Warszawa, dnia 17 kwietnia 2019 r.

Poz. 12

Z A R Z Ą D Z E N I E N R 1 1

M I N I S T R A C Y F R Y Z A C J I

z dnia 10 kwietnia 2019 r.

w sprawie Polityki zarządzania ryzykiem w Ministerstwie Cyfryzacji

Na podstawie art. 69 ust. 1 pkt 3 w związku z art. 68 ust. 2 pkt 7 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. Wprowadza się Politykę zarządzania ryzykiem w Ministerstwie Cyfryzacji stanowiącą załącznik do zarządzenia.

§ 2. Traci moc zarządzenie Nr 25 z dnia 31 grudnia 2013 r. Ministra Administracji i Cyfryzacji w sprawie wprowadzenia Polityki zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji (Dz. Urz. Min. Ad. i Cyf. z 2014 r. poz. 2).

§ 3. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

MAREK ZAGÓRSKI

MINISTER CYFRYZACJI

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 62, 1000, 1366, 1669, 1693, 2245, 2354 i 2500 oraz w Dz. U. z 2019 r. poz. 303, 326 i 534.

Załącznik do zarządzenia Ministra Cyfryzacji z dnia 10 kwietnia 2019 r. (poz. 12)

Polityka zarządzania ryzykiem w Ministerstwie Cyfryzacji

Rozdział 1

Postanowienia ogólne

§ 1. 1. Polityka zarządzania ryzykiem w Ministerstwie Cyfryzacji, zwana dalej „Polityką”, określa podejście do zarządzania ryzykiem w Ministerstwie Cyfryzacji, zwanym dalej „Ministerstwem”.

2. Celem wprowadzenia Polityki jest:

1) zwiększenie prawdopodobieństwa osiągnięcia celów i realizacji zadań Ministerstwa;
2) wykorzystanie możliwości i szans stojących przed Ministerstwem oraz ograniczenie ryzyka utraty szans;
3) usprawnienie i podniesienie efektywności procesu zarządzania Ministerstwem w ramach kontroli zarządczej;
4) ograniczenie potencjalnych, negatywnych skutków zdarzeń;
5) usprawnienie procesu planowania oraz oceny stopnia osiągnięcia celów i realizacji zadań;
6) efektywne wykorzystanie zasobów finansowych, ludzkich i materialnych;
7) doskonalenie wyników działalności w obszarze bezpieczeństwa, zgodności z przepisami prawa, zarządzania projektami, efektywności w działaniach operacyjnych, jakości świadczenia usług oraz ładzie organizacyjnym;
8) poprawa wizerunku Ministerstwa, budowa zaufania w stosunku do działalności Ministerstwa;
9) zapewnienie Kierownictwu Ministerstwa informacji o zagrożeniach realizacji zadań i osiągnięcia celów, w tym w szczególności określonych w ramach Planu działalności Ministra Cyfryzacji.

3. Polityka określa:

1) obszar i zasady zarządzania ryzykiem;
2) uczestników biorących udział w zarządzaniu ryzykiem;
3) poziomy i sposób zarządzania ryzykiem;
4) etapy zarządzania ryzykiem;
5) zasady monitorowania, informowania i raportowania ryzyka.

4. Polityka dotyczy członków Kierownictwa Ministerstwa i ma zastosowanie do wszystkich komórek organizacyjnych Ministerstwa oraz wszystkich pracowników zatrudnionych w Ministerstwie.

§ 2. 1. Ilekroć w Polityce jest mowa o:

1) planie działalności Ministra Cyfryzacji – należy przez to rozumieć Plan działalności, o którym mowa w rozporządzeniu Ministra Finansów z dnia 29 września 2010 r. w sprawie planu działalności i sprawozdania z jego wykonania (Dz. U. Nr 187, poz. 1254) sporządzony przez Ministra Cyfryzacji;
2) Ministrze – należy przez to rozumieć Ministra Cyfryzacji;
3) kierownictwie Ministerstwa – należy przez to rozumieć Ministra, Sekretarzy Stanu, Podsekretarzy Stanu oraz Dyrektora Generalnego Ministerstwa;
4) kierującym komórką organizacyjną – należy przez to rozumieć dyrektora komórki organizacyjnej Ministerstwa, zastępcę dyrektora lub inna osobę upoważnioną do kierowania tą komórką;
5) zarządzaniu ryzykiem – należy przez to rozumieć ogół działań podejmowanych dla zwiększenia prawdopodobieństwa osiągnięcia celów i realizacji zadań Ministerstwa będących elementem kontroli zarządczej;
6) kontroli zarządczej – należy przez to rozumieć sposób zarzadzania, ogół działań podejmowanych dla zapewnienia realizacji zadań i osiągnięcia celów, w sposób zgodny z prawem, efektywny, oszczędny i terminowy;
7) zarządzaniu ryzykiem – należy przez to rozumieć skoordynowane działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka;
8) proces zarządzania ryzykiem – należy przez to rozumieć systematyczne stosowanie polityki do działań w zakresie: identyfikowania, analizowania, oceny, postępowania z ryzykiem, monitorowania, przeglądu i komunikacji ryzyka;
9) prawdopodobieństwie – należy przez to rozumieć wielkość określającą możliwość, szansę wystąpienia zdarzenia, wyrażoną opisowo lub liczbowo;
10) ryzyku – należy przez to rozumieć możliwość zaistnienia zdarzenia, które będzie miało negatywny wpływ na realizację założonych celów i zadań Ministerstwa i które będzie miało charakter zagrożenia;
11) czynniku ryzyka – należy przez to rozumieć zdarzenie lub działanie lub zaniechanie, które może spowodować wystąpienie ryzyka;

12) szacowaniu ryzyka – należy przez to rozumieć całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka;
13) identyfikacji ryzyka – należy przez to rozumieć proces wyszukiwania, rozpoznawania i opisywania ryzyka;
14) analizie ryzyka – należy przez to rozumieć proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka;
15) poziomie ryzyka – należy przez to rozumieć wielkość, istotność ryzyka określaną jako iloczyn wpływu zdarzenia mogącego stanowić zagrożenie dla realizacji celów i zadań Ministerstwa oraz prawdopodobieństwa jego wystąpienia;
16) kryteriach ryzyka – należy przez to rozumieć ustalone poziomy odniesienia, względem których określa się ważność ryzyka;
17) ocenie ryzyka – należy przez to rozumieć proces porównywania wyników analizy ryzyka z kryteriami ryzyka pozwalający na zakwalifikowanie ryzyka do jednej z 4 kategorii: niskiego, średniego, wysokiego i bardzo wysokiego;
18) postępowaniu z ryzykiem – należy przez to rozumieć działania związane z modyfikacją ryzyka, działania zaradcze obniżające jego poziom (istotność);
19) działaniach zaradczych – należy przez to rozumieć działania polegające na wzmocnieniu mechanizmów kontroli (procedury, wytyczne, zasady, nadzór), zastosowanie zabezpieczeń (technicznych, organizacyjnych, finansowych);
20) przeglądzie ryzyka – należy przez to rozumieć działanie podejmowane w celu określenia przydatności, adekwatności oraz skuteczności procesu zarządzania ryzykiem, aktualnie zidentyfikowanych ryzyk i planu postępowania z ryzykiem;
21) monitorowaniu – należy przez to rozumieć ciągłe sprawdzanie, nadzorowanie, krytyczne obserwowanie lub określanie stanu, prowadzone w celu zidentyfikowania zmian w zakresie wymaganego lub oczekiwanego poziomu skuteczności procesu zarządzania ryzykiem;
22) właścicielu ryzyka – osobę odpowiedzialną za zarządzanie danym ryzykiem, posiadającą kompetencje do podjęcia działań zarządczych w stosunku do ryzyka, którym zarządza. Dla ryzyk związanych z osiąganiem celów i realizacją zadań komórki organizacyjnej właścicielem ryzyk jest kierujący daną komórką organizacyjną Ministerstwa. W szczególnych przypadkach dla ryzyk związanych z realizacją konkretnego projektu właścicielem ryzyka jest wyznaczony kierownik projektu. W przypadku ryzyk horyzontalnych obejmujących wszystkie komórki organizacyjne Ministerstwa

właścicielami ryzyka są kierujący komórkami organizacyjnymi Ministerstwa, każdy w zakresie celów i zadań kierowanej przez siebie komórki.

Rozdział 2

Obszar i zasady

§ 4. 1. Zarządzanie ryzykiem w Ministerstwie odbywa się poprzez:

1) strategiczne zarządzanie ryzykiem oparte na rocznej identyfikacji i analizie ryzyka;
2) operacyjne, bieżące zarządzanie ryzykiem polegające na ciągłej identyfikacji, analizie i ocenie ryzyka oraz podejmowaniu działań zaradczych na bieżąco – jako element zachodzących zmian i potrzeb.

2. Polityka zarządzania ryzykiem w Ministerstwie dotyczy następujących poziomów zarządzania ryzykiem:

1) poziom strategiczny – dotyczy zarządzania ryzykiem strategicznym w stosunku do najważniejszych celów i zadań określonych w Planie działalności Ministra Cyfryzacji;
2) poziom operacyjny – dotyczy zarządzania ryzykiem w stosunku do celów szczegółowych, przez które należy rozumieć cele i konkretne zadania jakie będą realizowane przez komórki organizacyjne Ministerstwa oraz jednostki podległe i nadzorowane przez Ministra, których realizacja jest konieczna do osiągnięcia celów strategicznych.

3. W procesie zarządzania ryzykiem wyróżnia się dwa poziomy ryzyka:

1) ryzyko strategiczne – ryzyko, które może spowodować niezrealizowanie celów strategicznych Ministerstwa, określonych w Planie Działalności Ministra Cyfryzacji lub zagrozić ich realizacji;
2) ryzyko operacyjne – ryzyko, które może spowodować niezrealizowanie celów i zadań szczegółowych, wynikających z bieżącej pracy komórek organizacyjnych Ministerstwa, a w konsekwencji mieć wpływ na ryzyko strategiczne.

4. Pomiędzy ryzykiem strategicznym a operacyjnym mogą wystąpić następujące zależności:

1) na konkretne ryzyko strategiczne ma wpływ szereg ryzyk operacyjnych. Oznacza to, że dane ryzyko strategiczne jest agregatem ryzyk operacyjnych związanych z celami i zadaniami szczegółowymi, których wykonanie zapewni osiągnięcie celu strategicznego;
2) określona grupa ryzyk operacyjnych wynika z dekompozycji danego ryzyka strategicznego;

3) w szczególnym przypadku materializacja pojedynczego ryzyka operacyjnego może doprowadzić do nieosiągnięcia celu strategicznego (bezpośredni związek danego ryzyka operacyjnego z ryzykiem strategicznym).

5. Zarządzanie ryzykiem realizowane jest we wszystkich obszarach działania Ministerstwa i w zakresie wszystkich komórek organizacyjnych Ministerstwa, czyli w zakresie departamentu, biura, wydziału, zespołu, stanowiska.

6. Zarządzanie ryzykiem jest wykonywane w zakresie realizacji zadań i osiągania określonych celów, wydajnego, ekonomicznego i efektywnego wykorzystania posiadanych zasobów.

7. Zarządzanie ryzykiem jest częścią odpowiedzialności kierownictwa oraz jest integralną częścią wszystkich procesów organizacyjnych, łącznie z planowaniem strategicznym i wszystkimi procesami zarządzania operacyjnego a także zarządzania projektami i zmianą.

8. Zarządzanie ryzykiem jest elementem podejmowania decyzji. Zarządzanie ryzykiem pomaga podejmującym decyzje w podjęciu świadomych, uzasadnionych wyborów, ustaleniu priorytetów działań oraz rozpoznawaniu alternatywnych kierunków działań.

9. Proces zarządzania ryzykiem jest udokumentowany zgodnie z zasadami określonymi w rozdziałach 3 do 8.

Rozdział 3

Zadania i odpowiedzialność

§ 5. 1. Na poziomie strategicznym za realizację Polityki odpowiada Minister, poprzez:

1) kształtowanie i wdrażanie polityki zarządzania ryzykiem oraz nadzór nad nią;
2) wyznaczanie kryteriów ryzyka poprzez określenie akceptowalnego poziomu ryzyka;
3) monitorowanie ryzyka na poziomie strategicznym;
4) wyznaczenie właścicieli ryzyka, w fazie strategicznego zarządzania ryzykiem.

2. W proces szacowania ryzyka na poziomie strategicznym włączeni są Sekretarz, Podsekretarze Stanu oraz Dyrektor Generalny Ministerstwa.

3. Minister może przypisać odpowiedzialność za zarządzanie ryzykiem strategicznym związanym z głównym celem Ministerstwa właściwemu merytorycznie Sekretarzowi, Podsekretarzowi Stanu lub Dyrektorowi Generalnemu Ministerstwa.

§ 6. 1. Na poziomie operacyjnym za realizację Polityki odpowiadają kierujący komórkami organizacyjnymi Ministerstwa poprzez:

1) identyfikację i udokumentowanie czynników ryzyka oraz ryzyk operacyjnych oraz strategicznych, które są istotne dla osiągnięcia celów i zadań szczegółowych, w odniesieniu do nadzorowanych obszarów działania z zastosowaniem arkusza stanowiącego załącznik nr 1 do Polityki;
2) analizę zidentyfikowanych ryzyk oraz określenie ich poziomu z uwzględnieniem prawdopodobieństwa oraz potencjalnego skutku, tj. wpływu na realizacje celów i zadań szczegółowych oraz celów strategicznych;
3) ocenę ryzyk poprzez porównanie poziomu ryzyka będącego wynikiem analizy z kryteriami ryzyka;
4) opracowanie planu postępowania z ryzykiem, a następnie prowadzenie działań związanych z jego realizacją;
5) monitorowanie ryzyka oraz mechanizmów kontrolnych;
6) przedstawianie Ministrowi informacji o działaniach związanych z zarządzaniem ryzykiem w szczególności o materializacji ryzyk strategicznych oraz podejmowaniu działań zaradczych;
7) okresowe przeglądy ryzyka pod kątem adekwatności efektywności i skuteczności, procesu zarządzania ryzykiem, zidentyfikowanych ryzyk i planu postępowania z ryzykiem;
8) ponowne przeprowadzenie szacowania ryzyka i weryfikację planu postępowania z ryzykiem, w przypadku zmiany czynników ryzyka wywołanych istotną zmianą środowiska jako elementu zachodzących zmian i potrzeb lub w przypadku kiedy Minister uzna to za konieczne.

2. Pracownicy komórek organizacyjnych Ministerstwa na poziomie operacyjnym odpowiadają za realizację mechanizmów postępowania z ryzykiem, uczestniczą w identyfikacji i analizie ryzyka.

§ 7. Zadania związane z koordynacją zarządzania ryzykiem na poziomie strategicznym realizuje Wydział Skarg, Kontroli i Wniosków Biura Ministra Ministerstwa poprzez:

1) inicjowanie procesu zarządzania ryzykiem strategicznym w Ministerstwie;
2) współpracę z kierującymi komórkami organizacyjnymi Ministerstwa, Sekretarzem, Podsekretarzami Stanu i Dyrektorem Generalnym Ministerstwa w zakresie analizy ryzyka strategicznego;
3) przygotowanie dla Ministra zestawienia zbiorczego ryzyk strategicznych zawartego w dokumencie „Analiza Ryzyka Ministerstwa Cyfryzacji”;

4) dokonywanie przeglądu Polityki i uaktualnianie dokumentacji związanej z Polityką.

Rozdział 4

Proces zarządzania ryzykiem na poziomie operacyjnym

§ 8. 1. Zarządzanie ryzykiem na poziomie operacyjnym prowadzone jest w sposób ciągły przez komórki organizacyjne Ministerstwa w odniesieniu do ich celów i zadań z uwzględnieniem celów i zadań określonych w Planie działalności Ministerstwa Cyfryzacji, a także celów i zadań jednostek podległych i nadzorowanych przez Ministra.

2. W przypadku gdy konieczność zarządzania określoną grupą ryzyk wynika z odrębnych przepisów prawa, Polityka dopuszcza stosowanie odrębnych (innych niż opisane w Polityce) procedur zarządzania ta grupą ryzyk. Dotyczy to ryzyka związanego z bezpieczeństwem informacji, cyberbezpieczeństwem, ochroną danych osobowych, zachowaniami korupcyjnymi, itp.

3. W przypadku ryzyka projektowego, Polityka dopuszcza stosowanie odrębnych (innych niż opisane w Polityce) procedur zarządzania ta grupą ryzyka zgodnie z wewnętrznymi procedurami zarządzania ryzykiem projektowym.

4. Niezależnie od stosowanej procedury zarządzania ryzykiem operacyjnym konieczne jest przeprowadzenie przeglądu ryzyka operacyjnego i agregacji ryzyk operacyjnych do ryzyk strategicznych zgodnie z § 11 ust.1 Polityki.

5. Identyfikacja czynników ryzyka i ryzyk odbywa się z wykorzystaniem arkusza stanowiącego załącznik nr 1 do Polityki w odniesieniu do następujących obszarów działania:

1) legislacja;
2) zamówienia publiczne;
3) budżet i finanse;
4) kadry i szkolenia;
5) informatyka;
6) bezpieczeństwo i ochrona informacji;
7) obsługa administracyjno-techniczna;
8) informacja i komunikacja;
9) informatyzacja administracji publicznej oraz podmiotów wykonujących zadania publiczne;
10) rozwój społeczeństwa informacyjnego i przeciwdziałanie wykluczeniu cyfrowemu;
11) rozwój usług świadczonych drogą elektroniczną;

12) ochrona danych osobowych;
13) telekomunikacja;
14) bezpieczeństwo cyberprzestrzeni;
15) rejestry państwowe i rejestr Centralnej Ewidencji Pojazdów i Kierowców;
16) usługi zaufania i identyfikacja elektronicznej.

6. Zidentyfikowane ryzyko należy opisać i przyporządkować do jednej z określonych poniżej kategorii ryzyka:

1) zarządzanie;
2) finanse;
3) bezpieczeństwo;
4) przepisy i procedury;
5) działalność operacyjna.

§ 9. 1. Po określeniu celów, zadań, obszarów działania, kategorii ryzyka, zidentyfikowane ryzyko podlega analizie mającej na celu określenie jego poziomu jako iloczynu wpływu zdarzenia mogącego stanowić zagrożenie dla realizacji celów i zadań Ministerstwa oraz prawdopodobieństwa jego wystąpienia.

2. Przy analizie ryzyka należy wziąć pod uwagę uwarunkowania mające wpływ na ryzyko zgodnie z załącznikiem nr 2 do Polityki.

3. Przy ocenie prawdopodobieństwa wystąpienia zdarzenia należy wziąć pod uwagę istniejące mechanizmy kontrolne, ich skuteczność i poziom wdrożenia.

4. Do szacowania prawdopodobieństwa wystąpienia zdarzenia mogącego stanowić zagrożenie stosuje się metodę punktową, zgodnie z poniższą skalą:

Ocena punktowa prawdopodobieństwa wystąpienia zdarzenia		
Prawdopodobieństwo zdarzenia	Punktacja	Opis
Rzadkie	1	Zdarzenie jest prawie niemożliwe do wystąpienia
Mało prawdopodobne	2	Nie oczekuje się wystąpienia zdarzenia lub brak jest informacji by zagrożenie się zmaterializowało
Możliwe	3	Zdarzenie możliwe do wystąpienia lub zagrożenie zmaterializowało się w podobnych podmiotach w podobnych warunkach
Prawdopodobne	4	Zdarzenie prawdopodobnie wystąpi, istnieje znaczna

		szansa wystąpienia zdarzenia
Prawie pewne	5	Prawie na pewno się wydarzy lub zmaterializowało się w przeszłości w Ministerstwie

5. Przy ocenie skutków wystąpienia zdarzenia należy wziąć pod uwagę zarówno skutki finansowe, jak i pozafinansowe, takie jak np.: utrata reputacji, konsekwencje prawne, utrata szansy, opóźnienie, obniżenie jakości pracy, w przypadku projektu obniżenie jakości produktu końcowego.

6. Do szacowania skutku wystąpienia zdarzenia mogącego stanowić zagrożenie stosuje się metodę punktową, zgodnie z poniższą skalą:

Skutek związany z danym zdarzeniem powodującym zagrożenie		
Skutek zdarzenia	Punktacja	Opis
Nieznaczny	1	Zdarzenie objęte ryzykiem powoduje nieznaczne zakłócenie lub opóźnienie w wykonywaniu zadań, nie wpływa na wizerunek jednostki. Skutki zdarzenia można łatwo usunąć.
Mały	2	Zdarzenie objęte ryzykiem powoduje małe zakłócenie lub opóźnienie w wykonywaniu zadań, częściowo wpływa na wizerunek jednostki. Skutki zdarzenia można usunąć.
Średni	3	Zdarzenie objęte ryzykiem powoduje średnią stratę posiadanych zasobów, małą stratę finansową, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań, wizerunek jednostki. Z wystąpieniem zdarzenia może się wiązać trudny proces przywracania stanu poprzedniego
Duży	4	Zdarzenie objęte ryzykiem powoduje poważną stratę posiadanych zasobów, średnia stratę finansową, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań, wizerunek jednostki. Z wystąpieniem zdarzenia wiąże się trudny proces przywracania stanu poprzedniego.
Krytyczny	5	Zdarzenie objęte ryzykiem powoduje uszczerbek

		mający krytyczny lub bardzo duży wpływ na realizację kluczowych zadań lub osiąganie założonych celów, poważny uszczerbek w zakresie jakości wykonywanych zadań, poważną stratę finansową albo niekorzystny wpływ na wizerunek jednostki. Z wystąpieniem zdarzenia wiąże się długotrwały i trudny proces przywracania stanu poprzedniego.

7. Szacowanie ryzyka oznacza wyznaczanie jego poziomu (istotności) i polega na pomnożeniu skutku wystąpienia zdarzenia mogącego stanowić zagrożenie (wyrażonego punktowo) przez prawdopodobieństwo jego wystąpienia (wyrażonego punktowo).

8. W celu dokonania oceny ryzyka przyjęto następujące kryteria ryzyka pozwalające na zakwalifikowanie danego ryzyka pod względem istotności do jednej z 4 kategorii:

Kryteria ryzyka		
Poziom ryzyka	Istotność ryzyka	Kategoria ryzyka
1 - 5	niska	ryzyko niskie
6 - 10	średnia	ryzyko średnie
12 - 16	wysoka	ryzyko wysokie
20 - 25	bardzo wysoka	ryzyko bardzo wysokie

9. Graficzne przedstawienie ryzyka prezentuje poniższe zestawienie:

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

Rozdział 5

Interpretacja wyników szacowania ryzyka i postępowanie z ryzykiem

§ 10. 1. Możliwe sposoby postępowania z ryzykiem to:

1) zapobieganie (ograniczanie) – działania polegające na zmniejszeniu poziomu ryzyka, w tym poprzez obniżenie prawdopodobieństwa wystąpienia lub zmniejszenia wpływu na osiągnięcie celów i realizację zadań, np. poprzez działania zaradcze w tym: wzmocnienie mechanizmów kontroli (procedury, wytyczne, zasady, nadzór), zastosowanie zabezpieczeń (technicznych, organizacyjnych, finansowych);

2) dzielenie ryzyka z inną stroną w tym np.: ubezpieczenie skutków materializacji ryzyka, outsourcing procesów generujących ryzyko;
3) tolerowanie ryzyka na podstawie świadomej decyzji – gdy istnieje konieczność realizacji zadań i osiągnięcia celu, i jednocześnie istnieją określone trudności i ograniczenia w przeciwdziałaniu ryzyku, a także w przypadku gdy koszty podjętych działań zaradczych mogłyby przekroczyć przewidywane korzyści wynikające z obniżenia poziomu ryzyka;
4) unikanie ryzyka – decyzja o nierozpoczynaniu lub niekontynuowaniu działań rodzących ryzyko.

2. Wprowadza się następujące podstawowe zasady postępowania z ryzykiem dla poszczególnych kategorii ryzyka:

1) ryzyko niskie – ryzyko to nie ma znaczącego wpływu na realizację celów i zadań. Dla ryzyka niskiego nie jest wymagane podejmowanie działań zaradczych. Ryzyko niskie jest ryzykiem akceptowalnym i podlega monitorowaniu w celu ewentualnego wykrycia wzrostu istotności/poziomu powyżej poziomu niskiego;
2) ryzyko średnie – ryzyko to może w sposób istotny wpłynąć na realizację celów i zadań. Ryzyko średnie jest ryzykiem tolerowanym warunkowo i podlega monitorowaniu. Należy także rozważyć potrzebę działań zaradczych i wprowadzenia dodatkowych mechanizmów kontroli mając na uwadze koszty ich wprowadzenia. Decyzję o tolerowaniu ryzyka średniego podejmuje właściciel ryzyka. Za monitoring ryzyka i ewentualne zaprojektowanie mechanizmów kontrolnych i działań zaradczych odpowiedzialny jest właściciel ryzyka;
3) ryzyko wysokie – ryzyko to może w sposób bardzo znaczący wpłynąć na realizację celów i zadań. Ryzyko wysokie jest ryzykiem tolerowanym warunkowo i wymaga wprowadzenia przez kierującego komórką organizacyjną Ministerstwa działań zaradczych i uzupełnienia wewnętrznych mechanizmów kontrolnych, które ograniczą prawdopodobieństwo wystąpienia ryzyka lub zmniejszą jego wpływ. Decyzję o tolerowaniu ryzyka wysokiego może podjąć członek Kierownictwa Ministerstwa na wniosek kierującego komórką organizacyjną Ministerstwa. Za monitoring ryzyka i podejmowanie działań zaradczych odpowiedzialny jest właściciel ryzyka;
4) ryzyko bardzo wysokie – ryzyko to stanowi poważne zagrożenie dla działalności Ministerstwa w tym realizacji jego celów i zadań. Ryzyko bardzo wysokie jest ryzykiem krytycznym i niezbędne jest natychmiastowe wprowadzenie silnych mechanizmów kontroli oraz zdecydowanych działań zaradczych. Ryzyko krytyczne podlega ciągłemu

monitoringowi i nie może być tolerowane w dłuższym okresie czasu. Decyzje o czasowym tolerowaniu ryzyka bardzo wysokiego podejmuje członek Kierownictwa Ministerstwa na wniosek kierującego komórką organizacyjną Ministerstwa. Właściciel ryzyka jest zobowiązany do zaprojektowania mechanizmów ograniczających poziom ryzyka bardzo wysokiego do niższego oraz kontroli realizacji zaplanowanych działań.

3. Minister może podjąć decyzję o akceptacji ryzyka średniego i ryzyka wysokiego bez podejmowania działań zaradczych.

4. Właściciele ryzyk na bieżąco monitorują ryzyko oraz podejmują działania zaradcze.

5. Dokumentacja analizy ryzyka i postępowania z ryzykiem na poziomie operacyjnym podlega akceptacji kierującego komórką organizacyjną Ministerstwa.

Rozdział 6

Proces zarzadzania ryzykiem na poziomie strategicznym

§ 11. 1. Po otrzymaniu zatwierdzonego Planu działalności Ministra Cyfryzacji na kolejny rok, kierujący komórkami organizacyjnymi Ministerstwa dokonują przeglądu ryzyk operacyjnych i przeprowadzają agregację ryzyk operacyjnych do ryzyk strategicznych dla celów i zadań strategicznych określonych w Planie Działalności Ministra Cyfryzacji na dany rok. Zależności pomiędzy ryzykami operacyjnymi a strategicznymi określone zostały w § 4 ust. 3.

2. Wyniki przeglądu i agregacji ryzyk operacyjnych do strategicznych dokumentowane są według arkusza stanowiącego załącznik nr 1 do Polityki.

3. Wyniki przeglądu i agregacji ryzyk operacyjnych do strategicznych po konsultacji z nadzorującym członkiem kierownictwa są zatwierdzane przez kierującego komórką organizacyjną Ministerstwa i przekazywane w terminie do 15 grudnia do Wydziału Skarg, Kontroli i Nadzoru Biura Ministra.

4. Na podstawie informacji o ryzykach strategicznych otrzymanych z komórek organizacyjnych Ministerstwa Wydział Skarg, Kontroli i Nadzoru Biura Ministra Ministerstwa opracowuje zestawienie zbiorcze ryzyk strategicznych Ministerstwa Cyfryzacji, z zastosowaniem arkusza stanowiącego załącznik nr 1 do Polityki.

5. Wydział Skarg, Kontroli i Nadzoru Biura Ministra Ministerstwa w terminie do dnia 30 grudnia przekazuje dokument zestawienia zbiorczego ryzyk strategicznych członkom Kierownictwa Ministerstwa.

6. Członkowie Kierownictwa Ministerstwa dokonują przeglądu, weryfikacji i analizy ryzyka na szczeblu strategicznym w terminie 14 dni od dnia otrzymania zestawienia zbiorczego ryzyk strategicznych, według zasad określonych w § 9 i 10.

7. Członkowie Kierownictwa Ministerstwa mogą identyfikować dodatkowe czynniki ryzyka nieuwzględnione w procesie identyfikacji na poziomie operacyjnym.

8. Po przeprowadzeniu analizy ryzyka na szczeblu strategicznym, członkowie Kierownictwa Ministerstwa przekazują wyniki do Wydziału Skarg, Kontroli i Nadzoru Biura Ministra Ministerstwa.

§ 12. 1. Po przeprowadzeniu procesu analizy ryzyka na poziomie operacyjnym oraz przeglądu i weryfikacji przez członków Kierownictwa Ministerstwa na poziomie strategicznym Wydział Skarg, Kontroli i Nadzoru Biura Ministra Ministerstwa opracowuje corocznie dokument „Analiza Ryzyka Ministerstwa Cyfryzacji".

2. Wydział Skarg, Kontroli i Nadzoru Biura Ministra Ministerstwa przekazuje opracowany na dany rok dokument „Analiza Ryzyka Ministerstwa Cyfryzacji" do Ministra Cyfryzacji.

3. Minister ustala priorytety dla ryzyk strategicznych stosując czterostopniową skalę priorytetu: bardzo wysoki, wysoki, średni, niski, przypisując każdemu odpowiednio wagę: 4, 3, 2, 1.

4. Minister corocznie zatwierdza dokument „Analiza Ryzyka Ministerstwa Cyfryzacji".

5. Minister, stosownie do potrzeb, przedstawia na posiedzeniu Kierownictwa Ministerstwa informacje o ryzykach, które mogą zagrozić realizacji głównych celów Ministerstwa oraz o podjętych i przewidywalnych działaniach zaradczych związanych z tymi ryzykami.

6. W razie konieczności Minister wyznacza właścicieli ryzyka.

7. Dokument „Analiza ryzyka Ministerstwa Cyfryzacji" jest corocznie przekazywany do komórek organizacyjnych Ministerstwa, stanowiąc narzędzie do monitorowania i zarządzania ryzykiem.

Rozdział 7

Monitorowanie ryzyka, raportowanie i informowanie

§ 13. 1. Wszyscy pracownicy mają obowiązek raportowania o dostrzeżonych czynnikach ryzyka kierującym komórkami organizacyjnymi Ministerstwa lub członkom Kierownictwa Ministerstwa. Informacje te są wykorzystywane w procesie zarządzania ryzykiem.

2. W Ministerstwie proces monitorowania ryzyka jest procesem ciągłym realizowanym przez Kierownictwo Ministerstwa na każdym szczeblu zarządzania, który pozwala na podejmowanie decyzji w odpowiednim czasie.

3. Kierujący komórkami organizacyjnymi Ministerstwa prowadzą monitorowanie ryzyk. W ramach monitorowania dokonują:

1) identyfikacji, analizy i oceny nowych ryzyk;
2) aktualizacji informacji o dotychczas zidentyfikowanych ryzykach;
3) przeglądu stanu realizacji planu postępowania z ryzykiem w tym postępu i opóźnień w jego realizacji;
4) oceny funkcjonowania mechanizmów kontrolnych pod kątem ich adekwatności, efektywności i skuteczności.

4. Kierujący komórkami organizacyjnymi Ministerstwa zobowiązani są do informowania podległych pracowników o ryzyku oraz planie postępowania z ryzykiem w zakresie ryzyk dotyczących danej komórki organizacyjnej.

5. Kierujący komórkami organizacyjnymi Ministerstwa zobowiązani są do przedstawiania Ministrowi informacji o działaniach związanych z zarządzaniem ryzykiem w szczególności o materializacji ryzyk strategicznych oraz podejmowania działań zaradczych.

§ 14. Niezależną ocenę zarzadzania ryzykiem w Ministerstwie przeprowadza audytor wewnętrzny Ministerstwa.

Rozdział 8

Aktualizacja Polityki

§ 15. 1. Polityka wraz z załącznikami podlega corocznym przeglądom, w terminie do dnia 31 maja, w celu ich aktualizacji.

2. Każda aktualizacja Polityki podlega akceptacji Ministra.

Załącznik nr 1
do Polityki zarządzania ryzykiem
w Ministerstwie Cyfryzacji

Nazwa komórki organizacyjnej:

Arkusz analizy ryzyka oraz postępowania z ryzykiem

Arkusz analizy ryzyka operacyjnego/strategicznego											
Lp.	cel ogólny	cel szczegółowy/ zadanie	obszar działania	kategoria ryzyka	opis ryzyka	prawdopodobieństwo	skutek	poziom ryzyka (istotność)	priorytet Ministra	właściciel ryzyka	sposób postępowania z ryzykiem
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
1.											
2.											
3.											

Akceptacja kierującego komórką organizacyjną Ministerstwa:

Załącznik nr 2
do Polityki zarządzania ryzykiem
w Ministerstwie Cyfryzacji

KATEGORIE RYZYKA I LISTA CZYNNIKÓW RYZYKA

I. Czynniki wpływające na prawdopodobieństwo wystąpienia danego zagrożenia:

1. Zarządzanie i organizacja:

1) czy kompetencje, zadania i odpowiedzialność pracowników są jasno i jednoznacznie określone?
2) czy zdefiniowano zadania wrażliwe?
3) czy istnieje transparentny i obiektywny system wynagradzania i motywowania pracowników?
4) czy zarobki pracowników są adekwatne do powierzonych im zadań i obowiązków?
5) czy występuje duża rotacja pracowników?
6) czy kwalifikacje pracowników i kierownictwa odpowiadają charakterowi wykonywanych obowiązków?
7) czy warunki pracy (pomieszczenia, wyposażenie) są odpowiednie do wykonywanych zadań?
8) czy organizacja przywiązuje dużą wagę do kwestii etyki i morale pracowników?
9) czy pracownicy mają możliwość podejmowania dodatkowego zatrudnienia/zajęć zarobkowych?

2. Finanse:

1) jaka jest wielkość, rodzaj dokonywanych operacji?
2) czy prowadzona jest na bieżąco sprawozdawczość i czy jest analizowana pod kątem nieprawidłowości?
3) czy występują zmiany systemu księgowego?
4) czy jednoznacznie określone są pełnomocnictwa do dysponowania środkami publicznymi?
5) czy powierzono uprawnienia pracownikom w związku z gospodarką finansową?

3. Bezpieczeństwo:

1) czy budynek i poszczególne pomieszczenia są odpowiednio zabezpieczone przed dostępem osób nieupoważnionych?

2) czy dostęp osób z zewnątrz jest monitorowany i dokumentowany (księgi gości, telewizja przemysłowa)?
3) czy spotkania z osobami z zewnątrz odbywają się w otwartych i monitorowanych pomieszczeniach?
4) czy dostęp do dokumentów jest zabezpieczony i odpowiednio określane są prawa dostępu do dokumentów dla poszczególnych pracowników?
5) czy korzystanie z dokumentów jest rejestrowane lub dokumentowane? Czy istnieją procedury korzystania z dokumentów niejawnych?
6) czy sieci i zasoby informatyczne są prawidłowo zabezpieczone przed nieuprawnionym dostępem (za pomocą haseł, certyfikatów)?
7) czy dostęp do sieci i zasobów informatycznych jest dokumentowany (w postaci logów)?
8) czy zostało zapewnione bezpieczeństwo przetwarzania informacji?
9) czy zostało zapewnione bezpieczeństwo danych osobowych?
10) czy zostało zapewnione cyberbezpieczeństwo?

4. Przepisy i procedury:

1) czy działalność jednostki jest opisana procedurami i czy są one przestrzegane i dokumentowane?
2) czy przepisy regulujące działalność jednostki są jasne i przejrzyste?
3) czy prowadzony jest regularnie audyt? Czy opisane są ścieżki audytu?
4) czy działalność jest udokumentowana, rejestrowana poddawana systematycznej kontroli wewnętrznej?
5) czy została opracowana i jest stosowana procedura zarządzania zmianami?
6) czy została opracowana i jest stosowana procedura zarządzania projektami?
7) czy została opracowana i jest stosowana procedura zapobiegania korupcji?

II. Możliwe skutki wystąpienia danego zagrożenia:

1) możliwość utraty reputacji oraz zaufania obywateli;
2) skutki finansowe dla budżetu;
3) skutki finansowe dla pracowników;
4) zaburzenia w funkcjonowaniu jednostki – niewywiązanie lub nieprawidłowe wywiązywanie się z powierzonych zadań;
5) zaburzenia w realizacji projektów w tym: przekroczenie budżetu, przekroczenie terminu, obniżenie jakości produktu końcowego;
6) reperkusje na arenie międzynarodowej;

7) dodatkowe, nieplanowane kontrole;
8) wywołanie zmian organizacyjnych;
9) odpowiedzialność dyscyplinarna;
10) utrata możliwości ubiegania się o środki unijne;
11) konsekwencje prawne.