Załącznik nr 1 do Zarządzenia nr 172/16
Wojewody Opolskiego z dnia 30.11.2016

SYSTEM ZARZĄDZANIA RYZYKIEM W OPOLSKIM URZĘDZIE WOJEWÓDZKIM W OPOLU

I. Postanowienia ogólne

§ 1.1. Celem dokumentu jest przedstawienie, przyjętej w Opolskim Urzędzie Wojewódzkim - zwanym dalej „Urzędem", polityki zarządzania ryzykiem z wykorzystaniem systemowego narzędzia wspomagającego w postaci oprogramowania e-Risk.

2. Polityka zarządzania ryzykiem w Urzędzie ma się przyczynić do realizacji celów i zadań Urzędu w sposób uwzględniający kryteria oszczędności, efektywności i skuteczności.

3. Celem stosowania polityki zarządzania ryzykiem jest w szczególności: ograniczenie ryzyka, ochrona zasobów, systemów i procesów oraz zapewnienie kierownictwu Urzędu, uzyskania wczesnej informacji o zagrożeniach dla realizacji wyznaczonych celów i realizowanych zadań.

§ 2. Polityka zarządzania ryzykiem w Urzędzie określa:

1) uprawnienia i obowiązki uczestników procesu zarządzania ryzykiem;
2) rolę Zespołu ds. Zarządzania Ryzykiem w procesie zarządzania ryzykiem;
3) sposób postępowania przy identyfikacji, analizie i ocenie ryzyk - w aplikacji e-Risk;
4) możliwe reakcje na ryzyko;
5) monitorowanie, przegląd ryzyk i raportowanie;
6) katalog obszarów ryzyk z przypisanymi ryzykami ogólnymi występującymi w Urzędzie;
7) procedurę przebiegu procesu zarządzania ryzykiem w Urzędzie;
8) instrukcję oceny ryzyka w Urzędzie.

§ 3. Przez użyte w załączniku określenia należy rozumieć:

1) **ryzyko** - możliwość zaistnienia zdarzenia, które będzie miało negatywny wpływ na realizację celów i zadań Urzędu;
2) **zarządzanie ryzykiem -** ogół działań, będących elementem kontroli zarządczej, które mają:
   a) przyczynić się do zwiększenia prawdopodobieństwa osiągnięcia celów i realizacji zadań przez Urząd, poprzez podejmowanie działań nakierowanych na ich realizację oraz monitorowanie wszystkich działań z tym związanych,
   b) prowadzić do ograniczenia ewentualnych negatywnych skutków zdarzeń do akceptowalnego poziomu - w szczególności w zakresie efektywnego zarządzania zasobami, zapewnienia ochrony majątku i efektywności finansowej oraz ochrony wizerunku Urzędu;
3) **proces zarządzania ryzykiem -** następujące po sobie czynności polegające na identyfikacji i analizie ryzyka, jego szacowaniu, reakcji na ryzyko, wdrażaniu mechanizmów kontroli i monitoringu ryzyk, które wspierane są odpowiednimi działaniami w ramach zarządzania ryzykiem;
4) **kierujący komórką organizacyjną** - należy przez to rozumieć dyrektorów wydziałów i biur oraz pracowników kierujących innymi komórkami organizacyjnymi Urzędu;
5) **właściciel ryzyka** - osobę odpowiedzialną za dane ryzyko w Urzędzie, w tym dyrektorów wydziałów i biur oraz pracowników kierujących innymi komórkami organizacyjnymi Urzędu, zgodnie z przyjętym w Urzędzie podziałem zadań wynikającym z przepisów szczególnych i dokumentów organizacyjnych.

II. Uprawnienia i obowiązki uczestników procesu zarządzania ryzykiem

§ 4. Wojewoda Opolski jako kierownik jednostki zobowiązuje podległą kadrę kierowniczą oraz pracowników Urzędu do realizacji zarządzania ryzykiem, zgodnie z ustaloną polityką zarządzania ryzykiem.

§ 5. Zespół Audytu Wewnętrznego odpowiada za koordynację i monitorowanie systemu zarządzania ryzykiem, z działaniami pozostałych uczestników procesu zarządzania ryzykiem w Urzędzie, w tym za:

1) dokonywanie przeglądu sposobu, w jaki kierujący komórkami organizacyjnymi identyfikują i zarządzają ryzykiem;
2) dokonywanie przeglądu działań podejmowanych w związku z występującym ryzykiem i występowania, w toku tych działań, do kierujących komórkami organizacyjnymi z pytaniami i prośbami o wyjaśnienie kwestii budzących wątpliwości;
3) bieżącą ocenę działań podejmowanych przez kierujących komórkami organizacyjnymi z wymaganiami wynikającymi z niniejszego zarządzenia;
4) wykonywanie doradztwa dla kierujących komórkami organizacyjnymi z obszaru zarządzania ryzykiem.

§ 6. 1. Kierujący komórkami organizacyjnymi Urzędu zobowiązani są do zarządzania ryzykiem na poziomie operacyjnym, w ramach powierzonych im zadań.

2. Kierujący komórkami organizacyjnymi mają obowiązek zapewnienia podległym pracownikom możliwości formalnego zgłaszania zmian w zakresie zidentyfikowanych ryzyk lub innych istotnych problemów.

3. Kierujący komórkami organizacyjnymi, w przypadku wystąpienia ryzyka o najwyższym poziomie istotności (nieakceptowanego) mają obowiązek wprowadzenia dodatkowych mechanizmów kontrolnych zmierzających do redukcji ryzyka lub przeniesienia go do średniego poziomu istotności oraz wyznaczenia pracowników odpowiedzialnych za ich wdrożenie i określenia planowanego terminu wdrożenia proponowanego mechanizmu kontrolnego. Wprowadzone do aplikacji ryzyka o najwyższym poziomie istotności zostają wyświetlone w module „Monity" - oznaczonym kolorem czerwonym.

4. Kierujący komórkami organizacyjnymi, w przypadku wystąpienia ryzyka o średnim poziomie istotności (akceptowanego warunkowo) podejmują decyzję co do wprowadzenia dodatkowych mechanizmów kontrolnych polegających na podjęcia działań zmierzających do redukcji ryzyka, likwidacji ryzyka lub przeniesieniu ryzyka do niskiego poziomu istotności. Obowiązkowo są zobowiązani do bieżącego monitorowania zidentyfikowanego ryzyka.

5. Kierujący komórkami organizacyjnymi, w przypadku wystąpienia ryzyka o najniższym poziomie istotności (możliwego do zaakceptowania) podejmują decyzję o jego tolerancji na tym poziomie i bieżącego monitorowania.

§ 7.1. Pracownicy Urzędu zobowiązani są do zgłaszania swoim przełożonym informacji o zdarzeniach, które mogą doprowadzić do negatywnych skutków w działalności Urzędu, w tym o potencjalnych nowych ryzykach bądź problemach mogących mieć wpływ na powstanie nowych ryzyk lub poziom istotności ryzyk już istniejących oraz zdarzeń, które mogą naruszyć reputację Urzędu w zakresie, w jakim występują one w działaniach pracownika.

2. Ponadto pracownicy zobowiązani są znać i przestrzegać obowiązujące zasady zarządzania ryzykiem, a także powinni być świadomi potrzeby rozpatrzenia zidentyfikowanych ryzyk w formalnym procesie.

III. Rola Zespołu ds. Zarządzania Ryzykiem w procesie zarządzania ryzykiem

§ 8.1. W celu stworzenia warunków zapewniających skuteczne zarządzanie ryzykiem w Urzędzie działa Zespół ds. Zarządzania Ryzykiem zwany dalej „Zespołem".

2. Do zadań Zespołu, należy pełnienie funkcji doradczej dla Wojewody w zakresie podejmowania działań mających na celu zwiększenie prawdopodobieństwa osiągnięcia celów Urzędu i zapewnienia właściwego ładu organizacyjnego (governance) oraz wymagających wdrożenia odpowiednich planów zarządzania ryzykiem.

3. Wojewoda zarządzeniem powołuje członków Zespołu.

§ 9. 1. Zespół zwoływany jest co najmniej dwa razy w roku (lub w razie potrzeby częściej) w terminach wskazanych przez Przewodniczącego Zespołu.

2. Zespół, w toku swojej działalności:
   1) dokonuje przeglądu ryzyk występujących w Urzędzie o najwyższym i średnim poziomie istotności;
   2) dokonuje przeglądu stosowanych, jak i proponowanych do stosowania mechanizmów kontrolnych związanych ze zidentyfikowanymi ryzykami o najwyższym i średnim poziomie istotności;
   3) zajmuje stanowisko co do ryzyk wspólnych - bez względu na ich poziom istotności.

3. Zespół sporządza dla Wojewody Opolskiego:
   1) informacje na temat ryzyk o najwyższym poziomie istotności (nieakceptowanym);
   2) opinie doradcze w zakresie sposobu postępowania z takim ryzykiem.

4. W celu przygotowania informacji lub opinii dla Wojewody Opolskiego w zakresie ryzyk o najwyższym poziomie istotności Zespół dokonuje analizy informacji przedstawionych przez właścicieli ryzyk.

5. Dokonując analizy informacji w zakresie zidentyfikowanych ryzyk, przedstawionych przez właścicieli ryzyk, Zespół może korzystać z modułu „Analiza" dostępnego w aplikacji e-Risk Portal, umożliwiającego wygenerowanie zestawień danych z bazy danych w postaci tabeli, wykresu, macierzy ryzyka.

6. Decyzje podjęte przez Zespół przekazywane są do wykonania kierującym komórkami organizacyjnymi.

IV. Sposób postępowania przy identyfikacji, analizie i ocenie ryzyk w aplikacji e-Risk Portal

§ 10. 1. Identyfikacja ryzyka dokonywana jest na poziomie operacyjnym, raz w roku podczas przygotowywania propozycji do Rocznego Planu Działalności Urzędu. Zidentyfikowane ryzyka powinny zostać wprowadzone do aplikacji e-Risk Portal, nie później niż do 15 stycznia roku następnego.

2. Właściciele ryzyk w Urzędzie otrzymują dostęp do aplikacji e-Risk Portal.

3. Właściciel ryzyka może wyznaczyć pracownika wspierającego go w procesie zarządzania ryzykiem. Wyznaczony pracownik wykonuje wówczas powierzone przez właściciela ryzyka czynności w aplikacji e-Risk Portal udostępnionej właścicielowi ryzyka.

§ 11. 1. Pełne ryzyko na jakie narażony jest Urząd, zanim nie zostaną podjęte działania na rzecz jego złagodzenia, określa się jako ryzyko nieodłączne.

2. Ryzyko, które pozostaje po podjęciu działań, mających na celu jego złagodzenie przy założeniu, że są one skuteczne, określa się jako ryzyko rezydualne.

§ 12. 1. Identyfikacja, analiza i ocena ryzyk w Urzędzie dokonywana jest w aplikacji e-Risk Portal przez właściciela ryzyka lub osobę przez niego wskazaną. Zalogowania się do aplikacji e-Risk Portal należy wykonać z poziomu przeglądarki Mozilla Firefox, wpisując adres: erisk w oknie przeglądarki, a następnie wpisując login i hasło użytkownika. Po zalogowaniu należy zatwierdzić bazę danych.

2. W celu wprowadzenia do aplikacji e-Risk Portal zidentyfikowanego ryzyka w strukturze aplikacji z głównego menu znajdującego się po lewej stronie okna należy wybrać moduł: „Ryzyko". W module tym, po dokonaniu wyboru odpowiedniej komórki organizacyjnej, należy uzupełnić trzy formularze, znajdujące się w zakładkach pośrodku okna, określone jako:

1) Cele do realizacji;
2) Ryzyko;
3) Proponowane mechanizmy kontrolne.

§ 13. 1. W pierwszym formularzu pn. „Cele do realizacji” należy w polu tekstowym obiekt wprowadzić cel, a następnie określić charakter celu, korzystając z listy rozwijalnej, poprzez dokonanie wyboru: bieżący, archiwalny.

2. Widok celu archiwalnego może zostać ukryty dla właściciela ryzyka, będzie wówczas widoczny tylko w danych archiwalnych.
3. Ukrycie i przywrócenie widoku celu archiwalnego może zostać dokonane przez Zespół Audytu Wewnętrznego, w tym celu należy dokonać odpowiedniego zgłoszenia w systemie EZD, korzystając z „Formularza modyfikacji wprowadzonych danych w aplikacji e-Risk Portal”, stanowiącego załącznik nr 1 do Systemu zarządzania ryzykiem.
4. Wprowadzony cel należy zaznaczyć, aby powiązać go z kolejnym formularzem „Ryzyko”.

§ 14.1. Drugi formularz pn. „Ryzyko” umożliwia wprowadzenie zidentyfikowanego ryzyka na dwa sposoby: poprzez funkcję „Dodaj nowy obiekt” lub poprzez funkcję „Biblioteka”, przy czym każde wprowadzone ryzyko poprzez funkcję „Dodaj nowy obiekt” zostaje automatycznie wpisane do „Biblioteki” z wszystkimi przypisanymi do niego atrybutami i wartościami.

2. W drugim formularzu pn. „Ryzyko”, korzystając z funkcji „Dodaj nowy obiekt” należy:
   1) w polu tekstowym obiekt wprowadzić zidentyfikowane ryzyko;
   2) określić czy ryzyko jest aktualne, korzystając z listy rozwijalnej, poprzez dokonanie wyboru: aktualne, nieaktualne;
      - w przypadku dokonania wyboru: ryzyko nieaktualne, należy wskazać przyczynę usunięcia ryzyka,
      - widok ryzyka nieaktualnego może zostać ukryty dla właściciela, będzie wówczas widoczny tylko w danych archiwalnych,
      - ukrycie i przywrócenie widoku ryzyka nieaktualnego może zostać dokonane przez Zespół Audytu Wewnętrznego, w tym celu należy dokonać odpowiedniego zgłoszenia w systemie EZD, korzystając z „Formularza modyfikacji wprowadzonych danych w aplikacji e-Risk Portal”, stanowiącego załącznik nr 1 do Systemu zarządzania ryzykiem;
   3) korzystając z listy rozwijalnej przyporządkować zidentyfikowane ryzyko do określonych przez Zespół obszarów ryzyka z przypisanymi ryzykami ogólnymi występującymi w Urzędzie, stanowiącymi załącznik nr 3 do niniejszego zarządzenia;
   4) określić przyczyny i skutki zidentyfikowanego ryzyka;
   5) korzystając z listy rozwijalnej należy przeanalizować każde zidentyfikowane ryzyko, w celu oszacowania ryzyka nieodłącznego poprzez określenie prawdopodobieństwa jego wystąpienia (ocena punktowa w skali od 1 do 5) oraz wpływu jaki będzie miało ewentualne wystąpienie ryzyka (ocena punktowa w skali od 1 do 5);
   6) ryzyko nieodłączne zostanie oszacowane przez aplikację po zapisaniu wprowadzonych danych;
   7) określić występujące mechanizmy kontrolne dla zidentyfikowanych ryzyk;

8) korzystając z listy rozwijalnej należy przeanalizować ponownie każde zidentyfikowane ryzyko, w celu oszacowanie ryzyka rezydualnego poprzez określenie prawdopodobieństwa jego wystąpienia (ocena punktowa w skali od 1 do 5) oraz wpływu jaki będzie miało ewentualne wystąpienie ryzyka (ocena punktowa w skali od 1 do 5) z uwzględnieniem stosowanych mechanizmów kontrolnych;
9) ryzyko rezydualne zostanie oszacowane przez aplikację po zapisaniu wprowadzonych danych;
10) wprowadzone ryzyko należy zaznaczyć, aby powiązać je z kolejnym formularzem „proponowane mechanizmy kontrolne".

3. W drugim formularzu pn. „Ryzyko", korzystając z funkcji „Biblioteka" należy wybrać odpowiednie ryzyko, zostanie ono wówczas dodane z wcześniej przypisanymi do niego atrybutami i wartościami, które można dostosować do kontekstu zidentyfikowanego przez właściciela ryzyka, poprzez funkcję „Oceń". Wprowadzone poprzez „Bibliotekę" ryzyko należy zaznaczyć, aby powiązać je z kolejnym formularzem „Proponowane mechanizmy kontrolne".

§ 15.1. Trzeci formularz pn. „Proponowane mechanizmy kontrolne" wypełnia:
1) obligatoryjnie właściciel ryzyka na najwyższym poziomie istotności, w odniesieniu do § 6 ust. 3 zarządzenia;
2) fakultatywnie właściciel ryzyka na średnim poziomie istotności, w odniesieniu do § 6 ust. 4 zarządzenia;
3) właściciel ryzyka na najniższym poziomie istotności nie wypełnia formularza „Proponowane mechanizmy kontrolne", w odniesieniu do § 6 ust 5 zarządzenia.

2. Uzupełniając formularz „Proponowane mechanizmy kontrolne" należy opisać proponowany mechanizm kontrolny wprowadzony w celu zminimalizowania ryzyka rezydualnego, określić pracownika odpowiedzialnego za jego wdrożenie oraz wskazać planowany termin wdrożenia, a następnie dokonać wyboru, korzystając z listy rozwijalnej, nazwy komórki organizacyjnej odpowiedzialnej za wdrożenie proponowanego mechanizmu kontrolnego, co skutkuje zawiadomieniem w module „Monity" wybranej komórki organizacyjnej o wprowadzonym proponowanym mechanizmie kontrolnym.

§ 16.1. Istnieje możliwość usunięcia wprowadzonego do aplikacji e-Risk Portal obiektu (celu do realizacji, ryzyka, proponowanego mechanizmu kontrolnego).

2. Usunięcie wprowadzonego obiektu może zostać dokonane przez Zespół Audytu Wewnętrznego. W tym celu należy dokonać odpowiedniego zgłoszenia w systemie EZD, korzystając z „Formularza modyfikacji wprowadzonych danych w aplikacji e-Risk Portal", stanowiącego załącznik nr 1 do „Systemu zarządzania ryzykiem".

3. Usunięcie obiektu jest nieodwracalne, wraz z dokonaniem tej czynności kasowane są również atrybuty historyczne danego obiektu. Zaleca się usuwanie tylko błędnie wprowadzonych obiektów, natomiast w przypadku gdy obiekt jest nieaktualny proponuje się ukrycie jego widoku.

§ 17. 1. Wprowadzone w aplikacji e-Risk Portal ryzyka podlegają ocenie na dwóch poziomach: „Oceń" i ‚Zatwierdź ocenę. Pomimo, że uprawnienia do dokonania oceny i zatwierdzania są rozdzielone może je przeprowadzić jeden użytkownik. W przypadku wyznaczenia przez właścicieli ryzyk pracowników wspierających ich w procesie zarządzania ryzykiem, czynności te mogą być wykonywane rozłącznie.

2. Ocena może zostać przeprowadzone w formularzu „Ryzyko" lub w module „Monity":
1) przeprowadzając ocenę w formularzu „Ryzyko" należy odszukać i otworzyć podlegające ocenie ryzyko i poprzez wybranie funkcji „Oceń'' przejść do trybu oceny, wprowadzić ewentualne zmiany bądź zatwierdzić wprowadzone dane - po zapisaniu przycisk „Oceń" będzie nieaktywny i ocena nie może już zostać zmieniona, a ponowna ocena będzie możliwa w kolejnym terminie oceny, zgodnie z ustawioną kwartalną bądź miesięczną częstotliwością lub gdy ocena zostanie odrzucona na poziomie zatwierdzania;

2) przeprowadzając ocenę w module „Monity” należy w oznaczonym kolorem zielonym monicie pn. „Oceń” odnaleźć podlegające ocenie ryzyko i wprowadzić ewentualne zmiany bądź zatwierdzić wprowadzone dane - po zapisaniu monit nie będzie wyświetlany do czasu kolejnego terminu oceny ryzyka lub gdy ocena zostanie odrzucona na poziomie zatwierdzania;
3) dokonując oceny poprzez formularz „Ryzyko” lub korzystając z modułu „Monity” użytkownik może zapisać wersję roboczą oceny, jednak tak dokonana ocena nie będzie możliwa do zatwierdzenia na kolejnym poziomie, wyświetli się informacja, że wczytane zostały robocze wartości oceny;
4) dokonując oceny ryzyka (w trybie podglądu formularza i w analizie) do czasu zaakceptowania oceny nie zmieniają się wartości wprowadzonych atrybutów.

3. Zatwierdzenie oceny może zostać przeprowadzone w formularzu „Ryzyko” lub w module „Monity”:
1) zatwierdzając ocenę z poziomu formularza „Ryzyko” należy odszukać i otworzyć podlegającą zatwierdzeniu ocenę ryzyka i poprzez wybranie funkcji „Zatwierdź ocenę” przejść do trybu akceptacji wprowadzonych danych, zatwierdzając bez zmian albo wprowadzając samodzielnie ewentualne zmiany lub odrzucając ocenę;
2) zatwierdzając ocenę w module „Monity” należy w oznaczonym kolorem pomarańczowym monicie pn. „Zatwierdź ocenę” odnaleźć podlegającą zatwierdzeniu ocenę i zatwierdzić bez zmian albo wprowadzić samodzielnie ewentualne zmiany lub odrzucić ocenę;
3) po zatwierdzeniu oceny wartości w formularzu zostaną zmienione na te, które zostały wybrane podczas dokonywania oceny, po zapisaniu przycisk „Zatwierdź ocenę” będzie nieaktywny, a monit nie będzie wyświetlany.

4. Określone przez Zespół obszary ryzyk, stanowią załącznik nr 3 do „Systemu zarządzania ryzykiem”.

5. Po corocznej identyfikacji ryzyk przez komórki organizacyjne Urzędu, Zespół ds. Zarządzania Ryzykiem aktualizuje występujące w Urzędzie obszary ryzyk.

§ 18. Wyznaczanie celów, identyfikację i analizę ryzyka dokonuje się zgodnie z „Procedurą przebiegu procesu zarządzania ryzykiem”, stanowiącą załącznik nr 2 do zarządzenia.

§ 19. Punktową ocenę ryzyka dokonuje się zgodnie z „Instrukcją oceny ryzyka”, stanowiącą załącznik nr 3 do zarządzenia.

§ 20. 1. W identyfikacji ryzyka biorą udział wszyscy pracownicy Urzędu, zgłaszając swojemu bezpośredniemu przełożonemu zdarzenia, które mogą mieć negatywny wpływ na osiągnięcie celów i zadań.

2. Kierujący komórkami organizacyjnymi w ramach swoich uprawnień opracowują zasady wewnętrznej identyfikacji ryzyk przez podległych pracowników - na poziomie oddziałów. Zgłoszone przez pracowników ryzyka, podlegają analizie pod kątem istotności dla realizacji celów, dokonywanej przez kierujących komórkami organizacyjnymi.

V. Możliwe reakcje na ryzyko

§ 21.1. Przyjmuje się następujące sposoby postępowania z ryzykiem:
1) redukcję ryzyka - w przypadku podjęcia działań mających na celu zmniejszenie ryzyka;
2) tolerancję ryzyka - w przypadku nie podejmowania działań ze względu na niskie ryzyko lub gdy nie istnieją obiektywne możliwości przeciwdziałania ryzyku lub gdy koszty podjętych działań mogą przekroczyć przewidywane korzyści;
3) transfer ryzyka - polegający na przeniesieniu części odpowiedzialności za ryzyko na innych uczestników procesu zarządzania ryzykiem lub podmioty zewnętrzne;
4) likwidację ryzyka - polegającą na wyeliminowaniu ryzyka lub zaprzestaniu

ryzykownych działań;

5) przesunięcie w czasie - polegające na zaniechaniu w danym momencie działań rodzących zbyt duże ryzyko.

2. Redukcja ryzyka może polegać na obniżaniu poziomu istotności ryzyka lub zmianie jego wartości punktowej nie powodującej zmiany poziomu istotności ryzyka.

§ 22.1. W przypadku wystąpienia ryzyka o najwyższym poziomie istotności - ryzyka nieakceptowanego, decyzje co do sposobu postępowania podejmuje Dyrektor Generalny, w uzgodnieniu z właścicielem ryzyka, mając na uwadze wymienione w § 21 ust. 1 możliwe reakcje na ryzyko.

2. Ryzyko o średnim poziomie istotności jest ryzykiem akceptowanym warunkowo, należy je na bieżąco monitorować. Właściciel ryzyka może określić propozycje postępowania z zidentyfikowanym ryzykiem, mając na uwadze wymienione w § 21 ust. 1 możliwe reakcje na ryzyko.

3. Ryzyka o niskim poziomie istotności jest ryzykiem możliwym do zaakceptowania, nie wymagającym szczególnej uwagi i nadzoru. Właściciel ryzyka ma obowiązek na bieżąco monitorować, czy dane ryzyko nie wzrasta.

VI. Monitorowanie, przegląd ryzyk i raportowanie

§ 23. 1. Monitorowanie ryzyka jest procesem ciągłym i polega na bieżącym obserwowaniu zidentyfikowanych ryzyk, w celu określenia czy w trakcie realizacji celów i zadań ich punktowe oceny w zakresie istotności uległy zmianie. Odstępstwa w trakcie realizacji celów i zadań poddawane są identyfikacji i analizie celem podjęcia odpowiednich działań zaradczych.

2. Ryzyka powinny być monitorowane przez osoby odpowiedzialne za realizacje konkretnych celów i zadań, poprzez ustalenie i zgłoszenie przełożonemu informacji o zdarzeniach mogących negatywnie wpłynąć na realizację celów i zadań w kontekście zidentyfikowanych ryzyk.

3. Monitorowania ryzyk dokonuje się w aplikacji e-Risk Portal, nie częściej niż raz na kwartał, poprzez funkcję „Oceń" i „Zatwierdź ocenę". W przypadku ryzyk o najwyższym poziomie istotności konieczne jest comiesięczny monitoring ryzyk.

4. Właściciele ryzyk otrzymują w formie wiadomości e-mail odpowiednio kwartalne/ miesięczne powiadomienia przypominające o monitorowaniu ryzyk, wysyłane automatycznie z aplikacji e-Risk Portal.

§ 24. 1. Dwa razy w roku, po zakończeniu pierwszego półrocza oraz na przełomie listopada/grudnia każdego roku, kierujący komórkami organizacyjnymi Urzędu powinni organizować przegląd ryzyk.

2. Przegląd ryzyk polega na spotkaniu kierującego komórką organizacyjną z podległą kadrą kierowniczą oraz osobami zajmującymi samodzielne stanowiska pracy, w zakresie zidentyfikowanych ryzyk.

3. Podczas przeglądu, powinny zostać omówione wszystkie ryzyka występujące w kierowanej komórce organizacyjnej, zwłaszcza ryzyka zaliczone do ryzyk o najwyższym i o średnim poziomie istotności.

4. Przegląd ryzyk polega na analizie zidentyfikowanych ryzyk, a następnie wyciągnięciu wniosków, czy dane ryzyko jest aktualne, czy jest prawidłowo oszacowane oraz czy pozostaje na takim samym poziomie, mimo podjętych działań.

5. Po przeprowadzeniu Przeglądu ryzyk właściciel ryzyka wypełnia formularz „Raport monitoringu ryzyk i bieżącej oceny realizacji celów i zadań w kierowanej komórce organizacyjnej", który stanowi załącznik nr 2 do „Systemu Zarządzania Ryzykiem w Opolskim Urzędzie Wojewódzkim" i przekazuje go w systemie EZD do Zespołu Audytu

Wewnętrznego. O terminie przekazania w/w Raportu pracownik Zespołu Audytu Wewnętrznego informuje kierujących wydziałami/biurami OUW poprzez system EZD.

6. Zespół Audytu Wewnętrznego na podstawie przekazanych przez Wydziały i Biura OUW „Raportów monitoringu ryzyk i bieżącej oceny realizacji celów i zadań w kierowanych komórkach organizacyjnych”, sporządza raport zbiorczy z Przeglądu Ryzyk w Opolskim Urzędzie Wojewódzkim, który przedkładany jest Wojewodzie Opolskiemu.

Załącznik nr 1
do „Systemu zarządzania ryzykiem
w Opolskim Urzędzie Wojewódzkim w Opolu"

FORMULARZ MODYFIKACJI wprowadzonych danych w aplikacji e-Risk Portal

Proszę o dokonanie następujących zmian w aplikacji e-Risk Portal w koncie użytkownika ..... w formularzu:
(proszę podać nazwę komórki organizacyjnej)

1) **Cele do realizacji** (proszę wypełnić właściwe)

- Usunięcie błędnie wprowadzonego celu
  Opis:…….
- Zablokowanie widoku archiwalnego celu
  Opis: …….
- Przywrócenie widoku archiwalnego celu
  Opis: …….

2) **Ryzyka / Proponowane mechanizmy kontrolne** (proszę wypełnić właściwe)

- Usunięcie błędnie wprowadzonego ryzyka /mechanizmu kontrolnego
  Opis: …….
- Zablokowanie widoku nieaktualnego ryzyka / mechanizmu kontrolnego
  Opis: …….
- Przywrócenie widoku nieaktualnego ryzyka / mechanizmu kontrolnego
  Opis: …….

3) **Inne zmiany:**

Opis: **…….**

(podpis właściciela ryzyka)

Opole, dn……..

Załącznik nr 2
do „Systemu zarządzania ryzykiem
w Opolskim Urzędzie Wojewódzkim w Opolu"

Raport monitoringu ryzyk i bieżącej oceny realizacji celów i zadań w kierowanej komórce organizacyjnej

Półroczny / Roczny Przegląd Ryzyk	**Rok**
Właściciel ryzyka (komórka organizacyjna):	

I. Informacja na temat potencjalnych zagrożeń przy realizacji celów i zadań

Czy w okresie ……. półrocza 20 …. r w nadzorowanym przeze mnie obszarze działalności OUW :

- zostały zrealizowane cele i zadania wynikające z Rocznego Planu Działalności Urzędu ?

  TAK □ NIE □

- wystąpiły ryzyka wskazane w Wydziałowym Rejestrze Ryzyk ?

  TAK □ NIE □

- wystąpiły ryzyka wskazane w Rejestrze Ryzyk występujących w OUW ?

  TAK □ NIE □

- zmienił się poziom istotności zidentyfikowanych zagrożeń ?

  TAK □ NIE □

- zidentyfikowano nowe zagrożenia, które nie byłyby ujęte w Wydziałowym Rejestrze Ryzyk oraz w Rejestrze Ryzyk Występujących w OUW i poprzez swoje wystąpienie mogłyby zagrozić realizacji celów i zadań Urzędu ?

  TAK □ NIE □

II. Działanie/proces w jakim występują zagrożenia, informacja na temat podjętych działań

Czy w analizowanym okresie w nadzorowanym przeze mnie obszarze działalności wystąpiły ryzyka ?

TAK □ NIE □

I. Niezrealizowany cel :

……..

1. **Ryzyko** (opis z Wydziałowego Rejestru Ryzyk):…….

   a. Przyczyny wystąpienia : ……..
   b. Skutki wystąpienia : ……..
   c. Proponowane działania :……..
   d. Podjęte przeciwdziałania……..

Czy ryzyko w sposób poważny zagraża realizacji celów i zadań Urzędu ?

TAK □ NIE □

II. Niezrealizowany cel :

……..

Ryzyko (opis z Wydziałowego Rejestru Ryzyk):…….

   e. Przyczyny wystąpienia : ……..
   f. Skutki wystąpienia : ……..
   g. Proponowane działania :……..
   h. Podjęte przeciwdziałania……..

Czy ryzyko w sposób poważny zagraża realizacji celów i zadań Urzędu ?

TAK □ NIE □

III. Propozycje aktualizacji/ usprawnień Systemu Zarządzania Ryzykiem w OUW

1. **Propozycje aktualizacji obszarów ryzyk**

TAK □ NIE □

Opis……

2. **Propozycje zgłoszenia nowych ryzyk** zidentyfikowanych w nadzorowanym obszarze działania Urzędu **(informacje o nowych zidentyfikowanych ryzykach należy dodatkowo złożyć w formie wydziałowego rejestru ryzyk wygenerowanego z systemu e-Risk).**

TAK □ NIE □

3. Działanie/ proces w jakim występuje możliwość usprawnienia

Proponowane działania: ……..

Spodziewane efekty ……..

4. Efekty działań eliminujących, podjętych w przypadku ryzyk, które wystąpiły w poprzednim okresie sprawozdawczym

Czy podjęte działania przynoszą spodziewane efekty ?

TAK □ NIE □

Opis……...

Czy podjęte działania są wystarczające ?

TAK □ NIE □

Opis……...

Czy istnieje konieczność podejmowania jakichkolwiek działań?

TAK □ NIE □

Opis……...

Czy wydziałowy rejestr ryzyk w programie e-RISK został zaktualizowany ?

TAK □ NIE □

Niniejsze sprawozdanie opiera się na mojej ocenie i informacjach dostępnych w czasie jego sporządzania pochodzących z :

- ☐ Bieżącego monitoringu, Rocznego Planu Działalności Urzędu, sprawowanego nadzoru kierowniczego, Wydziałowego Rejestru Ryzyka, itp.
- ☐ Wyników audytu wewnętrznego
- ☐ Wyników samooceny kontroli zarządczej
- ☐ Wyników kontroli wewnętrznych
- ☐ Wyników kontroli zewnętrznych
- ☐ Innych źródeł informacji (należy wymienić):……...

Opole, dn……

……..
podpis osoby składającej raport

Załącznik nr 3
do „Systemu zarządzania ryzykiem
w Opolskim Urzędzie Wojewódzkim w Opolu"

Tabela 1: Katalog obszarów ryzyk z przypisanymi ryzykami ogólnymi występującymi w Opolskim Urzędzie Wojewódzkim w Opolu

Na podstawie zidentyfikowanych ryzyk w poszczególnych komórkach organizacyjnych Urzędu, Zespół ds. Zarządzania Ryzykiem opracował katalog obszarów ryzyk - jako formę wsparcia przy identyfikacji ryzyk, przeznaczoną dla uczestników procesu zarządzania ryzykiem.

W celu pogrupowania zidentyfikowanych ryzyk wzbogacono katalog obszarów ryzyk o ryzyka ogólne.

Docelowo poprowadzone zostaną prace nad dalszym doskonaleniem obszarów ryzyk oraz wpisujących się w zidentyfikowane obszary - ryzyk ogólnych.

Przedstawiona tabela nie określa zamkniętego katalogu, uczestnicy procesu identyfikując nowe ryzyka mogą je zgłaszać do zbiorczej bazy prowadzonej przez Zespół Audytu Wewnętrznego.

Lp.	Obszary ryzyk	Ryzyka ogólne
1.	**Nieprawidłowa realizacja zadań Wojewody** **Realizacja zadań**	1. Niewykonanie operatów szacunkowych, określających wartość przejętych nieruchomości stanowiących podstawę ustalenia słusznego odszkodowania 2. Nieterminowe lub wadliwe wydanie istotnych decyzji lub umów o znaczących skutkach finansowych 3. Opublikowanie wadliwych aktów prawnych 4. Brak wiedzy dotyczący zadań do realizacji (np. brak wiedzy o zmianach w przepisach prawa) 5. Niewłaściwe działania organów kontroli 6. Naruszenie ustawy o zamówieniach publicznych 7. Niewykorzystanie środków dotacji budżetowych 8. Niezrealizowanie planu kontroli *i* audytu 9. Brak realizacji, nieterminowa lub nieprawidłowa realizacja zadań Wojewody
2.	**Naruszenie wizerunku administracji rządowej Wizerunek**	1. Brak reakcji lub opóźniona reakcja na zdarzenia kryzysowe oraz wydarzenia wywołujące wysoce negatywne reakcje społeczne 2. Wadliwa analiza przekazywanych uchwał organów stanowiących samorządów o dużym znaczeniu 3. Wadliwe lub nieterminowe decyzje wydziałów urzędu 4. Wzrastająca liczba uzasadnionych skarg 5. Niewłaściwa obsługa klienta zewnętrznego 6. Istotne naruszenie zasad etyki w służbie cywilnej 7. Brak przekazywania informacji o zaistniałych zagrożeniach do służb prasowych Wojewody 8. Niewłaściwe monitorowanie doniesień medialnych przez służby prasowe Wojewody 9. Brak realizacji zadań będących w obszarze zainteresowań opinii publicznej 10. Utrata informacji zawartych w dokumentach przechowywanych w Urzędzie

3.	**Zagrożenie finansowe**	1. Zachwianie równowagi budżetowej - strony wydatkowej 2. Zakłócenie płynności finansowej 3. Nieosiągnięcie planowanego poziomu dochodów budżetu państwa 4. Niedobór środków finansowych na wynagrodzenia, związany z zakończeniem realizacji projektów, zmianą przepisów prawa 5. Niecelowe i nieoszczędne dokonywanie wydatków publicznych, z pominięciem zasad uzyskiwania najlepszych efektów z danych nakładów, służących osiągnięciu założonych celów, a także w sposób niepozwalający na terminową realizację zadań 6. Niedobór środków finansowych w stosunku do planu na realizację zadań modernizacyjnych.
4.	**Nieprawidłowe zarzadzanie zasobami ludzkimi**	1. Wadliwe przeprowadzenie postępowania naborów i konkursów 2. Brak właściwego systemu motywacyjnego (system finansowy i niefinansowy) 3. Nieprawidłowy proces oceny pracowników 4. Nierealizowanie Programów Indywidualnego Rozwoju Zawodowego 5. Brak powołania organu przeciwdziałającego mobbingowi i brak ustalonych zasad antymobbingowych. 6. Realizacja zadań przez pracowników nie posiadających właściwych kwalifikacji
5	**Wystąpienie awarii lub nieprawidłowości w zarządzaniu infrastrukturą informatyczną i techniczną Urzędu**	1. Poważna awaria systemu informatycznego 2. Wystąpienie naturalnych zdarzeń losowych (np. powódź, pożar) i zdarzeń krytycznych zagrażających życiu i zdrowiu (np. bezpośrednia napaść, wybuch, atak terrorystyczny) 3. Nieprzestrzeganie zasad polityki bezpieczeństwa 4. Udostępnienie danych z systemu informatycznego 5. Brak możliwości stworzenia lub utrzymania rejestrów i zbiorów (np. zbiór meldunkowy) 6. Wadliwe umowy serwisowe w obszarze ochrony danych 7. Wystąpienie przerw w dostawie mediów 8. Awarie i uszkodzenia sprzętu 9. Brak odpowiedniego sprzętu 10. Niewłaściwe zarządzanie środowiskiem pracy (porażenie prądem, brak szkoleń pracowników z obsługi sprzętu przeciwpożarowego, przepisów BHP)
6.	**Nieprawidłowości w wykonywaniu kontroli zarządczej**	1. Brak RPDZ Urzędu 2. Brak właściwej koordynacji RPDZ i zarządzania ryzykiem 3. Niezgodność realizacji z założeniami dokumentu 4. Brak monitorowania RPDZ Urzedu 5. Nierzetelna ocena materiału dowodowego przy sporządzaniu decyzji, umów i porozumień 6. Nie zapewnienie ciągłości działalności (w tym przeciążenie stanowisk pracy, brak lub ograniczona możliwość realizacji podstawowych zadań)