakcie zmian technologicznych, organizacyjnych i kadrowych. Obszar /proces uregulowany jest dużą liczbą aktów prawnych (wewnętrznych i zewnętrznych). Zagrożenia naruszają bezpieczeństwo danych, a przede wszystkim prawa lub wolność osób fizycznych. Realizacja raz w tygodniu.
3	prawdopodobne	Istnieje duże prawdopodobieństwo na wystąpienie ryzyka w ciągu najbliższego okresu. W ciągu ostatniego roku obszar /proces podlegał zmianom technologicznym, organizacyjnym lub kadrowym, z których część może wymagać poprawek i działań dostosowawczych. Obszar/proces objęty dużą liczbą regulacji prawnych zewnętrznych i wewnętrznych. Zagrożenia mogą wywierać istotny wpływ na naruszenie praw lub wolności osób fizycznych i bezpieczeństwo. Realizacja raz na trzy miesiące.
2	możliwe	Ryzyko prawdopodobnie wystąpi w najbliższym okresie. W ciągu ostatniego roku obszar /proces podlegał ograniczonym zmianom organizacyjnym, technologicznym i kadrowym. Obszar/proces objęty w małym stopniu regulacjami zewnętrznymi, które mogły podlegać w ostatnim okresie zmianom. Zagrożenia mogą wywierać średni wpływ na naruszenie praw lub wolności osób fizycznych i bezpieczeństwo. Może dotyczyć zadań o istotnym znaczeniu dla celów działalności. Realizacja raz na rok.
1	mało prawdopodobne	Ryzyko prawdopodobnie nie wystąpi. W ostatnim okresie (np. 1 rok) obszar/proces nie podlegał zmianom technologicznym, organizacyjnym i kadrowym, bądź podlegał zmianom w minimalnym stopniu i uznaje się je za wdrożone. Obszar/proces w małym zakresie objęty regulacjami o charakterze zewnętrznym. Nie podlegały one zmianom. Zagrożenia mogą wywierać niewielki wpływ na naruszenie praw lub wolności osób fizycznych i bezpieczeństwo. Niepożądane zakłócenia mogą

		powodować utrudnienia w realizacji zadań. Potencjalne zakłócenia wykonywania zadań nie mają wpływu na realizację celów. Realizacja raz na dwa lata.
0	rzadkie	Ryzyko nie występuje lub może wystąpić w zupełnie wyjątkowych sytuacjach. Nie wprowadzono w ostatnim roku istotnych zmian technologicznych, organizacyjnych i kadrowych. Przetwarzanie danych i jego zakresu określają zewnętrzne regulacje prawne. Mniej niż raz na dwa lata.

2) **Uwaga.** Dla niektórych sytuacji przyjmuje się niezerowe wartości prawdopodobieństwa, pomimo, że sytuacja występuje niezmiernie rzadko. Przykładem są: klęski żywiołowe, katastrofy naturalne, pożar, powódź.

Rozdział 7. Wpływ zagrożenia wystąpienia ryzyka

§ 24. Ocena wpływu zagrożenia wystąpienia ryzyka opiera się na oszacowaniu potencjalnych skutków, a więc wyników oddziaływania, jakie zaistnienie danego rodzaju ryzyka może mieć wpływ na realizację celów oraz zadań (jakość rezultatów/znaczenia/wpływów). Uwzględnia się przy tym, w szczególności konsekwencje prawne, finansowe i organizacyjne zaistnienia danego zdarzenia oraz jego wpływ na realizację celów i zadań, wizerunek jednostki, bezpieczeństwo pracowników oraz bezpieczeństwo informacji, cyberbezpieczeństwo i ochronę danych osobowych.

§ 25. Ocenę wpływu zagrożenia zaistnienia ryzyka, wykonuje się według skali numerycznej od 0 do 4, gdzie 4 oznacza najwyższą wagę. Do oceny wartości zasobów przyjęto Tabelę Istotności Zasobów o 5-cio stopniowej skali wartości. Wartość 4 oznacza największą istotność.

Wartość	**Skala skutków**	**Opis oddziaływania (skutków)**
4	bardzo wysokie	Bardzo poważny wpływ na realizację zadania (poważne zagrożenie terminu jego realizacji) i osiągnięcie celu; poważne konsekwencje prawne; zagrożenie bezpieczeństwa pracowników; bardzo poważne zagrożenie bezpieczeństwa dla informacji i danych osobowych; zagrożenia spowodują brak zachowania ciągłości procesów działania, utrzymania funkcjonalności systemów niezbędnych do wykonywania podstawowych celów; brak odpowiednich mechanizmów kontrolnych bądź istniejące mechanizmy okazują się nieskuteczne; poważne straty finansowe; poważny wpływ na wizerunek jednostki;
3	poważne	Poważny wpływ na realizację zadania (zagrożenie terminu jego realizacji) i osiągnięcie celu; zagrożenie bezpieczeństwa pracowników; niezgodność z przepisami prawa lub poważna niezgodność z postanowieniami umów; poważne naruszenie zasad przetwarzania danych w tym danych osobowych, mogące doprowadzić do utraty bezpieczeństwa przetwarzania danych w tym danych osobowych; niska skuteczność istniejących mechanizmów kontrolnych, umiarkowane straty finansowe; umiarkowany wpływ na wizerunek jednostki;

Wartość	Skala skutków	Opis oddziaływania (skutków)
2	średnie	Średni wpływ na realizację zadania (zagrożenie terminu jego realizacji) i osiągnięcie celu; niezgodność z przepisami prawa lub średnia niezgodność z postanowieniami umów lub średnia niezgodność z procedurami; możliwe konsekwencje prawne; możliwy wpływ na bezpieczeństwo informacji i danych w tym danych osobowych; brak wpływu na bezpieczeństwo pracowników; możliwy wpływ na wizerunek jednostki; możliwy skutek finansowy; istniejące mechanizmy kontrolne tylko w pewnym stopniu mogą ograniczyć skutki ewentualnych zakłóceń;
1	niskie	Mały wpływ na realizację zadania i osiągnięcie celu; brak skutków prawnych; mały skutek finansowy; brak wpływu na bezpieczeństwo pracowników; brak wpływu na bezpieczeństwo informacji i danych w tym danych osobowych; istniejące mechanizmy kontrolne powinny ograniczyć skutki ewentualnych zakłóceń; niewielki wpływ na wizerunek jednostki;
0	nieznaczne	Brak wpływu na realizację zadania i osiągnięcie celu; niska niezgodność z procedurami/przepisami prawa, brak skutków prawnych; nie występuje zagrożenie utraty dobrego wizerunku; brak skutku finansowego; brak wpływu na bezpieczeństwo pracowników; brak wpływu na bezpieczeństwo informacji i danych, w tym danych osobowych; brak wpływu na wizerunek jednostki; brak konieczności stosowania zabezpieczeń w danym obszarze.

Ocena ryzyka dotyczy wszystkich obszarów funkcjonowania CIUWO. Przy czym podczas oceny, która dotyczy obszaru zarządzania usługami IT oraz bezpieczeństwa informacji (w tym ochrony danych osobowych) zgodnie z wytycznymi normy PN-ISO/IEC 27005 bierze się pod uwagę wpływ na poufność, integralność oraz dostępność aktywa i zasobu informacyjnego oraz wartość aktywa i zasobu informacyjnego.

Ryzyko utraty jakości usług IT oraz bezpieczeństwa dla aktywów i zasobów informacyjnych należy obliczać posługując się „Arkuszem identyfikacji, oceny oraz określenia metody przeciwdziałaniu ryzyku" stanowiącym załącznik nr 1 do regulaminu. W celu wykonania analizy należy dobrać wartości odpowiednich parametrów zgodnie z definicjami.

Rozdział 8. Istotność ryzyka

§ 26. Istotność ryzyka wyrażona jest jako iloczyn (wyrażonych punktowo) prawdopodobieństwa wystąpienia ryzyka oraz potencjalnych skutków jego wystąpienia. Określenie istotności ryzyka pozwala na dokonanie oceny i hierarchizacji ryzyka, tj. uporządkowanie zidentyfikowanych i oszacowanych rodzajów ryzyka ze względu na ich znaczenie (od najpoważniejszych do najmniej poważnych rodzajów ryzyka), w zależności od stopnia, w jakim dane ryzyko zagraża realizacji zadań i celów CIUWO i/lub bezpieczeństwu informacji i danych, w tym danych osobowych.

§ 27. Z uwagi na pięciostopniową skalę zarówno prawdopodobieństwa, jak i skutków wystąpienia ryzyka, istotność danego rodzaju ryzyka może przyjąć wartości liczbowe od 0 do 96.

Należy przyjąć poziom ryzyka akceptowalnego dla każdego z obszarów lub procesów CIUWO, lub przyjąć globalną wartość ryzyka akceptowalnego. Wynik porównania wartości ryzyk dla

zagrożeń i wartości ryzyka akceptowalnego jest podstawą procesu zarządzania ryzykiem, w którym powinno się reagować na ryzyka ponad akceptowalne na kilka sposobów np. stosując dodatkowe zabezpieczenia.

W przyjętym modelu należy kierować się poniższą ogólną mapą ryzyka.

Skutki dla organizacji	**Prawdopodobieństwo scenariusza zdarzenia**			
	Niskie	**Średnie**	**Wysokie**	**Bardzo wysokie**
Bardzo wysokie	19-24	25-48	49-72	Powyżej 72
Wysokie	13-18	19-24	25-48	49-72
Średnie	7-12	13-18	19-24	25-48
Niskie	1-6	7-12	13-18	19-24

Dla poszczególnych obszarów mapa ryzyka przedstawia się następująco:

Skutki dla organizacji	**Prawdopodobieństwo scenariusza zdarzenia**			
	Niskie	**Średnie**	**Wysokie**	**Bardzo wysokie**
Bardzo wysokie	4	8	12	16
Wysokie	3	6	9	12
Średnie	2	4	6	8
Niskie	1	2	3	4

Ryzyka w kolorze niebieskim należy monitorować, czy nie zbliżają się do kolejnego obszaru. Kolorem pomarańczowym zaznaczono te ryzyka, którymi należy zająć się w dłuższym okresie. Natomiast kolorem czerwonym zaznaczono te ryzyka, którymi należy zająć się natychmiast.

Rozdział 9. Akceptowany poziom ryzyka

§ 28. Ryzykiem akceptowalnym przyjętym w CIUWO jest ryzyko o niskim poziomie istotności oznaczone kolorem białym.

§ 29. Ryzyko o średnim (oznaczone kolorem niebieskim) i wysokim (oznaczone kolorem pomarańczowym) poziomie istotności przekracza akceptowalny poziom ryzyka i wymaga ustalenia i podjęcia działań ograniczających to ryzyko przez zmniejszenie jego skutku lub prawdopodobieństwa wystąpienia ryzyka.

§ 30. Ryzyko o bardzo wysokim poziomie istotności oznaczone kolorem czerwonym wymaga natychmiastowego ustalenia i podjęcia działań ograniczających to ryzyko przez zmniejszenie jego skutku lub prawdopodobieństwa wystąpienia ryzyka.

§ 31. W stosunku do każdego rodzaju ryzyka, którego poziom istotności mieści się w akceptowanym dla CIUWO poziomie ryzyka, można również wskazać odpowiednie działania służące wdrożeniu określonego rodzaju reakcji na ryzyko.

Rozdział 10. Rodzaj reakcji na ryzyko i wyznaczenie właściciela ryzyka

§ 32. Metodami przeciwdziałania ryzyku są:

1) **kontrolowanie i ograniczanie ryzyka (K)** – działanie w celu zmniejszenia ryzyka. Przykładem tej formy jest stosowanie mechanizmów kontroli zarządczej lub też wprowadzenie dodatkowych procedur kontrolnych w danym procesie. Jest to podstawowy rodzaj reakcji na ryzyko,
2) **przeniesienie ryzyka (P)** – przekazanie ryzyka podmiotowi zewnętrznemu. Najczęściej przybiera formę ubezpieczenia lub zatrudnienia innego podmiotu do dokonywania określonych działań i przejęcia ryzyka za wynagrodzeniem,
3) **zakończenie działań obarczonych ryzykiem wewnętrznym (Z)** – polega na wycofaniu się z danego rodzaju działalności,
4) **tolerowanie ryzyka (T)** – świadome podjęcie ryzyka, brak dodatkowych działań, najczęściej wynika z ograniczenia możliwości podjęcia określonych działań albo zbyt wysokich kosztów ewentualnych działań w stosunku do potencjalnych korzyści. Forma ta może być uzupełniona przez plany awaryjne.

§ 33. W celu przeanalizowania określenia metody przeciwdziałania ryzyku należy przeanalizować:

1) przyczyny (źródła) ryzyka i możliwe scenariusze rozwoju wydarzeń,
2) istniejące mechanizmy kontrolne stosowane w celu ograniczenia lub uniknięcia tego ryzyka,
3) skuteczność istniejących mechanizmów kontroli, tj. zakres, w jakim przeciwdziałają ryzyku, a poprzez to ułatwiają lub utrudniają realizację ustalonych celów i zadań.

Rozdział 11. Odpowiedzialność

§ 34. Zapewnienie funkcjonowania systemu zarządzania ryzykiem należy do zadań Dyrektora CIUWO.

§ 35. Kierownicy/koordynatorzy komórek organizacyjnych dokonują identyfikacji ryzyka, oceny ryzyka oraz określenia metod przeciwdziałania ryzyku, na etapie opracowywania propozycji planu działania CIUWO, wypełniając „Arkusz identyfikacji, oceny oraz określenia metody przeciwdziałaniu ryzyku", według wzoru zamieszczonego w załączniku nr 1.

§ 36. W ramach systemu zarządzania bezpieczeństwem informacji kierownicy/koordynatorzy komórek organizacyjnych CIUWO postępują zgodnie z wytycznymi Procedury identyfikacji i klasyfikacji aktywów i zasobów informacyjnych oraz zarządzania ryzykiem, tj.:

1) dokonują identyfikacji i klasyfikacji informacji,
2) dokonują oceny ryzyk (przeprowadzają analizę ryzyka oraz opracowują plany postępowania z ryzykiem dla zagrożeń o ryzyku większym niż ustalony poziom ryzyka akceptowalnego),
3) identyfikują zagrożenia i podatności,
4) dobierają rodzaje zabezpieczeń,
5) szacują ryzyko (w trzech niezależnych aspektach: poufności, integralności i dostępności).

§ 37. W ramach zapewnienia ochrony danych osobowych kierownicy/koordynatorzy komórek organizacyjnych CIUWO:

1) identyfikują kontekst przetwarzania danych osobowych oraz samego ryzyka dla danych osobowych i zasobów biorących udział procesie analizy ryzyka,

2) przeprowadzają analizę operacji przetwarzania oraz oceniają, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
3) szacują prawdopodobieństwo wystąpienia zdefiniowanych rodzajów ryzyka, a także określają wartości prawdopodobnych strat (skutku wystąpienia zdarzenia) oraz dokonują analizy ryzyka.

§ 38. Oceniając ryzyko w zakresie bezpieczeństwa danych osobowych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych osób, których dane dotyczą.

§ 39. W ramach ochrony danych osobowych Inspektor Ochrony Danych uczestniczy w procesie identyfikacji ryzyka, weryfikuje rejestr ryzyka i przedstawia w razie konieczności zalecenia w kontekście ochrony danych osobowych.

§ 40. Koordynacja zadań związanych z zarządzaniem ryzykiem w CIUWO, należy do kompetencji Zespołu ds. Organizacji.

§ 41. W odniesieniu do każdego ryzyka ustalany jest właściciel ryzyka.

§ 42. Wszyscy pracownicy CIUWO zobowiązani są do aktywnego udziału w zarządzaniu ryzykiem, w szczególności przez:
1) stosowanie się do obowiązujących w CIUWO regulacji w zakresie zarządzania ryzykiem,
2) bieżące identyfikowanie ryzyka i informowanie o nim przełożonych,
3) podejmowanie działań w celu zminimalizowania skutków ryzyka lub prawdopodobieństwa jego wystąpienia.

§ 43. Rola audytu wewnętrznego/ kontroli wewnętrznej w procesie zarządzania ryzykiem obejmuje:
1) dokonywanie oceny adekwatności, skuteczności i efektywności systemu zarządzania ryzykiem w obszarach objętych zadaniami zapewniającymi,
2) świadczenie usług o charakterze doradczym z zachowaniem zasady niezależności i obiektywizmu,
3) wspieranie Dyrektora CIUWO w usprawnianiu procesu zarządzania ryzykiem.

Rozdział 12. Rejestr ryzyka

§ 44. Zbiorcza informacja na temat ryzyk przedstawiana jest w formie rejestru ryzyka, sporządzonego według wzoru określonego w załączniku nr 1 do niniejszego dokumentu.

§ 45. Rejestr ryzyka podlega zatwierdzeniu przez Dyrektora CIUWO.

§ 46. Dyrektor CIUWO, zatwierdzając rejestr ryzyka, podejmuje decyzję o:
1) rodzaju reakcji na ryzyko w stosunku do każdego ryzyka,
2) rodzaju działań zapobiegawczych lub korygujących mających przeciwdziałać wystąpieniu danego ryzyka,
3) częstotliwości raportowania, w zależności od poziomu istotności ryzyka.

§ 47. Zatwierdzony przez Dyrektora CIUWO rejestr ryzyka jest jawny dla wszystkich pracowników jednostki.

Rozdział 13. Terminy i tryb pracy

§ 48. Identyfikacja, analiza i ocena ryzyka oraz ustalenie metod przeciwdziałania ryzyku dokonywane są raz w roku, podczas przygotowania propozycji do rocznego planu działania CIUWO na rok następny.

§ 49. Wstępnej identyfikacji, analizy i oceny ryzyka oraz ustalenia metod przeciwdziałania ryzyku dokonują kierujący komórkami organizacyjnymi CIUWO.

§ 50. Wyniki oceny, o której mowa w § 48 i § 49, przedkładane są Koordynatorowi Zespołu ds. Organizacji w terminie i formie przez niego określonej, celem sporządzenia przez niego informacji zbiorczej

§ 51. Koordynator Zespołu ds. Organizacji przedkłada informację zbiorczą zawierającą propozycje kierowników komórek organizacyjnych Dyrektorowi CIUWO celem akceptacji.

§ 52. Kierujący komórkami organizacyjnymi, w przypadku istotnych zmian warunków funkcjonowania podległych im komórek, zobowiązani są do dokonywania w ciągu roku aktualizacji zidentyfikowanych ryzyk oraz informowania o tym Koordynatora Zespołu ds. Organizacji.

Rozdział 14. Monitorowanie i raportowanie

§ 53. Monitorowanie ryzyka jest procesem ciągłym, realizowanym na każdym szczeblu zarządzania, pozwalającym na podejmowanie decyzji przez Dyrektora CIUWO w odpowiednim czasie.

§ 54. W ramach monitoringu dokonywany jest przegląd aktualności ryzyk, adekwatności ich oceny, podjętych działań oraz skuteczności mechanizmów kontroli i identyfikacja nowych ryzyk.

§ 55. Zidentyfikowane ryzyko oraz ustalone metody jego ograniczania są na bieżąco oceniane przez:

1) kierujących komórkami organizacyjnymi, którzy oceniają poziom zidentyfikowanego ryzyka oraz skuteczność stosowanych metod jego ograniczania,
2) Kierownictwo CIUWO – w ramach bieżącego zarządzania Centrum, w tym w szczególności w trakcie narad z kierującymi komórkami organizacyjnymi.

§ 56. Kierujący komórkami organizacyjnymi:

1) do 15 kwietnia, 15 lipca, 15 października oraz 15 stycznia przekazują do Koordynatora Zespołu ds. Organizacji informację dotyczącą oceny ryzyk o bardzo wysokim poziomie istotności. Ocena dotyczy poprzedzającego ją kwartału (styczeń-marzec, kwiecień-czerwiec, lipiec-wrzesień, październik-grudzień) i zawiera w szczególności ocenę skuteczności zaproponowanych (przyjętych) metod przeciwdziałania ryzyku oraz wpływu tych metod na poziom istotności ryzyka.

2) do dnia 15 lipca i 15 stycznia przekazują do Koordynatora Zespołu ds. Organizacji informację dotyczącą oceny ryzyk o wysokim poziomie istotności. Ocena dotyczy poprzedzającego ją półrocza (styczeń-czerwiec, lipiec-grudzień) i zawiera w szczególności ocenę skuteczności zaproponowanych (przyjętych) metod przeciwdziałania ryzyku oraz wpływu tych metod na poziom istotności ryzyka.

§ 57. Koordynator Zespołu ds. Organizacji niezwłocznie przekazuje Dyrektorowi informację zbiorczą dotyczącą informacji, o których mowa w § 56.

§ 58. Kierujący komórkami organizacyjnymi, w przypadku istotnych zmian warunków funkcjonowania podległych im komórek, zobowiązani są również do dokonywania na bieżąco, w trakcie roku kalendarzowego aktualizacji zidentyfikowanych ryzyk.

§ 59. Kierujący komórkami organizacyjnymi do 15 stycznia każdego roku przekazują do Koordynatora Zespołu ds. Organizacji informację dotyczącą oceny ryzyk zidentyfikowanych w roku poprzednim, zawierającą w szczególności ocenę skuteczności zaproponowanych (przyjętych) metod przeciwdziałania ryzyku oraz wpływu tych metod na poziom istotności ryzyka.

§ 60. Na podstawie uzyskanych informacji, o których mowa w § 59, Koordynator Zespołu ds. organizacji sporządza sprawozdanie wraz z oceną (wnioskami), które przedkłada do dnia 31 stycznia Dyrektorowi CIUWO do akceptacji.

Arkusz identyfikacji, oceny oraz określenia metody przeciwdziałaniu ryzyku

Lp.	Cel do osiągnięcia	Nazwa Zadanie	Nazwa Aktywów/zasób/ informacja	Opis wykorzystania podatności przez zagrożenie (Sytuacja/zagrożenie)	Podatność	Prawdopodobieństwo zdarzenia (0-4)	Wpływ zagrożenia (0, 1, 2, 3, 4)						Ryzyko = P x Wpływ Bezpieczeństwo informacji | Jakość usług IT Poufność (7*8)	Ryzyko = P x Wpływ Bezpieczeństwo informacji | Jakość usług IT Dostępność (7*9)	Ryzyko = P x Wpływ Bezpieczeństwo informacji | Jakość usług IT Integralność (7*10)	Ryzyko = P x Wpływ Realizacja podstawowych zadań (7*11)	Ryzyko = P x Wpływ Realizacja praw Podmiotu danych (7*12)	Ryzyko = P x Wpływ Reputacja / wizerunek (7*13)	Ryzyko = Suma ryzyk Całościowe (14+15+16+17+18 +19)	Właściciel ryzyka (lub Kierownik Komórki Organizacyjnej)	Postępowanie z ryzykiem wraz z terminem realizacji Propozycja Właściciela ryzyka /Decyzja Dyrektora (Plan Postępowania tworzony jest dla wartości nieakceptowalnych)	Prawdopodobieństwo zdarzenia (1-4) po wdrożeniu planu postępowania z ryzykiem	Wpływ zagrożenia (1-4) po wdrożeniu planu postępowania z ryzykiem						Ryzyko po wdrożeniu planu postępowania z ryzykiem = P x Wpływ Bezpieczeństwo informacji | Jakość usług IT Poufność (23*24)	Ryzyko po wdrożeniu planu postępowania z ryzykiem = P x Wpływ Bezpieczeństwo informacji | Jakość usług IT Dostępność (23*25)	Ryzyko po wdrożeniu planu postępowania z ryzykiem = P x Wpływ Bezpieczeństwo informacji | Jakość usług IT Integralność (23*26)	Ryzyko po wdrożeniu planu postępowania z ryzykiem = P x Wpływ Realizacja podstawowych zadań (23*27)	Ryzyko po wdrożeniu planu postępowania z ryzykiem = P x Wpływ Realizacja praw Podmiotu danych (23*28)	Ryzyko po wdrożeniu planu postępowania z ryzykiem = P x Wpływ Reputacja / wizerunek (23*29)	Nr ryzyka
							Bezpieczeństwo informacji | Jakość usług IT Poufność	Bezpieczeństwo informacji | Jakość usług IT Dostępność	Bezpieczeństwo informacji | Jakość usług IT Integralność	Realizacja podstawowych zadań	Realizacja praw Podmiotu danych	Reputacja/ wizerunek											Bezpieczeństwo informacji | Jakość usług IT Poufność	Bezpieczeństwo informacji | Jakość usług IT Dostępność	Bezpieczeństwo informacji | Jakość usług IT Integralność	Realizacja podstawowych zadań	Realizacja praw Podmiotu danych	Reputacja/ wizerunek							