Polityka zarządzania ryzykiem w Naczelnej Dyrekcji Archiwów Państwowych

Rozdział 1

Przepisy ogólne

§ 1. Ilekroć w Polityce zarządzania ryzykiem w Naczelnej Dyrekcji Archiwów Państwowych, zwanej dalej „NDAP", jest mowa o:

1) akceptowalnym poziomie ryzyka – należy przez to rozumieć jasno określony poziom ryzyka, wobec którego właściciel ryzyka nie podejmuje dalszych działań (godzi się na jego istnienie);
2) aktywach – należy przez to rozumieć środki materialne i niematerialne oraz zasoby majątkowe o wiarygodnie określonej wartości, powstałe w wyniku przeszłych zdarzeń;
3) czynniku ryzyka – należy przez to rozumieć okoliczności, stan prawny, stan faktyczny, działania, zaniechania oraz wydarzenia zewnętrzne i wewnętrzne, które mogą, ale nie muszą wywołać ryzyko wystąpienia nieprawidłowości;
4) działaniach zaradczych – należy przez to rozumieć działania wzmacniające mechanizmy kontroli (procedury, wytyczne, zasady, nadzór) i zastosowane zabezpieczenia (techniczne, organizacyjne, finansowe);
5) kontekście wewnętrznym – należy przez to rozumieć środowisko wewnętrzne, w którym NDAP dąży do osiągnięcia swoich celów;
6) kontekście zewnętrznym – należy przez to rozumieć środowisko zewnętrzne, w którym NDAP dąży do osiągnięcia swoich celów;
7) kryteriach ryzyka – należy przez to rozumieć poziomy odniesienia, względem których określana jest waga ryzyka, oparte na celach organizacyjnych oraz na zewnętrznym i wewnętrznym kontekście działalności NDAP, mogące pochodzić w szczególności z norm, przepisów prawa i innych wymagań;

8) podatności – należy przez to rozumieć słabość wynikającą z czynników wewnętrznych lub czynników ludzkich, która może zostać wykorzystana przez zagrożenie, powodując niekorzystne skutki;
9) pracowniku realizującym zadania z zakresu kontroli zarządczej – należy przez to rozumieć pracownika Wydziału Organizacyjnego NDAP;
10) reakcji na ryzyko – należy przez to rozumieć wybór i wdrożenie środków, polegających w szczególności na przeciwdziałaniu, przesunięciu, transferze, tolerowaniu, unikaniu lub usunięciu źródła ryzyka;
11) rozliczalności – należy przez to rozumieć właściwość pozwalającą przypisać określone działanie do osoby fizycznej lub procesu oraz umiejscowić je w czasie;
12) ryzyku – należy przez to rozumieć prawdopodobieństwo wystąpienia dowolnego zdarzenia, działania lub braku działania, którego skutkiem może być szkoda w majątku lub wizerunku NDAP, albo które przeszkodzi w osiągnięciu wyznaczonych celów i zadań;
13) ryzyku nieakceptowalnym – należy przez to rozumieć ryzyko wymagające podjęcia reakcji z uwagi na jego wysokie prawdopodobieństwo lub ewentualne skutki, które stanowi realne zagrożenie dla realizacji priorytetowych celów i zadań;
14) ryzyku szczątkowym – należy przez to rozumieć ryzyko jakie pozostaje po przeprowadzeniu działań zmierzających do zminimalizowania wpływu (skutków) oraz prawdopodobieństwa wystąpienia niepomyślnych zdarzeń, w tym działań kontrolnych podjętych w odpowiedzi na ryzyko;
15) skutku – należy przez to rozumieć konsekwencje lub rezultat zdarzenia wyrażone ilościowo, mające wpływ pozytywny lub negatywny na osiągnięcie celu, przy czym. skutek może być pewny lub niepewny;
16) szacowaniu ryzyka – należy przez to rozumieć identyfikację oraz analizę i ocenę ryzyka;
17) środkach kontroli ryzyka – należy przez to rozumieć wszystko, co modyfikuje ryzyko (hamuje ryzyko lub zmniejsza prawdopodobieństwo jego wystąpienia), w tym procesy, polityki, urządzenia, praktyki, procedury i fizyczne działania;
18) właścicielu ryzyka – należy przez to rozumieć osobę kierującą komórką organizacyjną NDAP i osobę zajmującą jednoosobowe samodzielne stanowisko ds. ochrony danych osobowych,

które są odpowiedzialne za identyfikowanie i zarządzanie ryzykiem w danym obszarze działalności NDAP;

19) zagrożeniu – należy przez to rozumieć wszystkie niekorzystne czynniki mogące przyczynić się do wystąpienia negatywnego zdarzenia;

20) zarządzaniu ryzykiem – należy przez to rozumieć proces, którego celem jest identyfikacja potencjalnych ryzyk mogących mieć wpływ na realizację zadań NDAP oraz podjęcie działań uniemożliwiających wystąpienie ryzyk lub – jeśli ryzyko się zmaterializowało – odpowiednie zarządzenie skutkami.

§ 2. 1. Polityka zarządzania ryzykiem w Naczelnej Dyrekcji Archiwów Państwowych, zwana dalej ”Polityką”, służy minimalizacji wpływu zagrożeń na realizację zadań ustawowych i regulaminowych NDAP, przyjętych w dokumentach strategicznych i planistycznych.

2. W NDAP identyfikowane są ryzyka:

1) akceptowalne;

2) istotne;

3) nieakceptowalne.

3. Ryzyko akceptowalne to ryzyko ocenione według macierzy ryzyk, o której mowa w § 12 ust. 7, na poziomie średnim.

4. Polityka będzie poddawana cyklicznej kontroli pod kątem jej aktualności nie rzadziej niż co trzy lata.

5. Mając na uwadze rolę pracowników NDAP, w szczególności kadry kierowniczej, w procesie analizy ryzyka, przeprowadza się cykliczne szkolenia z tego zakresu.

§ 3. Wobec ryzyk w obszarze bezpieczeństwa informacji podejmuje się działania na podstawie odrębnej procedury SZBI.5, stanowiącej element Systemu Zarządzania Bezpieczeństwem Informacji, dostępnej pod adresem:

https://nadpanstwowych.sharepoint.com/sites/intranet/SitePages/BEZPIECZE%C5%83STWO-INFORMACJI.aspx

§ 4. 1. Polityka stanowi narzędzie zarządzania NDAP i ma zastosowanie do wszystkich komórek organizacyjnych NDAP oraz do wszystkich pracowników.

2. Polityka może mieć zastosowanie także do ryzyk identyfikowanych w archiwach państwowych pod warunkiem, że NDAP ma realny wpływ na przeciwdziałanie tym ryzykom lub zarządzenie nimi w przypadku ich materializacji.

3. Polityka jest realizowana z uwzględnieniem kontekstu wewnętrznego oraz kontekstu zewnętrznego działalności NDAP.

4. Kontekst wewnętrzny działalności NDAP stanowią:

1) ład organizacyjny, struktura organizacyjna, role i rozliczalność;
2) regulacje wewnętrzne, cele i strategie ustanowione w celu ich osiągnięcia;
3) zdolności rozumiane jako zasoby i wiedza (np. kapitał, czas, ludzie, procesy, systemy i technologie);
4) systemy informacyjne, przepływ informacji i procesy podejmowania decyzji (formalne i nieformalne);
5) relacje z wewnętrznymi interesariuszami, ich postrzeganie i wartości; kultura organizacyjna;
6) normy, wytyczne i modele przyjęte przez NDAP oraz forma i zakres relacji zawartych w zawartych przez NDAP umowach i porozumieniach.

5. Kontekst zewnętrzny działalności NDAP stanowią:

1) środowisko kulturowe, społeczne, polityczne, prawne, regulacyjne, finansowe, technologiczne, ekonomiczne, naturalne oraz konkurencyjne;
2) kluczowe czynniki i trendy mające wpływ na cele NDAP oraz relacje z zewnętrznymi interesariuszami, ich postrzeganie i wartości.

6. Wszyscy pracownicy NDAP są obowiązani do znajomości i przestrzegania Polityki, a w zakresie swoich kompetencji do:

1) monitorowania poziomu ryzyka w trakcie realizacji obowiązków służbowych;
2) informowania przełożonych o zdarzeniach, które mogą doprowadzić do negatywnych skutków dla działalności NDAP, w tym o potencjalnych zagrożeniach lub istotnych zmianach poziomu ryzyka.

§ 5. 1. Celem przyjętego podejścia do zarządzania ryzykiem jest:

1) wykrycie potencjalnych zdarzeń, które mogą wywrzeć wpływ na działalność NDAP, w szczególności zapewnienie bezpieczeństwa zasobów;

2) zarządzanie zidentyfikowanymi ryzykami, tj. zapewnienie, iż ryzyka są identyfikowane i analizowane na bieżąco, a dla ryzyk nieakceptowalnych są opracowywane i wdrażane odpowiednie plany postępowania;
3) efektywne wyznaczanie kierunków i celów działalności przez właściwe planowanie, realizację i koordynację działań na poziomie NDAP;
4) usystematyzowanie analizy, tj. zapewnienie powtarzalności i porównywalności wyników oceny ryzyka przeprowadzanej w różnych obszarach działalności NDAP;
5) precyzyjne określenie odpowiedzialności związanej z zarządzaniem poszczególnymi ryzykami;
6) możliwość działania w zmieniającym się otoczeniu faktycznym i prawnym.

2. Polityka realizowana jest w oparciu o:
1) planowanie strategiczne, które odnosi się do przeprowadzanej identyfikacji i analizy ryzyka;
2) planowanie operacyjne, które odnosi się do bieżącej identyfikacji i analizy ryzyka przez komórki organizacyjne;
3) ocenę ryzyka i podejmowanie działań zaradczych, zgodnie z przepisami Polityki.

3. Niezbędne warunki funkcjonowania Polityki to:
1) jasne (spójne) cele i zadania oraz mierzalne wskaźniki ich realizacji;
2) wskazanie, jaki poziom ryzyka jest akceptowalny dla wyznaczonych celów i zadań;
3) bieżący monitoring realizacji celów i zadań;
4) wysoka świadomość właścicieli ryzyk i umiejętne wykorzystanie wniosków z bieżącego monitoringu realizacji celów.

§ 6. 1. Proces zarządzania ryzykiem jest przeprowadzany w każdym roku w cyklach półrocznych:
1) pierwszy cykl dotyczy ryzyk, które mogą wystąpić w pierwszym półroczu;
2) drugi cykl dotyczy ryzyk, które mogą wystąpić w drugim półroczu.

2. Czynności w ramach każdego cyklu realizowane są następująco:

czynność w ramach procesu	odpowiedzialny za realizację	terminy graniczne	
		I. cykl	II. cykl

identyfikacja, analiza i ocena ryzyka w komórce organizacyjnej	właściciel ryzyka	pierwsza połowa stycznia	pierwsza połowa lipca
przygotowanie i przekazanie do pracownika realizującego zadania z zakresu kontroli zarządczej rejestrów ryzyk oraz informacji o stanie ryzyk wykazanych w poprzednim cyklu	właściciel ryzyka	pierwsza połowa stycznia	pierwsza połowa lipca
przygotowanie i przekazanie do pracownika realizującego zadania z zakresu kontroli zarządczej planu postępowania dla ryzyka nieakceptowalnego (jeśli wystąpiło) wraz z propozycją reakcji na to ryzyko	właściciel ryzyka	pierwsza połowa stycznia	pierwsza połowa lipca
przegląd poprzednio zgłoszonych ryzyk oraz stanu radzenia sobie z nimi i porównanie z aktualnie zgłoszonymi	pracownik realizujący zadania z zakresu kontroli zarządczej	druga połowa stycznia	druga połowa lipca
przygotowanie zbiorczego rejestru ryzyk oraz planu postępowania z ryzykiem nieakceptowalnym	pracownik realizujący zadania z zakresu kontroli zarządczej	druga połowa stycznia	druga połowa lipca
przekazanie zbiorczego rejestru oraz planu postępowania z ryzykiem nieakceptowalnym do Dyrektora Generalnego	pracownik realizujący zadania z zakresu kontroli zarządczej	druga połowa stycznia	druga połowa lipca
spotkanie z kierującymi (właścicielami ryzyk) i omówienie planu postępowania z ryzykiem nieakceptowalnym	Dyrektor Generalny NDAP	druga połowa stycznia	druga połowa lipca
pismo Dyrektora Generalnego do Naczelnego Dyrektora AP wraz z rekomendacjami ws. postępowania z ryzykiem nieakceptowalnym	Dyrektor Generalny NDAP	druga połowa stycznia	druga połowa lipca

decyzja Naczelnego Dyrektora Archiwów Państwowych w sprawie planu postępowania z ryzykiem nieakceptowalnym	Naczelny Dyrektor Archiwów Państwowych	po otrzymaniu rekomendacji	po otrzymaniu rekomendacji
poinformowanie właścicieli ryzyk o decyzji Naczelnego Dyrektora w sprawie planu postępowania z ryzykiem nieakceptowalnym	pracownik realizujący zadania z zakresu kontroli zarządczej	po decyzji Naczelnego Dyrektora	po decyzji Naczelnego Dyrektora
wdrożenie planu postępowania z ryzykiem nieakceptowalnym	właściciel ryzyka	po otrzymaniu informacji o decyzji Naczelnego Dyrektora	po otrzymaniu informacji o decyzji Naczelnego Dyrektora
bieżący monitoring	właściciel ryzyka	cały cykl	cały cykl

3. W spotkaniu Dyrektora Generalnego NDAP z właścicielami ryzyk mogą uczestniczyć inne osoby przez niego wskazane, w szczególności:

1) naczelnik komórki organizacyjnej NDAP koordynującej realizację kontroli zarządczej;

2) pracownik realizujący zadania z zakresu kontroli zarządczej.

§ 7. Odpowiedzialność za prawidłowy przebieg procesu zarządzania ryzykiem ponoszą:

1) Dyrektor Generalny NDAP, który odpowiada za zarządzanie ryzykiem na poziomie strategicznym m.in. przez:
   a) przygotowanie i realizację polityki zarządzania ryzykiem,
   b) nadzór i monitorowanie skuteczności procesu zarządzania ryzykiem,
   c) przedstawienie Naczelnemu Dyrektorowi rekomendacji dotyczących proponowanych rozwiązań;
2) właściciele ryzyk, którzy odpowiadają za zarządzanie ryzykiem m.in. przez:
   a) identyfikację, analizę i ocenę ryzyk z uwzględnieniem posiadanych środków kontroli,
   b) raportowanie o zmaterializowaniu się ryzyka,
   c) przygotowanie propozycji sposobu postępowania z ryzykiem,
   d) wdrożenie planu postępowania z ryzykiem,

e) monitorowanie ryzyka oraz dostarczenie na czas kompletnej i wiarygodnej informacji na temat ryzyka,

f) współpracę z pracownikiem NDAP realizującym zadania z zakresu kontroli zarządczej;

3) pracownik NDAP realizujący zadania z zakresu kontroli zarządczej, który odpowiada za koordynację procesu zarządzania ryzykiem na poziomie NDAP przez:

a) przekazywanie właścicielom ryzyka niezbędnych informacji w zakresie ryzyk oraz mechanizmów kontroli,

b) koordynację procesu analizy ryzyka w ramach poszczególnych cykli,

c) wspieranie Naczelnego Dyrektora Archiwów Państwowych i Dyrektora Generalnego NDAP w procesie zarządzania ryzykiem.

Rozdział 2

Realizacja

§ 8. 1. Szacowanie ryzyka to proces, na który składają się trzy główne elementy:

1) identyfikacja;

2) analiza;

3) ocena.

2. Proces przebiega według następującego schematu:

1) identyfikacja, w ramach której:

a) nazywane jest ryzyko i definiowany obszar, z jakiego ono pochodzi,

b) typuje się działania, w których może wystąpić ryzyko,

c) typuje się aktywa, których może dotyczyć ryzyko,

d) bada się, czy ryzyko mogło już wystąpić (zmaterializować się);

2) analiza, w ramach której:

a) bada się czynniki ryzyka (co może sprawić materializację),

b) bada się środki kontroli (posiadane zabezpieczenia);

3) ocena, w ramach której:

a) ocenia się prawdopodobieństwo wystąpienia ryzyka,

b) ocenia się, jaki wpływ na NDAP będzie mieć wystąpienie ryzyka,

c) ocenia się istotność ryzyka oraz w razie potrzeby tworzy się plan postępowania z ryzykiem, a ponadto można określić ryzyko szczątkowe, tzn. ocenić, czy oprócz profilaktyki możliwe są jeszcze inne działania.

§ 9. 1. Ryzyko identyfikuje się wyszukując, rozpoznając i opisując występujące lub możliwe do wystąpienia niebezpieczeństwa w obszarach działalności NDAP.

2. Istnieją dwa źródła ryzyka:

1) zagrożenia bezpośrednie (zdarzenia szkodliwe), które powodują, że cele i zadania NDAP nie zostaną osiągnięte;
2) szanse (zdarzenia korzystne), które dają możliwość skutecznego i efektywnego osiągnięcia celów i realizacji zadań (ryzyko utracenia korzyści).

3. Ryzyka bada się uwzględniając następujące poziomy:

1) stanowiska pracy i zakres zadań realizowanych na tych stanowiskach;
2) zadania bieżące komórki organizacyjnej;
3) działania w komórce organizacyjnej;
4) posiadane aktywa;
5) realizowane projekty;
6) zagrożenia związane z realizacją zadań komórki organizacyjnej;
7) wyniki szacowania ryzyka w nadzorowanym obszarze;
8) warunki współpracy z podmiotami zewnętrznymi oraz ich zmiany.

4. Identyfikowane ryzyka dzielą się na:

1) zewnętrzne, tj. pochodzące spoza NDAP i wywierające na nią wpływ
2) wewnętrzne, tj. powstające w NDAP.

5. Ryzyka, które wystąpią (zmaterializują się), wywołują określone skutki:

1) natychmiastowe (operacyjne), gdy konieczne jest zarządzenie nimi w celu minimalizacji szkody;
2) odłożone w czasie (biznesowe), np. stopniowa utrata dobrej reputacji.

6. Skutki natychmiastowe wystąpienia ryzyka klasyfikuje się jako:

1) bezpośrednie (np. poniesione nieuzasadnione koszty);
2) pośrednie (np. związane z naruszeniem prawa i procedur).

§ 10. 1. Obszary działalności NDAP, w ramach, których rozpoznaje się ryzyka, stanowią:

1) w ramach obszaru zarządzania:

a) gremia kolegialne,

b) organizacja,

c) zbiory aktów normatywnych, legislacja i obsługa prawna,

d) strategie, programy, planowanie, sprawozdawczość i analizy,

e) informatyzacja,

f) skargi, wnioski, interpelacje i inne wystąpienia,

g) zgłoszenia sygnalistów,

h) reprezentacja i promocja NDAP,

i) współdziałanie z innymi podmiotami,

j) kontrole, audyt i szacowanie ryzyka;

2) w ramach obszaru spraw kadrowych:

a) wyjaśnienia, interpretacje i opinie, dotyczące zagadnień z zakresu spraw kadrowych,

b) nawiązywanie, przebieg i rozwiązywanie stosunku pracy oraz innych form zatrudnienia,

c) ewidencja osobowa,

d) bezpieczeństwo i higiena pracy,

e) szkolenie i doskonalenie zawodowe osób zatrudnionych,

f) dyscyplina pracy,

g) działalność socjalna,

h) ubezpieczenia osobowe i opieka zdrowotna,

i) zapewnienie dostępności osobom ze szczególnymi potrzebami;

3) w ramach obszaru administrowania:

a) wyjaśnienia, regulacje, interpretacje i opinie dotyczące zagadnień z zakresu spraw administrowania,

b) inwestycje i remonty,

c) administrowanie i eksploatowanie obiektów,

d) gospodarka materiałowa,

e) transport, łączność oraz infrastruktura informatyczna i telekomunikacyjna,

f) ochrona obiektów i mienia oraz sprawy obronne,

g) zamówienia publiczne;

4) w ramach obszaru finansów:

a) wyjaśnienia, interpretacje, opinie dotyczące zagadnień z zakresu spraw finansowo-księgowych,

b) planowanie i realizacja budżetu,

c) rachunkowość i obsługa finansowa,

d) obsługa finansowa funduszy specjalnych, w tym zagranicznych,

e) opłaty i ustalanie cen,

f) inwentaryzacja,

g) dyscyplina finansów publicznych;

5) w ramach obszaru zasobu archiwalnego i dokumentacji o czasowym okresie przechowywania:

a) nadzór nad dokumentacją państwowych i samorządowych jednostek organizacyjnych,

b) ewidencja narastającego państwowego zasobu archiwalnego,

c) niepaństwowy zasób archiwalny,

d) powierzanie i użyczanie materiałów archiwalnych,

e) szkolenie archiwistów zakładowych,

f) postępowanie z dokumentacją o czasowym okresie przechowywania,

g) informacje o dokumentacji o czasowym okresie przechowywania;

6) w ramach obszaru gromadzenia i przekazywania materiałów archiwalnych:

a) gromadzenie, przekazywanie i przejmowanie materiałów archiwalnych,

b) przejmowanie materiałów reprodukowanych,

c) scalanie i rozmieszczanie państwowego zasobu archiwalnego,

d) przekazywanie materiałów archiwalnych innym instytucjom,

e) przechowywanie materiałów archiwalnych poza archiwami państwowymi;

7) w ramach obszaru opracowania zasobu archiwalnego:

a) metodyka opracowywania materiałów archiwalnych,

b) ewidencja zasobu archiwalnego,

c) rejestracja poloników;

8) w ramach obszaru zabezpieczania i udostępniania materiałów archiwalnych:

a) nadzór nad konserwacją zasobu archiwalnego,

b) reprografia, w tym digitalizacja;

c) ochrona materiałów archiwalnych,

d) korzystanie z zasobu archiwalnego,

e) udostępnianie materiałów archiwalnych,

f) usługi wspierające udostępnianie materiałów archiwalnych,

g) wypożyczanie materiałów archiwalnych,

h) realizacja kwerend,

j) zabezpieczanie, ewidencja i ochrona narodowego zasobu archiwalnego w instytucjach polonijnych;

9) w ramach obszaru działalności naukowej i wydawniczej:

a) działalność naukowa w archiwach państwowych,

b) wydawnictwa;

10) obszar dotacji przyznawanych przez Naczelnego Dyrektora Archiwów Państwowych.

2. Podczas identyfikowania możliwych ryzyk w obszarach bierze się pod uwagę także dostępne aktywa, które w wyniku zmaterializowania się ryzyka mogą ucierpieć, zostać nieprawnie udostępnione podmiotom trzecim lub utracone.

3. Aktywa opisuje się w zależności od przyjętych kryteriów w podziale na:

1) podstawowe i wspierające;

2) aktywa materialne i aktywa niematerialne.

4. Aktywa podstawowe stanowią:

1) osoby, tj. decydenci (ścisłe kierownictwo NDAP), zarządzający (kierujący komórkami organizacyjnymi NDAP) oraz pozostali pracownicy;

2) procesy i działania:

a) takie, których utrata uniemożliwia wypełnienie zadań NDAP,

b) niejawne,

c) zmodyfikowane i wywierające wpływ na realizację działań NDAP,

d) związane z wymogami prawnymi i umowami zawartymi przez NDAP,

e) informacje podstawowe związane z działalnością NDAP oraz dotyczące jej strategicznych kierunków,

f) dane wrażliwe, w tym osobowe,

g) informacje o dużych wartościach.

5. Aktywa wspierające stanowią:

1) sprzęt i oprogramowanie;

2) siedziba NDAP i jej lokalizacja (wszystkie budynki, istniejące strefy bezpieczeństwa fizycznego, urządzenia i systemy dostarczane przez operatorów telekomunikacyjnych, sieć energetyczna NDAP oraz rezerwowe źródła zasilania);

3) Naczelny Dyrektor Archiwów Państwowych jako centralny organ administracji rządowej i struktura organizacyjna, a także wykonawcy, z którymi NDAP zawarła umowy.

6. Aktywa materialne (nieruchomości, sprzęt i wyposażenie, gotówka itp.) dzielą się na:

1) widoczne;

2) niezbędne do zapewnienia bezawaryjnego funkcjonowania;

3) możliwe do zwartościowania;

4) powszechnie dostępne i łatwe w zbyciu;

5) objęte ochroną własności.

7. Aktywa niematerialne (wizerunek NDAP, wiedza pracowników, licencje, prawa autorskie, własność intelektualna, patenty, bazy danych i rejestry, pracownicy, współpracownicy i usługodawcy itp.) dzielą się na:

1) niewidoczne, trudno wymierne;

2) rzadkie, trudne do skopiowania;

3) możliwe do wykorzystania z ograniczeniami prawnymi.

8. Liczba zasobów, w których dostępne są aktywa, może mieć wpływ na ich bezpieczeństwo, przy czym rozproszenie aktywów utrudnia ich ewidencjonowanie i ochronę.

9. W przypadku aktywów, które powinny być dostępne, zwiększenie liczby miejsc, gdzie one się znajdują, wpływa na zwiększenie ich dostępności.

10. Lokalizując posiadane aktywa, bierze się pod uwagę liczbę zasobów, w których aktywa się znajdują oraz wpływ tej liczby na podatność aktywu, tzn. czy zwiększenie liczby miejsc zwiększa czy zmniejsza podatność aktywu, czy też nie ma na nią wpływu.

11. Określając wartości aktywów:

1) rozważa się, jaki wpływ na funkcjonowanie NDAP będzie miała ich utrata, awaria lub inne problemy z tym związane, przy czym im większy ten wpływ, tym większa wartość aktywów;

2) ocenia się wartość aktywów z punktu widzenia tego, jak ważne są dla realizacji celów i najlepiej wyraża się tę wartość w pieniądzu.

12. W przypadku aktywów niematerialnych, gdy trudno określić wartość kwotowo, można przyjąć inny sposób oceny wartości, tj. względną ocenę istotności aktywów w stosunku do pozostałych aktywów („istotniejsze niż", „mniej istotne niż").

§ 11. 1. Przy analizie poszczególnych ryzyk bierze się pod uwagę następujące kryteria:

1) czynniki ryzyka (podatność), czyli co może spowodować, że ryzyko się zmaterializuje;

2) możliwe do zastosowania środki kontroli (zabezpieczenia).

2. Czynnikami ryzyka (przyczynami możliwego wystąpienia ryzyka) są w szczególności:

czynnik ryzyka	przykłady
ludzie	niskie kwalifikacje pracowników
	brak procedur
	nieprzestrzeganie procedur
	brak upoważnienia do podejmowania kluczowych decyzji (również w sytuacji kryzysowej)
	niewłaściwa współpraca z innymi komórkami organizacyjnymi oraz podmiotami zewnętrznymi niedobór dostawców i usługodawców
	zła reputacja instytucji, kryzys wizerunkowy
procesy, systemy, zarządzanie	nieskuteczne mechanizmy kontroli realizacji zadań lub brak kontroli/nadzoru
	brak przypisanej odpowiedzialności
	usterki sprzętu i systemów
	brak planu zastępczego w sytuacji nadzwyczajnej

	brak zabezpieczenia budżetowego brak lub błędna sprawozdawczość
	przeszłe niepowodzenia w osiąganiu celów
	przeszłe przypadki nieprawidłowości lub nadużyć
zdarzenia zewnętrzne i czynności zlecone na zewnątrz	„siła wyższa”
	nietypowe zjawiska
	brak lub zła współpraca z podmiotem zewnętrznym
	brak umiejętności wykorzystania nowoczesnych technologii
	przekazanie odpowiedzialności za realizację na niewłaściwy podmiot
	niewystarczająca infrastruktura
	zmiany polityczne i naciski zewnętrzne
	zmiany prawne

3. Do oceny posiadanych środków kontroli ryzyka stosuje się następującą skalę:

nieskuteczne środki kontroli ryzyka	1 pkt	Środki kontroli ryzyka funkcjonują nieformalnie lub cechuje je bardzo wysoki potencjał do poprawy lub zastosowane zabezpieczenia nie mają wpływu na podatności.
średnia skuteczność środków kontroli ryzyka	2 pkt	Środki kontroli wprowadzono formalnie, stwierdzono nieznaczne uchybienia w stosowaniu, cechuje je niewielki potencjał do poprawy lub zastosowane zabezpieczenia w większości obszarów chronią przed wykorzystaniem podatności.
wysoka skuteczność środków kontroli ryzyka	3 pkt	Środki kontroli wprowadzono formalnie, nie stwierdzono uchybień w stosowaniu, są adekwatne i optymalne do stawianych przed nimi zadań lub zastosowane zabezpieczenia chronią skutecznie przed wykorzystaniem podatności.

§ 12. 1. Ocena ryzyka uwzględnia następujące elementy:

1) prawdopodobieństwo wystąpienia ryzyka;

2) wpływ, jaki będzie miało wystąpienie ryzyka na NDAP (komórkę organizacyjną).

2. Prawdopodobieństwo wystąpienia ryzyka szacuje się zgodnie z następującą tabelą:

średnie prawdopodobieństwo wystąpienia ryzyka	2 pkt	Wystąpienie ryzyka jest mało realne lub w ciągu ostatniego roku nie występowały zdarzenia związane z ryzykiem lub ryzyko materializowało się w ciągu ostatnich 3 lat. Wykorzystanie w sposób świadomy lub nieświadomy podatności jest mało realne.
wysokie prawdopodobieństwo wystąpienia ryzyka	3 pkt	Wystąpienie ryzyka jest realne lub w ciągu ostatniego roku występowały pojedyncze zdarzenia związane z ryzykiem lub ryzyko materializowało się w ciągu ostatniego roku. Wykorzystanie w sposób świadomy lub nieświadomy podatności jest realne.
bardzo wysokie prawdopodobieństwo wystąpienia ryzyka	4 pkt	Prawie pewne, że ryzyko wystąpi lub w ciągu ostatniego półrocza ryzyko materializowało się lub występowały liczne zdarzenia związane z ryzykiem. Wykorzystanie w sposób świadomy lub nieświadomy podatności jest prawie pewne.

3. W przypadku wyznaczania poziomu prawdopodobieństwa wystąpienia ryzyka (niskie/średnie/wysokie/bardzo wysokie), które może być wywołane przez wiele przyczyn, należy, wskazując poziom, odnieść się do tej przyczyny, która jest najbardziej realna i w największym stopniu przekłada się na prawdopodobieństwo wystąpienia analizowanego ryzyka.

4. Wpływ ryzyka ocenia się według następującej skali:

		Finanse	Prawo	Realizacja procesów i celów statutowych	Wizerunek
średni wpływ ryzyka	2 pkt	Odczuwalny wpływ na budżet komórki organizacyjnej	Niesystemowa niezgodność z procedurami i regulacjami wewnętrznymi bez	Utrudnienia w realizacji procesu powodujące zakłócenie lub opóźnienie	Pojedyncze negatywne informacje o działalności NDAP w mediach

na NDAP			wpływu na zgodność z przepisami prawa	w wykonaniu zadań lub realizacji celu komórki organizacyjnej lub zakłócenia w działalności odczuwalne dla ograniczonej liczby interesariuszy	lokalnych, regionalnych lub branżowych lub nie wywołuje zmniejszenia zaufania obywateli do NDAP
wysoki wpływ ryzyka na NDAP	3 pkt	Bardzo duży wpływ na budżet komórki organizacyjnej oraz zauważalny wpływ na budżet NDAP	Może powodować problemy z wywiązaniem się z obowiązków nałożonych prawem, niezgodność z postanowieniami umów lub systemową niezgodność z procedurami i regulacjami wewnętrznymi	Utrudnienia w realizacji kilku procesów lub duże opóźnienia w realizacji zadania, skutkujące zagrożeniem realizacji celów statutowych i ustawowych lub zakłócenia w działalności odczuwalne dla grupy interesariuszy	Negatywne informacje o działalności NDAP w mediach regionalnych, branżowych oraz w niewielkim stopniu w mediach ogólnopolskich o dużym zasięgu lub utrata zaufania obywateli do NDAP
bardzo wysoki wpływ ryzyka na NDAP	4 pkt	Znaczący wpływ na budżet NDAP	Wywołuje niezgodność z procedurami i regulacjami wewnętrznymi kwalifikowaną jako naruszenie przepisów prawa zagrożone karą lub niezgodność z postanowieniami	Wstrzymanie możliwości realizacji kluczowych procesów lub celów statutowych i ustawowych lub zakłócenia w działalności odczuwalne dla	Negatywne informacje o działalności NDAP w mediach ogólnopolskich o dużym zasięgu wymagające działań w celu poprawy utraconego wizerunku; trwała

			umów grożące procesem sądowym	większości interesariuszy	utrata zaufania obywateli

5. Poziom ryzyka może być wynikiem następującej identyfikacji:

1) średnie prawdopodobieństwo wystąpienia ryzyka x średni wpływ tego ryzyka na działalność = ryzyko na poziomie 4 pkt (akceptowalne);
2) wysokie prawdopodobieństwo wystąpienia ryzyka x średni wpływ tego ryzyka na działalność = ryzyko na poziomie 6 pkt (istotne);
3) bardzo wysokie prawdopodobieństwo wystąpienia ryzyka x średni wpływ tego ryzyka na działalność = ryzyko na poziomie 8 pkt (istotne);
4) średnie prawdopodobieństwo wystąpienia ryzyka x wysoki wpływ tego ryzyka na działalność = ryzyko na poziomie 6 pkt (istotne);
5) wysokie prawdopodobieństwo wystąpienia ryzyka x wysoki wpływ tego ryzyka na działalność = ryzyko na poziomie 9 pkt (istotne);
6) bardzo wysokie prawdopodobieństwo wystąpienia ryzyka x wysoki wpływ tego ryzyka na działalność = ryzyko na poziomie 12 pkt (nieakceptowalne);
7) średnie prawdopodobieństwo wystąpienia ryzyka x bardzo wysoki wpływ tego ryzyka na działalność = ryzyko na poziomie 8 pkt (istotne);
8) wysokie prawdopodobieństwo wystąpienia ryzyka x bardzo wysoki wpływ tego ryzyka na działalność = ryzyko na poziomie 12 pkt (nieakceptowalne);
9) bardzo wysokie prawdopodobieństwo wystąpienia ryzyka x bardzo wysoki wpływ tego ryzyka na działalność = ryzyko na poziomie 16 pkt (nieakceptowalne).

6. Podczas oceny bierze się pod uwagę najbardziej prawdopodobny skutek wystąpienia ryzyka. Jeżeli z ryzykiem nie wiąże się dany rodzaj skutku, wartość tego ryzyka przyjmuje się na poziomie 1 pkt.

7. Bazowym wzorem opisującym poziom ryzyka (istotność) jest następująca formuła wykorzystująca wartości punktowe prawdopodobieństwa i wpływu wystąpienia ryzyka:

WR = PR x W

gdzie:

WR – wartość (poziom) ryzyka

PR – prawdopodobieństwo wystąpienia ryzyka

W – wpływ wystąpienia ryzyka (maksymalna wartość)

gdzie:

Macierz ryzyka

PRAWDOPODOBIEŃSTWO:

Ś – średnie = 2 pkt

W – wysokie = 3 pkt

BW – bardzo wysokie = 4 pkt

PRAWDOPODOBIEŃSTWO

BW	8	12	16
W	6	9	12
Ś	4	6	8
	Ś	W	BW

WPŁYW:

Ś – średni = 2 pkt

W – wysoki = 3 pkt

BW - bardzo wysoki = 4 pkt WPŁYW

8. Jeżeli zaistnieje taka potrzeba, właściciel ryzyka konsultuje wartość punktową prawdopodobieństwa i wpływu z przedstawicielami innych komórek organizacyjnych NDAP.

9. Po zidentyfikowaniu poziomu (istotności) ryzyka na podstawie poniższej tabeli właściciel ryzyka planuje działanie:

POZIOM RYZYKA	OPIS DZIAŁANIA
ŚREDNI (Ś)	poziom ryzyka akceptowalny - działanie możemy przesunąć w czasie, ale wymaga okresowego monitorowania
WYSOKI (W)	poziom ryzyka istotny – działanie powinniśmy podjąć jak najszybciej, wymaga stałego monitorowania
BARDZO WYSOKI (BW)	poziom ryzyka nieakceptowalny- wymaga natychmiastowego działania (i wdrożenia planu postępowania z ryzykiem)

10. W przypadku, gdy wystąpi ryzyko akceptowalne, właściciel ryzyka:

1) uwzględnia je w rejestrze ryzyk;

2) na bieżąco je monitoruje;

3) nie musi go minimalizować (toleruje).

11. W przypadku, gdy wystąpi ryzyko istotne, właściciel ryzyka:

1) uwzględnia je w rejestrze ryzyk;

2) na bieżąco je monitoruje;

3) może uruchomić działania minimalizujące, o ile takie działanie jest możliwe.

12. W przypadku, gdy wystąpi ryzyko nieakceptowalne, właściciel ryzyka:

1) uwzględnia je w rejestrze ryzyk;

2) na bieżąco je monitoruje;

3) obligatoryjnie wypełnia plan postępowania z ryzykiem, o którym mowa w § 14 ust. 4, i przekazuje Dyrektorowi Generalnemu NDAP.

13. W odniesieniu do ryzyk można podjąć następujące działanie:

1) przeciwdziałanie ryzyku polegające na wdrożeniu mechanizmów kontroli, których celem jest ograniczenie ryzyka do poziomu akceptowalnego, podjęciu działań minimalizujących prawdopodobieństwo lub skutki wystąpienia ryzyka lub obu jednocześnie;

2) przesunięcie ryzyka polegające na odłożeniu w czasie wykonania zadań, z którymi się wiąże określone ryzyko;

3) transfer ryzyka (dzielenie ryzyka z inną stroną lub stronami) polegający na ograniczeniu prawdopodobieństwa i efektu wystąpienia danego zdarzenia przez przeniesienie ryzyka

w całości lub częściowo na podmiot zewnętrzny lub zleceniu innej instytucji realizacji zadań wspierających, np. outsourcing;

4) tolerowanie ryzyka polegające na niepodejmowaniu dodatkowych działań w odpowiedzi na ryzyko w sytuacji, gdy ryzyko jest zarządzane w sposób wystarczający lub modyfikacja ryzyka jest nieopłacalna, stanowiące akceptację ciężaru strat wynikających z konkretnego ryzyka, przy czym ryzyka skrajne, nieakceptowalne można zaakceptować w przypadku, gdy nie ma możliwości podjęcia działań ograniczających poziom danego ryzyka;

5) unikanie ryzyka polegające na nierozpoczynaniu lub niekontynuowaniu działań powodujących ryzyko (świadoma decyzja o nieangażowaniu się lub odejściu od ryzyka, eliminacja narażenia na konkretne ryzyko);

6) usunięcie źródła ryzyka polegające na działaniach, które mają wyeliminować źródła ryzyka czyli elementy, które same lub w połączeniu z innymi mają wewnętrzny potencjał, aby powodować powstanie ryzyka.

14. Opracowując działania minimalizujące ryzyko, należy rozważyć wdrożenie zabezpieczeń:

1) organizacyjnych (procedury);

2) technicznych (systemy);

3) fizycznych (zabezpieczenie).

15. Monitorowanie ryzyka polega na okresowym sprawdzeniu, czy:

1) status ryzyka się nie zmienił (zmaterializowane/niezmaterializowane);

2) poziom ryzyka się nie zmienił (akceptowalny/istotny/nieakceptowalny);

3) nie pojawiły się nowe ryzyka.

Rozdział 3

Rejestr ryzyk

§ 13. 1. Rejestr ryzyk, którego wzór stanowi załącznik nr 1 do Polityki, jest zbiorem ryzyk zidentyfikowanych w komórce organizacyjnej NDAP.

2. Rejestr ryzyk zawiera następujące dane:

1) nazwę wydziału/departamentu;

2) liczbę porządkową;

3) numer ryzyka;

4) obszar działalności;

5) obszar ryzyka;

6) nazwę ryzyka;

7) grupę aktywów, których dotyczy ryzyko;

8) informację, czy w poprzedniej analizie ryzyko było zgłoszone;

9) informację, czy od poprzedniej analizy ryzyko uległo materializacji lub wystąpiły istotne zdarzenia;

10) czynniki ryzyka;

11) informację o zastosowanych środkach kontroli;

12) prawdopodobieństwo wystąpienia ryzyka – wartość punktowa;

13) prawdopodobieństwo wystąpienia ryzyka – wartość opisowa;

14) wpływ wystąpienia ryzyka – wartość punktowa;

15) wpływ wystąpienia ryzyka – wartość opisowa;

16) poziom ryzyka (istotność) – w wartości punktowej;

17) poziom ryzyka (istotność) – w wartości opisowej;

18) poziom ryzyka, który właściciel mógłby zaakceptować – w wartości punktowej;

19) reakcja na ryzyko;

20) informację, czy dla ryzyka zostanie opracowany plan postępowania z ryzykiem.

3. Właściciel ryzyka przekazuje rejestr ryzyk pracownikowi realizującemu zadania z zakresu kontroli zarządczej. Następnie rejestry otrzymane z komórek organizacyjnych NDAP są przekazywane Dyrektorowi Generalnemu NDAP jako zbiorczy rejestr ryzyk.

Rozdział 4

Plan postępowania z ryzykiem nieakceptowalnym

§ 14. 1. Dla ryzyk ocenionych jako nieakceptowalne właściciel ryzyka obligatoryjnie przygotowuje plan postępowania z ryzykiem nieakceptowalnym, zwany dalej „planem postępowania z ryzykiem”, w ramach którego przedstawia propozycję działań zmierzających do zminimalizowania ryzyka.

2. W planie postępowania z ryzykiem właściciel ryzyka wskazuje status działań wobec każdego z tych ryzyk jako jedną z opcji:

1) działanie zgłoszone do planu i przed realizacją;

2) działanie w trakcie realizacji wraz z terminem ukończenia;

3) działanie wdrożone;

4) działanie wycofane z realizacji (wraz z uzasadnieniem powodu wycofania).

3. Za wdrożenie planów postępowania z ryzykiem oraz monitorowanie postępów we wdrażaniu planów odpowiada właściciel ryzyka.

4. Wzór formularza planu postępowania z ryzykiem stanowi załącznik nr 2 do Polityki.

	Opis ryzyka										Ocena ryzyka								
	l.p.	Numer ryzyka	Obszar działalności	Obszar ryzyka	Nazwa ryzyka	Grupa aktywów, których dotyczy ryzyko	Informacja czy ryzyko było zgłoszone przy poprzedniej analizie?	Informacja czy od ostatniej analizy ryzyko uległo materializacji lub wystąpiły istotne zdarzenia?	Czynniki ryzyka	Informacja o zastosowanych środkach kontroli ryzyka	Prawdopodobieństwo wystąpienia ryzyka - wartość punktowa	Prawdopodobieństwo wystąpienia ryzyka - wartość opisowa	Wpływ wystąpienia ryzyka - wartość punktowa	Wpływ wystąpienia ryzyka - wartość opisowa	Poziom ryzyka (istotność) - wartość punktowa	Poziom ryzyka (istotność) - wartość opisowa	Poziom ryzyka, który właściciel mógłby zaakceptować - wartość punktowa	Reakcja na ryzyko	Informacja czy dla ryzyka zostanie opracowany plan postępowania z ryzykiem?
Departament / Wydział																			

Załącznik nr 2

WZÓR

Plan postępowania z ryzykiem nieakceptowalnym

<table>
<tr><td>Przygotował (imię i nazwisko)</td><td colspan="2"></td></tr>
<tr><td>Komórka organizacyjna
(właściciel ryzyka)</td><td colspan="2"></td></tr>
<tr><td>Obszar działalności</td><td colspan="2"></td></tr>
<tr><td>Obszar ryzyka</td><td colspan="2"></td></tr>
<tr><td>Nazwa ryzyka</td><td colspan="2"></td></tr>
<tr><td>Poziom ryzyka</td><td colspan="2"></td></tr>
<tr><td>Skutki ryzyka</td><td colspan="2"></td></tr>
<tr><td>Działania zaplanowane/podjęte wobec ryzyka</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Aktualny status działań</td><td>☐ działanie zgłoszone do planu i przed realizacją</td><td>☐ działanie w trakcie realizacji i z określonym terminem ukończenia

planowany termin ukończenia działań minimalizujących (dzień, miesiąc, rok):</td></tr>
<tr><td>☐ działanie wdrożone</td><td>☐ działanie wycofane z realizacji wraz z uzasadnieniem
uzasadnienie:</td></tr>
<tr><td>Wymagany udział innych komórek organizacyjnych w realizacji działań</td><td>TAK
(nazwa komórki organizacyjnej, w jakim zakresie udział)</td><td>NIE</td></tr>
<tr><td>Rekomendacje Dyrektora Generalnego NDAP dla Naczelnego Dyrektora Archiwów Państwowych</td><td colspan="2">☐ rekomenduję zaproponowany sposób działania
☐ nie rekomenduję zaproponowanego sposobu działania</td></tr>
</table>