

ZARZĄDZENIE Nr 31/19
DYREKTORA CENTRUM USŁUG INFORMATYCZNYCH
W BIAŁYMSTOKU
z dnia 31 grudnia 2019 roku

**w sprawie określenia wytycznych w zakresie ustalenia systemu zarządzania
ryzykiem w Centrum Usług Informatycznych w Białymstoku**

Na podstawie art. 69 ust. 1 pkt 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019, poz. 869¹) oraz § 9 ust. 1, § 13 pkt 5 Statutu Centrum Usług Informatycznych w Białymstoku stanowiącego załącznik Nr 1 do uchwały Nr L/769/19 Rady Miasta Białystok z dnia 21 maja 2018 r. w sprawie utworzenia jednostki budżetowej Centrum Usług Informatycznych w Białymstoku oraz nadania jej statutu², § 6 ust. 4, § 11 pkt. 1 Regulaminu Organizacyjnego Centrum Usług Informatycznych w Białymstoku w związku z Komunikatem Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla jednostek sektora finansów publicznych (Dz. Urz. Ministra Finansów z 30 grudnia 2009 r., nr 15, poz. 84) oraz Komunikatem Nr 3 Ministra Finansów z dnia 16 lutego 2011 r. w sprawie szczegółowych wytycznych w zakresie samooceny kontroli zarządczej dla jednostek sektora finansów publicznych (Dz. Urz. Ministra Finansów z 11 marca 2011 r., Nr 2, poz. 11) oraz Komunikatem nr 6 Ministra Finansów z dnia 6 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem (Dz. Urz. Ministra Finansów z 18 grudnia 2012 r., poz. 56), zarządzam, co następuje:

§1

Określa się wytyczne w zakresie ustalenia systemu zarządzania ryzykiem w Centrum Usług Informatycznych w Białymstoku zgodnie z załącznikiem do niniejszego zarządzenia.

§2

Wykonanie zarządzenia powierzam Zastępcy Dyrektora, Głównemu Księgowemu oraz kierownikom komórek organizacyjnych .

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

¹ Zmiana tekstu jednolitego wymienionej ustawy została ogłoszona w Dz. U. z 2019 r. poz. 1622, 1649 i 2020.

² zmienionej uchwałą Nr X/136/19 Rady Miasta Białystok z dnia 15 kwietnia 2019 r. zmieniającej uchwałę w sprawie utworzenia jednostki budżetowej Centrum Usług Informatycznych w Białymstoku oraz nadania jej statutu zmienionej uchwałą Nr XVII/265/19 Rady Miasta Białystok z dnia 2 grudnia 2019r. zmieniającej uchwałę w sprawie utworzenia jednostki budżetowej Centrum Usług Informatycznych w Białymstoku oraz nadania jej statutu

Załącznik do zarządzenia Nr 31/19
Dyrektora Centrum Usług
Informatycznych w Białymstoku
z dnia 31 grudnia 2019 r. w sprawie
określenia wytycznych w zakresie
ustalenia systemu zarządzania
ryzykiem w Centrum Usług
Informatycznych w Białymstoku

WYTYCZNE

w zakresie ustalenia systemu zarządzania ryzykiem w Centrum Usług Informatycznych w Białymstoku

Rozdział I

POSTANOWIENIA OGÓLNE

1. Celem wytycznych jest:
 - 1) zapewnienie spójnego i jednolitego modelu systemu zarządzania ryzykiem w Centrum Usług Informatycznych w Białymstoku, zgodnego z powszechnie przyjętymi w jednostkach sektora finansów publicznych standardami kontroli zarządczej;
 - 2) podniesienie jakości kontroli zarządczej oraz zapewnienie prawidłowego jej przebiegu.
2. Wytyczne uwzględniają specyfikę zadań Centrum Usług Informatycznych w Białymstoku, które je wdraża i warunków, w których jednostka funkcjonuje.

Rozdział II

SYSTEM ZARZĄDZANIA RYZYKIEM

1. System kontroli zarządczej w Centrum Usług Informatycznych w Białymstoku bazuje m.in. na systemie zarządzania ryzykiem.
2. Zarządzanie ryzykiem w Centrum Usług Informatycznych w Białymstoku ma przyczynić się do poprawy funkcjonowania jednostki, we wszystkich obszarach zarządzania oraz ograniczyć ewentualne skutki zdarzeń do akceptowalnego poziomu, w szczególności w zakresie efektywnego zarządzania zasobami, zapewnienia ochrony majątku i efektywności finansowej oraz ochrony wizerunku w Centrum Usług Informatycznych w Białymstoku.
3. Ryzykiem jest zdarzenie o określonym prawdopodobieństwie (zdarzenie niepewne), którego wystąpienie może mieć negatywny wpływ na realizację założonych celów, planów i zadań w Centrum Usług Informatycznych w Białymstoku.
4. Na system zarządzania ryzykiem składa się: określenie celów i zadań, identyfikacja, analiza ryzyka jak i reakcja na ryzyko oraz monitorowanie i ocena. Takie podejście pozwoli zidentyfikować zagrożenia na które narażona jest jednostka, a w odpowiedzi na nie - podjąć działania zaradcze. W pierwszej kolejności należy:

- 1) określić cele i zadania Centrum Usług Informatycznych w Białymstoku w co najmniej rocznej perspektywie, a ich wykonanie należy monitorować za pomocą wyznaczonych mierników;
- 2) zapewnić odpowiedni system monitorowania realizacji celów i zadań jednostki;
- 3) przeprowadzić ocenę realizacji celów i zadań pod względem oszczędności, efektywności i skuteczności;
- 4) wskazać osoby odpowiedzialne za ich wykonanie.

Rozdział III

IDENTYFIKACJA RYZYKA

1. Przed przystąpieniem do identyfikacji ryzyka występującego w poszczególnych komórkach organizacyjnych CUI , dyrektor, jego zastępca, kierownicy ustalają listę celów i zadań do realizacji. Do ww. listy, co najmniej raz w roku, należy opracować wykaz ryzyk (zdarzeń niepewnych), wraz z funkcjonującymi jak i proponowanymi mechanizmami kontrolnymi, ograniczającymi występujące ryzyko. Zadaniem kierowników komórek organizacyjnych jest uzyskanie odpowiedzi na pytanie, co może w przyszłości nastąpić, gdy wyznaczony cel nie zostanie osiągnięty.

Przy identyfikacji ryzyka należy:

- 1) nie rzadziej niż raz w roku dokonywać identyfikacji ryzyka w odniesieniu do wyznaczonych celów i zadań;
- 2) zidentyfikowane ryzyka poddać analizie mającej na celu określenie prawdopodobieństwa wystąpienia danego ryzyka i możliwych jego skutków;
- 3) określić akceptowalny poziom ryzyka;
- 4) dokonać hierarchizacji ryzyka (uporządkować je malejąco według przyznanych ocen);
- 5) do każdego zidentyfikowanego ryzyka określić rodzaj wymaganej reakcji;
- 6) określić działania, które należy podjąć w celu zmniejszenia danego ryzyka do akceptowalnego poziomu.

Przykładowe kategorie ryzyka, które mogą wystąpić w Centrum Usług Informatycznych w Białymstoku przedstawia tabela stanowiąca załącznik nr 1 do wytycznych. Tabela nie określa zamkniętego katalogu ryzyka, które mogą wystąpić w ww. jednostkach.

Rozdział IV

ANALIZA RYZYKA

1. Każde zidentyfikowane ryzyko podlega analizie mającej na celu oszacowanie:
 - 1) prawdopodobieństwa jego wystąpienia (P) - ocena punktowa w skali od „1” do „5”;
 - 2) wpływu (skutku, strat), jaki będzie miało ewentualne wystąpienie tego zdarzenia (S) - ocena punktowa w skali od „1” do „5”.
2. Łączna relacja (iloczyn) tych dwóch wartości określa **istotność ryzyka** i obliczana jest

według wzoru:

$$\text{Istotność ryzyka} = P \times S$$

gdzie:

P - prawdopodobieństwo wystąpienia ryzyka;

S - wielkość straty, skutku, bądź wpływu, jaki będzie miało ewentualne wystąpienie tego zdarzenia.

3. Sposób określenia prawdopodobieństwa wystąpienia ryzyka obrazuje poniższa tabela:

% w ciągu roku

opis	Rzadkie	Mało prawdopodobne	Średnie	Prawdopodobne	Prawie pewne
P	0-20%	21-40%	41-60%	61-80%	81-100%
wartości	1	2	3	4	5

gdzie :

- 1) **rzadkie** - ryzyko wystąpi raz na 5 lat, bardzo mała szansa na wystąpienie w najbliższym roku;
- 2) **mało prawdopodobne** - ryzyko występuje średnio raz na 3 lata;
- 3) **średnie** - ryzyko występuje średnio raz na 2 lata;
- 4) **prawdopodobne** - ryzyko występuje średnio raz na rok lub raz na dwa lata (lub ryzyko będzie systematycznie narastać);
- 5) **prawie pewne** - ryzyko prawdopodobnie wystąpi w najbliższym roku budżetowym.

4. Do określenia wpływu (oddziaływania, skutku) ryzyka na realizację zadań stosuje się następujące definicje, gdzie przypisane im wartości odnoszą się do:

	1	2	3	4	5
Opis	Nieznaczne	Małe	Średnie	Poważne	Katastrofalne

gdzie:

- 1) **nieznaczne** - rozwiązanie problemu wymagało będzie nieznacznego nakładu czasu/zasobów. Problem nie spowoduje trwałej szkody i wywrze mały wpływ na wyniki finansowe;
- 2) **małe** - rozwiązanie problemu będzie wymagało pewnego nakładu czasu/zasobów. Usunięcie skutków (powstałych strat) będzie wymagało czasu. Może mieć wpływ na wyniki finansowe, których ranga będzie wymagała ujawnienia. Może spowodować zakłócenia w działalności;
- 3) **średnie** - rozwiązanie problemu będzie wymagało umiarkowanego nakładu czasu/zasobów - w tym kierownictwa wyższego szczebla. Usunięcie skutków (strat) będzie trudne. Wywrze wpływ na wyniki finansowe. Może doprowadzić do

niezrealizowania kluczowego celu;

- 4) **poważne** - rozwiązanie problemu będzie wymagało dużego nakładu czasu/zasobów - w tym kierownictwa wyższego szczebla. Usunięcie skutków (strat) będzie bardzo trudne lub nieraz wręcz niemożliwe. Wywrze istotny wpływ na wyniki finansowe i stanie się istotnym wydarzeniem publicznym. Prawdopodobnie doprowadzi do niezrealizowania kluczowego celu;
- 5) **katastrofalne** - rozwiązanie problemu będzie wymagało bardzo dużego nakładu czasu/zasobów - w tym kierownictwa wyższego szczebla. Usunięcie skutków (strat) będzie bardzo trudne lub wręcz niemożliwe. Wywrze istotny wpływ na wyniki finansowe i stanie się ważnym wydarzeniem publicznym. Doprowadzi do braku realizacji kluczowego celu.

5. Istotność ryzyka przedstawia poniższa macierz ryzyka:

Wpływ (skutek)

Katastrofalne- 5	5	10	15	20	Ryzyka w wysokie 25
Poważne - 4	4	8	12	16	20
Srednie - 3	3	<i>Ryzyko średnie</i>		12	15
Małe - 2	2	4	6	8	10
Nieznaczące -1	1	2	3	4	5
	Rzadkie 1	Mało prawdopodobne 2	Srednie 3	Prawdopodobne 4	Prawie pewne 5

Prawdopodobieństwo

6. Ryzykiem akceptowalnym jest ryzyko małe.
7. Ryzyko średnie jest sygnałem do podjęcia działań naprawczych.
8. Ryzyko wysokie jest ryzykiem nieakceptowalnym i wymaga podjęcia działań w celu zmniejszenia ryzyka do akceptowalnego poziomu.
9. Dyrektorzy i kierownicy komórek organizacyjnych CUI są zobowiązani udokumentować przeprowadzoną w podległej jednostce analizę ryzyka w szczególności poprzez utworzenie Rejestru ryzyka dla wyznaczonych celów i zadań na każdy kolejny rok.
10. Wzór Rejestru zidentyfikowanego ryzyka stanowi załącznik nr 2 do niniejszych wytycznych.

Kategorie ryzyka

Poniższa tabela przedstawia kategorie ryzyka wraz z przykładami dotyczącymi jego możliwych źródeł (przyczyn) oraz skutków. Tabela nie określa zamkniętego katalogu ryzyka.

Ryzyko finansowe	
Budżetowe	Związane z planowaniem dochodów i wydatków, dostępnością środków publicznych, dokonywaniem wydatków i pobieraniem dochodów.
Oszustwa i kradzieży	Związane ze stratą środków rzeczowych i finansowych będącą wynikiem przestępstwa lub wykroczenia.
Podlegające ubezpieczeniu	Związane ze stratami finansowymi, które mogą być przedmiotem ubezpieczenia np. ryzyko pożaru, wypadku.
Zamówień publicznych i zlecenia zadań publicznych	Związane z podejmowaniem decyzji oraz udzielaniem zamówień publicznych lub zlecaniem zadań publicznych innym podmiotom np. ryzyko naruszenia zasad, form lub trybu ustawy o zamówieniach publicznych.
Odpowiedzialności	Związane z obowiązkiem zapłaty kwot pieniężnych tytułem np. odszkodowań, odsetek karnych, kosztów procesowych. .
Realizacja programów współfinansowanych ze środków UE	Związane z wystąpieniem nieprawidłowości przy wykorzystaniu środków z UE.
Ryzyko dot. zasobów ludzkich	
Zarządzanie zasobami ludzkimi	Związane z liczebnością i kompetencjami pracowników, szkoleniami, wprowadzaniem nowych zadań bez zabezpieczenia etatowego.
Bhp	Związane ze zdrowiem pracowników i wypadkami przy pracy.
Ryzyko działalności	
Regulacji wewnętrznych	Związane z istnieniem i adekwatnością regulacji wewnętrznych.
Organizacji i podejmowania decyzji	Związane ze strukturą organizacyjną organizacją pracy oraz przekazywaniem obowiązków i uprawnień np. ryzyko nieprecyzyjnie określonych obowiązków, ryzyko braku formalnie powierzonych obowiązków, ryzyko nieodpowiedniej struktury organizacyjnej, ryzyko nieprawidłowo wydane decyzji.
Kontroli wewnętrznej	Związane z funkcjonowaniem systemu kontroli wewnętrznej np. ryzyko niedostatecznej kontroli, ryzyko nieskutecznych mechanizmów kontrolnych.
Informacji	Związane z jakością informacji na podstawie których podejmowane są decyzje nn. ryzyko braku komunikacji wewnętrznej i zewnętrznej.
Reputacji	Związane z reputacją CUI np. ryzyko negatywnych opinii.
Systemów informatycznych	Związane z używanymi w Urzędzie systemami i programami informatycznymi oraz ochroną zawartych w nich danych np. ryzyko awarii, ryzyko udostępnienia danych osobom nieuprawnionym, ryzyko nieuprawnionej modyfikacji danych.
Ryzyko zewnętrzne	
Infrastruktury	Związane z infrastrukturą np. wyposażeniem, bazą lokalową środkami transportu i środkami łączności.
Gospodarcze	Związane z czynnikami ekonomicznymi, np. kursy walut, inflacja.
Środowiska prawnego	Związane ze skomplikowaniem i zmianami prawa oraz niejednolitym orzecznictwem.

Rejestr ryzyka										
Identyfikacja ryzyka				Analiza ryzyka			Odpowiedź na ryzyko			
Lp-	Cel/Zadanie	Zidentyfikowane ryzyko - nazwa ryzyka	Opis ryzyka	Prawdopodobieństwo wystąpienia ryzyka (P)	Skutki wystąpienia ryzyka (S)	Istotność ryzyka (5x6)	Działania podjęte	Reakcja na ryzyko	Działania planowane	Właściciel ryzyka (osoba odpowiedzialna)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	9)	(10)	(11)
1.										
2.										

Legenda:

1. Liczba porządkowa.
2. **Cel/zadanie** — rozumiany jako mniejszy obszar działalności jednostki, w którym mogą wystąpić niepożądane zjawiska.
3. **Nazwa ryzyka** - ryzyko, które może wpłynąć na realizację celu bądź zadania.
4. **Opis ryzyka** - informacja, na czym polega zidentyfikowane ryzyko.
5. **Prawdopodobieństwo wystąpienia ryzyka (P)** - wartości przyznane w skali 1 do 5, zgodnie z hasłowym opisem zawartym w „wytycznych”.
6. **Skutki wystąpienia ryzyka (S)** - wartości przyznane w skali I do 5, zgodnie z hasłowym opisem zawartym w „wytycznych”.
7. **Istotność ryzyka - iloczyn skutków wystąpienia ryzyka i prawdopodobieństwa (P x S).**
8. **Działania podjęte** - działania już podjęte przez dyrektora jednostki organizacyjnej Urzędu lub kierownika miejskiej jednostki organizacyjnej w stosunku do zidentyfikowanego ryzyka, np. procedur)' postępowania (zarządzenia i instrukcje), nadzór funkcjonalny itd.
9. **Reakcja na ryzyko** - reakcja dyrektora na zidentyfikowane ryzyko.
Istnieją następujące metody reakcji na ryzyko:
 - a) kontrolowanie i przeciwdziałanie—**K**;
 - b) tolerowanie -**T**;
 - c) transfer ryzyka - **TR**
10. **Działania planowane** - to działania, które zamierza podjąć dyrektor w stosunku do zidentyfikowanego ryzyka. W przypadku, gdy działania podjęte są wystarczające i w opinii dyrektora nie ma potrzeby wprowadzania dodatkowych regulacji czy też działań należy wpisać w kolumnie: „kontynuacja” .
11. **Właściciel ryzyka (osoba odpowiedzialna)** - osoba, która jest odpowiedzialna za nadzór zagadnień w tym obszarze.