**Załącznik do zarządzenia Nr 713/2022/P**

**Prezydenta Miasta Poznania**

**z dnia 22.09.2022 r.**

**PROCES ZARZĄDZANIA RYZYKIEM W MIEŚCIE**

**§ 1**

**(Cel procesu zarządzania ryzykiem)**

Celem procesu zarządzania ryzykiem jest zwiększenie prawdopodobieństwa realizacji celów strategicznych, zadań budżetowych oraz należytej ochrony zasobów, w tym czynności przetwarzania, w sposób oszczędny, terminowy, efektywny i zgodny z prawem poprzez wprowadzenie jednolitego i powszechnego sposobu analizy ryzyka oraz określenie związanych z tym obowiązków, tak aby ograniczyć możliwość wystąpienia dowolnego zdarzenia, działania lub zaniechania działania, którego skutkiem może być zagrożenie (szkoda) lub niewykorzystana szansa.

**§ 2**

**(Proces zarządzania ryzykiem)**

# 1. Proces zarządzania ryzykiem obejmuje:

1) ustalenie kontekstu (otoczenia);

# identyfikację i analizę ryzyka;

# reakcję na ryzyko;

# dokumentowanie i monitorowanie;

# komunikację.

# Do zarządzania ryzykiem w Mieście stosuje się przeznaczone do tego oprogramowanie, tj. odpowiednio:

# dla ryzyk do zadań budżetowych procesowych (typu B);

# dla ryzyk do zadań budżetowych projektowych (typu P);

# dla ryzyk do zasobów lub czynności przetwarzania (typu BI);

# dla ryzyk celu i priorytetów strategicznych typu S (typu S);

# Szczegółowe wytyczne dotyczące obsługi oprogramowania przeznaczonego do zarządzania ryzykiem w Mieście określa Pełnomocnik Prezydenta ds. systemu zarządzania w Instrukcji obsługi modułu do zarządzania ryzykiem w Mieście. Za rozpowszechnienie ww. instrukcji w wydziałach Urzędu oraz miejskich jednostkach organizacyjnych odpowiedzialny jest Wydział Organizacyjny (dokument dostępny jest na stronie głównej aplikacji Smarter).

**Dział I**

**Zarządzanie ryzykiem na poziomie operacyjnym**

**§ 3**

**(Ustalenie kontekstu)**

1. Ustalenie kontekstu (otoczenia) na poziomie operacyjnym to zdefiniowanie podstawowych zasad i kryteriów potrzebnych do zarządzania ryzykiem, określenia jego zakresu i granic oraz ustanowienie odpowiedniej struktury organizacyjnej do jego realizacji.
2. Kontekst ustala się poprzez identyfikację parametrów wpływających na poziom istotności ryzyka. Wyróżnia się parametry:

1) wewnętrzne – środowisko wewnętrzne, w którym organizacja dąży do osiągnięcia swoich celów (m.in. ład organizacyjny, kultura organizacyjna, struktura organizacyjna, polityki, cele i strategie, zadania, zasoby i wiedza, mechanizmy kontroli, systemy informatyczne, przepływ informacji, sytuacja finansowa, normy, wytyczne i modele przyjęte przez organizację);

2) zewnętrzne – środowisko zewnętrzne, w którym organizacja dąży do osiągnięcia swoich celów (m.in. środowisko kulturowe, społeczne, polityczne, prawne, regulacyjne, technologiczne, ekonomiczne, naturalne, a także inne czynniki i trendy mające wpływ na cele organizacji oraz relacje z klientamiUrzędu lub m.j.o.).

**§ 4**

**(Identyfikacja i analiza ryzyka)**

1. Identyfikacja ryzyka następuje poprzez analizę ustalonego kontekstu (otoczenia) wydziału, m.j.o. lub zespołu projektowego, weryfikację tych parametrów, które mogą przyczyniać się do pojawienia się ryzyka w przyszłości, oraz badanie i zbieranie informacji o rozpoznanym ryzyku w: wydziale, m.j.o., realizowanym projekcie, zasobie albo czynności przetwarzania. Ryzyko może być rozpoznane jako zagrożenie lub niewykorzystana szansa.
2. Podczas identyfikacji ryzyka należy uwzględnić w szczególności:
3. cel główny i cele szczegółowe wynikające z priorytetów strategicznych Miasta;
4. cele zadań budżetowych oraz inne cele wydziału lub m.j.o.;
5. zidentyfikowane w organizacji podatności oraz stosowane zabezpieczenia w obszarze bezpieczeństwa informacji w organizacji;
6. wszelkie rekomendacje stanowiące wytyczne w zakresie zabezpieczeń prawnych, informatycznych oraz organizacyjnych;
7. rejestr incydentów;
8. planowane działania w zakresie usprawnień zasobów;
9. wyniki audytów wewnętrznych i kontroli wewnętrznych oraz wyniki kontroli zewnętrznych związane w szczególności z osiąganiem celów i realizowaniem zadań budżetowych;
10. wyniki przeprowadzonej samooceny funkcjonowania kontroli zarządczej;
11. wyniki wdrożenia reakcji na ryzyko z poprzedniego roku kalendarzowego podjętej lub ustanowionej w celu ograniczenia lub przeciwdziałania jego wystąpieniu.
12. Zaleca się korzystać z metod wspomagających identyfikację ryzyka, takich jak burza mózgów, diagram Ishikawy, oraz przeprowadzać identyfikację ryzyka w grupach składających się z przedstawicieli różnych poziomów struktury organizacyjnej.
13. W terminach wskazanych w § 7 identyfikuje się ryzyka na rok następny. Polega to na przeglądzie ryzyk wskazanych w oprogramowaniu przeznaczonym do zarządzania ryzykiem, w szczególności na analizie mającej na celu sprawdzenie, czy zidentyfikowane ryzyka przestaną istnieć w roku następnym lub czy mogą wystąpić nowe ryzyka, które zmaterializują się w kolejnym roku.
14. Identyfikacja i analiza ryzyka dokonywana jest zgodnie z Instrukcją, o której mowa   
    w § 2 ust. 3. Instrukcja podzielona została na rozdziały dotyczące odpowiednio:
15. nadawania uprawnień do oprogramowania przeznaczonego do zarządzania ryzykiem   
    w Mieście;
16. zadań budżetowych procesowych (typu B);
17. zadań budżetowych projektowych (typu P);
18. zasobów i czynności przetwarzania (typu BI).

**§ 5**

**(Próg akceptowalności ryzyka)**

1. Przez próg akceptowalności ryzyka należy rozumieć taki poziom jego wartości, jaki organizacja jest gotowa przyjąć i przy którym nie jest wymagane podejmowanie reakcji na ryzyko.
2. Ryzykiem akceptowalnym jest ryzyko, którego poziom osiągnął wartość „ryzyko znikome” lub „ryzyko akceptowalne”. Wymaga ono monitorowania, o którym mowa   
   w § 8.
3. Nieakceptowalne jest ryzyko, którego poziom osiągnął wartość „ryzyko krytyczne”. Wymaga ono podjęcia reakcji na ryzyko, o której mowa w § 6.

**§ 6**

**(Reakcja na ryzyko)**

1. Reakcja na ryzyko podejmowana jest w stosunku do każdego ryzyka o wartości „ryzyko krytyczne”, na podstawie uzyskanych wyników z oprogramowania, o którym mowa   
w § 2 ust. 2 i 3.

2. Przez reakcję na ryzyko należy rozumieć postępowanie z ryzykiem, tj.:

1) przeciwdziałanie lub ograniczanie ryzyka – podejmowanie lub ustanawianie działań   
w celu minimalizacji skutków ryzyka;

2) przeniesienie ryzyka – przekazanie ryzyka podmiotowi zewnętrznemu, np. w drodze ubezpieczenia lub zlecenia usług;

1. tolerowanie ryzyka – występuje w przypadku, gdy koszty przeciwdziałania ryzyku przekraczają jego potencjalne korzyści lub zdolności do skutecznego przeciwdziałania ryzyku są ograniczone;
2. zaniechanie działania – występuje w przypadku, gdy koszty reakcji na ryzyko nie uzasadniają jej wdrożenia (a szczególnie gdy przewyższają koszty wykonania zadania); następuje wtedy odstąpienie od realizacji zadania, które jest jednocześnie zadaniem fakultatywnym dla wydziału i m.j.o. (tj. niewynikającym z przepisów prawa lub innych unormowań).

3. Podejmowane reakcje na ryzyko, o których mowa w ust. 2, powinny być poddane analizie pod względem ich adekwatności i racjonalności.

1. W sytuacji, gdy określone reakcje na ryzyko przekraczają zasoby danego wydziału albo m.j.o. (lub ich wdrożenie będzie obejmować więcej niż jeden wydział bądź jedną m.j.o.), należy dokonać analizy m.in. aspektów finansowych, prawnych i organizacyjnych dotyczących korzyści wynikających z wdrożenia tych działań oraz udokumentować je zgodnie z § 7 ust. 2.

**§ 7**

**(Dokumentowanie w procesie zarządzania ryzykiem)**

1. Dokumentowanie w procesie zarządzania ryzykiem odbywa się za pomocą oprogramowania przeznaczonego do zarządzania ryzykiem w Mieście i jest prowadzone w następujący sposób:

1. sporządza się zestawienie ryzyka do zadań budżetowych procesowych (typu B);
2. sporządza się zestawienie ryzyka do zadań budżetowych projektowych (typu P);
3. sporządza się zestawienie ryzyka do zasobów (typu BI);
4. kierownik m.j.o. w terminie do 30 września każdego roku zatwierdza zestawienie ryzyka typu B oraz typu BI na kolejny rok kalendarzowy;
5. kierownik m.j.o., wobec której bezpośredni nadzór sprawują osoby wymienione w zarządzeniu Prezydenta w sprawie zadań i kompetencji Prezydenta, powierzenia określonych spraw Miasta Zastępcom Prezydenta i Sekretarzowi oraz zakresu zadań Skarbnika, w terminie do 15 października każdego roku zatwierdza zestawienie ryzyk typu B i BI na kolejny rok kalendarzowy;
6. wydział nadzorujący m.j.o. analizuje informacje zawarte w zestawieniu ryzyk,   
   o którym mowa w pkt 4, w celu ich wykorzystania przy wykonywaniu czynności związanych z nadzorem oraz opracowywaniu własnego zestawienia ryzyk typu B   
   na kolejny rok kalendarzowy;
7. dyrektor wydziału, w tym dyrektor wydziału nadzorującego m.j.o,   
   w terminie do 15 października każdego roku zatwierdza zestawienie ryzyk typu B na kolejny rok kalendarzowy;
8. osoba zarządzająca projektem w terminie do 15 listopada każdego roku zatwierdza zestawienie ryzyk typu P na kolejny rok kalendarzowy;
9. przewodniczący Zespołu ds. Bezpieczeństwa Informacji do 15 października każdego roku zatwierdza zestawienie ryzyk typu BI dla Urzędu na kolejny rok kalendarzowy.
10. W przypadku określenia reakcji na ryzyko, o których mowa w § 6 ust. 4, do zestawienia ryzyk należy dołączyć analizę kosztów i korzyści wynikających z ich wdrożenia.
11. Zatwierdzone zestawienia ryzyk, o których mowa w ust. 1 pkt 4, 5, 6, 7 i 8, załącza się do protokołu z przeglądu zarządzania lub dokumentuje się zgodnie z Instrukcją kancelaryjną – w przypadku m.j.o., w których nie funkcjonuje wspólny z Urzędem system zarządzania zgodny z normami PN-EN ISO 9001:2015 oraz PN-EN ISO 14001:2015.
12. Zatwierdzone zestawienie ryzyk, o którym mowa w ust. 1 pkt 9, dokumentowane jest przez Biuro Cyfryzacji i Cyberbezpieczeństwa zgodnie z Instrukcją kancelaryjną.

**§ 8**

**(Monitorowanie w procesie zarządzania ryzykiem)**

1. Dyrektor wydziału, kierownik m.j.o. oraz osoba zarządzająca projektem monitorują wszystkie zidentyfikowane ryzyka oraz aktualizują zestawienie ryzyk, w tym w szczególności dokonują identyfikacji nowych ryzyk, zmiany wartości ryzyk lub przeglądu ustalonych reakcji na ryzyko.
2. Zestawienie ryzyka typu B oraz typu BI monitoruje się w oprogramowaniu przeznaczonym do zarządzania ryzykiem w Mieście za każdym razem, gdy zachodzi przypuszczenie zaistnienia zmian w zestawieniu lub zidentyfikowania nowego ryzyka, ale nie rzadziej niż cztery razy w roku, w terminach:
3. od 1 do 30 kwietnia;
4. od 1 do 31 lipca;
5. odpowiednio od 15 września do 15 października (co jest jednoznaczne z identyfikacją ryzyk na kolejny rok);
6. od 1 do 31 stycznia.

3. Wyniki monitorowania ryzyk typu B w wydziale przedstawiane są podczas kwartalnych przeglądów zarządzania i odnotowywane w protokole z tego przeglądu.

4. Wyniki monitorowania ryzyk typu BI w Urzędzie przedstawiane są podczas spotkań Zespołu ds. Bezpieczeństwa Informacji.

5. Wyniki monitorowania ryzyk typu B i BI w m.j.o. przedstawiane są podczas kwartalnych przeglądów zarządzania i odnotowywane w protokole z tego przeglądu.

6. Ryzyka typu B i typu BI monitorowane są przez m.j.o., w których nie funkcjonuje wspólny z Urzędem system zarządzania, zgodny z normami PN-EN ISO 9001:2015 oraz PN-EN ISO 14001:2015, co najmniej raz do roku w terminie od 1 do 30 kwietnia. Dyrektor wydziału nadzorującego m.j.o. może podjąć decyzję o kwartalnym monitorowaniu ryzyka przez m.j.o. w terminach określonych w ust. 2.

7. Ryzyko do zadań budżetowych projektowych typu P1, P2 i P3 monitoruje się w okresach kwartalnych, natomiast ryzyko do zadań budżetowych projektowych typu P4, P5 i P6 w okresach półrocznych, określonych w wytycznych do sporządzania informacji o realizacji zadań projektowych w danym roku. Wyniki monitorowania przedstawiane są podczas kwartalnych przeglądów zarządzania i odnotowywane w protokole z tego przeglądu.

8. Osoba zarządzająca projektem i kierownik m.j.o., w której nie wprowadzono kwartalnych przeglądów zarządzania, powinni ustanowić inną formę prezentacji i przechowywania wyników monitorowania zidentyfikowanych ryzyk oraz aktualizacji zestawienia ryzyk, a także ustalić z wydziałem nadzorującym m.j.o. sposób umożliwiający dokumentowanie informacji o wynikach monitorowania i aktualizacji.

**§ 9**

**(Zgłaszanie ryzyk przez pracowników)**

* 1. Każdy pracownik Urzędu, m.j.o. i zespołu projektowego ma prawo zgłaszać swojemu przełożonemu podczas wykonywania bieżącej pracy informacje dotyczące ryzyk (zagrożeń lub szans), które mogą wpływać na realizację zadania budżetowego.
  2. Każdy pracownik Urzędu ma prawo zgłaszać swojemu przełożonemu podczas wykonywania bieżącej pracy informacje dotyczące ryzyk, które mogą mieć wpływ na utratę jednego z atrybutów bezpieczeństwa informacji danego zasobu.
  3. Zgłoszenia ryzyk, o których mowa w ust. 2, przekazywane są przez dyrektora wydziału Urzędu do Zespołu ds. Bezpieczeństwa Informacji.
  4. Każdy pracownik m.j.o. ma prawo zgłaszać swojemu przełożonemu podczas wykonywania bieżącej pracy informacje dotyczące ryzyk, które mogą mieć wpływ na utratę jednego z atrybutów bezpieczeństwa informacji danego zasobu.
  5. Ryzyka, o których mowa w ust. 1, podlegają analizie pod kątem oddziaływania   
     i prawdopodobieństwa ich wystąpienia, natomiast po weryfikacji przez dyrektora wydziału, kierownika m.j.o. lub osobę zarządzającą projektem rejestruje się je w sposób określony w § 7 i 8.
  6. Ryzyka, o których mowa w ust. 2 i 4, podlegają analizie pod kątem oddziaływania   
     i prawdopodobieństwa ich wystąpienia, natomiast po weryfikacji przez Zespół   
     ds. Bezpieczeństwa Informacji lub kierownika m.j.o. rejestruje się je w sposób określony w § 7 i 8.

**§ 10**

**(Komunikacja)**

1. Komunikacja polega na zapewnieniu, przekazywaniu lub uzyskaniu informacji   
   w procesie zarządzania ryzykiem; to sposób służący do porozumiewania się podczas całego przebiegu procesu, tj. przede wszystkim informowania o zidentyfikowanym ryzyku, wynikach jego analizy, ustalonych reakcjach na ryzyko.
2. Komunikacja zachodzi w szczególności podczas:

1) narad Prezydenta z zastępcami Prezydenta, Sekretarzem i Skarbnikiem;

2) spotkań Prezydenta z dyrektorami wydziałów oraz kierownikami m.j.o.;

3) spotkań dyrektorów wydziałów lub kierowników m.j.o. z pracownikami;

4) przeglądów zarządzania;

5) konsultacji wewnętrznych.

1. Pełnomocnik Prezydenta ds. systemu zarządzania w uzasadnionych przypadkach może zmienić terminy identyfikacji, analizy, monitorowania i dokumentowania ryzyka oraz termin przekazania raportu, o którym mowa w § 13.
2. Wydziały pełniące funkcję wydziału nadzorującego m.j.o. mają stały dostęp w trybie przeglądu do ryzyk podległych jednostek w narzędziu informatycznym, z wyłączeniem ryzyk typu BI.
3. Biuro Kontroli oraz Audytor Miasta mają pełen dostęp w trybie przeglądu do wszystkich ryzyk zidentyfikowanych przez wydziały oraz m.j.o., z którego mogą korzystać przy prowadzeniu odpowiednio kontroli i audytu wewnętrznego, w którym oceniają funkcjonowanie systemu kontroli zarządczej. Wyniki tej oceny mogą być przekazywane do Pełnomocnika Prezydenta ds. systemu zarządzania w celu ich wykorzystania do poprawy funkcjonowania zarządzania ryzykiem oraz usprawnienia systemu kontroli zarządczej.
4. Dostęp do zestawienia ryzyk typu BI Urzędu, z wyjątkiem ust. 5, powinien być każdorazowo uzgadniany z Biurem Cyfryzacji i Cyberbezpieczeństwa.

**§ 11**

**(Ocena skutków dla ochrony danych – raport DPIA)**

1. Ocena skutków dla ochrony danych stanowi szczegółową weryfikację przestrzegania przepisów w zakresie ochrony danych osobowych oraz zapewnienie ochrony praw i wolności osoby, której dane dotyczą.
2. Dyrektor wydziału lub kierownik m.j.o. jest zobowiązany do niezwłocznego przeprowadzenia oceny skutków dla ochrony danych (tj. sporządzenia raportu DPIA) w przypadku:
3. wystąpienia co najmniej jednej przesłanki, o której mowa w art. 35 ust. 3 rozporządzenia ogólnego o ochronie danych osobowych (RODO);
4. wystąpienia dla danej czynności przetwarzania (typu BI) ryzyka krytycznego naruszenia praw lub wolności osób fizycznych (art. 35 ust. 1 RODO);
5. planowania bądź wykonywania czynności przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (rodzaj operacji podlegających temu wymogowi został określony w komunikacie Prezesa Urzędu Ochrony Danych Osobowych, sporządzanym na podstawie art. 54 ust. 1 pkt 1 ustawy o ochronie danych osobowych w związku z art. 35 ust 4 i 6 RODO).
6. Ocena skutków powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy mające minimalizować ryzyko związane z naruszeniem praw i wolności osób, których dane dotyczą, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie RODO.
7. Ocenę skutków dla ochrony danych należy udokumentować za pomocą oprogramowania przeznaczonego do zarządzania ryzykiem w Mieście, zgodnie z przyjętym wzorem raportu DPIA.
8. Sporządzenie raportu DPIA powinno zostać zakończone akceptacją Inspektora Ochrony Danych oraz Administratora Danych Osobowych. Raport DPIA należy przechowywać zgodnie z Instrukcją kancelaryjną funkcjonującą w jednostce.
9. Uzyskanie wartości krytycznej dla oceny skutków dla ochrony danych wymaga przekazania dokumentu do konsultacji z Prezesem Urzędu Ochrony Danych Osobowych.

**Dział II**

**Proces zarządzania ryzykiem na poziomie strategicznym**

**§ 12**

**(Zarządzanie ryzykiem na poziomie strategicznym)**

1. Ustalenie kontekstu (otoczenia, sytuacji makroekonomicznej Miasta) to w szczególności rozpoznanie i określenie sytuacji społeczno-gospodarczej Poznania, kierunków jego rozwoju oraz stopnia zaawansowania realizacji celu i priorytetów strategicznych na podstawie analizy wskaźników strategicznych, w tym badań jakości życia i dostępnych badań jakości usług publicznych.
2. Identyfikacja i analiza ryzyka typu S następuje poprzez rozpoznanie kontekstu (otoczenia, sytuacji makroekonomicznej) i ustalenie obszarów zagrożeń w Mieście w zakresie celu i priorytetów strategicznych.
3. Ustala się obszary zagrożeń poprzez analizę wskaźników strategicznych wskazanych w Strategii Rozwoju Miasta Poznania 2020+, a także – w benchmarkingu z 4 największymi miastami w Polsce (Warszawa, Kraków, Łódź, Wrocław) – poprzez analizę wskaźników strategicznych, przy przyjęciu roku 2010 oraz roku 2015 jako lat bazowych.
4. Reakcja w obszarze zagrożeń podejmowana jest w stosunku do negatywnej zmiany wskaźnika w ciągu ostatnich 5 lat, która została oznaczona kolorem czerwonym   
   w systemie monitoringu Strategii Rozwoju Miasta Poznania 2020+ (tj. powyżej progu akceptowalności). Powyższa reakcja ustalana jest poprzez wskazanie najważniejszych kierunków interwencji w ramach strategicznych priorytetów rozwoju Miasta na najbliższe lata. Za przygotowanie propozycji działań rozwojowych odpowiada Wydział Rozwoju Miasta i Współpracy Międzynarodowej, który przekazuje je do weryfikacji Komitetowi Sterującemu.
5. Proces zarządzania ryzykiem na poziomie strategicznym (typu S) dokumentuje się w następujący sposób:
   1. sporządza się zestawienie ryzyk celu i priorytetów strategicznych (typu S), korzystając z przeznaczonego oprogramowania do zarządzania ryzykiem w Mieście;

2) dyrektor Wydziału Rozwoju Miasta i Współpracy Międzynarodowej w terminie do   
15 października każdego roku zatwierdza zestawienie ryzyk typu S na kolejny rok kalendarzowy i wraz z informacją o wykonaniu celu oraz priorytetów strategicznych przekazuje je do wiadomości Komitetowi Sterującemu.

1. Monitorowanie obszarów zagrożeń i komunikowanie na poziomie strategicznym określone jest w systemie monitoringu Strategii Rozwoju Miasta Poznania 2020+. Monitoruje się zgodnie z przyjętą metodyką poprzez system wskaźników ustalonych w Strategii Rozwoju Miasta Poznania 2020+ dla celu i priorytetów strategicznych.

**Dział III**

**Zarządzanie ryzykiem na poziomie zarządczym**

**§ 13**

**(Raport z analizy procesu zarządzania ryzykiem i rejestr ryzyka Miasta)**

1. Pełnomocnik Prezydenta ds. systemu zarządzania gromadzi informacje, o których mowa w § 7 i 8, za pomocą przeznaczonego oprogramowania do zarządzania ryzykiem   
   w Mieście i na ich podstawie prowadzi rejestr ryzyka Miasta na kolejny rok.
2. Pełnomocnik Prezydenta ds. systemu zarządzania w terminie do 31 marca każdego roku przedstawia Prezydentowi i decernentom analizę procesu zarządzania ryzykiem, która jest częścią sprawozdania z funkcjonowania systemu zarządzania.
3. Pełnomocnik Prezydenta ds. systemu zarządzania na bieżąco udostępnia rejestr ryzyka Miasta Prezydentowi i właściwym decernentom. Udostępnienie może się odbywać w oprogramowaniu do zarządzania ryzykiem lub w innej formie, w ramach której może zostać dokonana analiza i priorytetyzacja ryzyk.
4. Pełnomocnik Prezydenta ds. systemu zarządzania w ramach procesu okresowej oceny pracowników przygotowuje dla Prezydenta, jego zastępców, Skarbnika i Sekretarza zestawienia ryzyk krytycznych w podziale na podległe im wydziały i m.j.o. Decernenci mogą również w ramach przeprowadzanej oceny pracy dyrektora wydziału lub kierownika m.j.o. priorytetyzować ryzyka.

**§ 14**

**(Schemat przebiegu procesu zarządzania ryzykiem)**

1. Schemat przebiegu procesu zarządzania ryzykiem w Mieście określa proces PDS-08.

2. Właścicielem procesu PDS-08 Zarządzanie ryzykiem, czyli osobą odpowiedzialną za jego działanie, realizację celu i ciągłe doskonalenie, jest Pełnomocnik Prezydenta ds. systemu zarządzania, który co najmniej raz w roku dokonuje przeglądu i analizy przebiegu procesu w związku z zapewnieniem jego aktualności.