ELEMENT 5 WERSJA 1.6

MONITOROWANIE JAKOŚCI USŁUG PUBLICZNYCH

OGÓLNE ZASADY DOTYCZĄCE PROCESU ZARZĄDZANIA RYZYKIEM

Kraków – Poznań Lipiec 2012

Spis treści

Wprowadzenie

Wśród wymagań, jakie uofp stawia zarządzającym w sektorze finansów publicznych największą trudność w dużych JST zwykle sprawia wdrożenie skutecznego procesu zarządzania ryzykiem.
Docelowo należy zmierzać do budowy jednolitego systemu obejmującego nie tylko urząd, ale także miejskie jednostki, jednak proces ten musi być rozłożony w czasie.
Zarządzanie ryzykiem, jeśli nie ma być atrapą wymaga odpowiedniego poziomu zarządzania, a przede wszystkim mierzalnego ustalania celów i rozliczania ich przy pomocy miar oraz odpowiedniego przypisania odpowiedzialności pozwalającego określić „właścicieli" ryzyka.
Model zarządzania JST, który zaproponowaliśmy w ramach projektu spełnia wszystkie w/w warunki i pozwala na zorganizowanie procesu zarządzania ryzykiem w sposób przejrzysty i pożyteczny.
Ponieważ ryzyko to możliwość wystąpienia dowolnego zdarzenia mającego znaczący wpływ na organizację i wykonanie jej zadań, wiec źródeł ryzyk może być bardzo wiele i dotyczą one wszystkich obszarów zarządzania w organizacji.
Dlatego w ramach projektu zostanie przygotowany prosty moduł wspomagający zarządzanie ryzykiem połączony z funkcjonalnością hurtowni danych.
JST wdrażające bardziej złożony proces zarządzania ryzykiem powinny rozważyć zakup odpowiedniego narzędzia informatycznego.
Prócz wspomagania informatycznego ważne jest, aby proces ten był aktualizowany i **systematycznie usprawniany, w miarę rozwijania się kultury i świadomości zarządzania** ryzykiem wśród pracowników

Przygotowując zasady zarządzania ryzykiem zgodnie z naszym modelem należy określić następujące elementy:

1. Przyjęty zakres i systematyka dla zarządzania ryzykiem
2. Diagnoza, analiza potrzeb w zakresie zarządzania ryzykiem,
3. Rodzaje , tryby postępowania w różnych obszarach
4. Cel procesu zarządzania ryzykiem
5. Odpowiedzialność
6. Mierniki i wskaźniki dla monitorowania ryzyk
7. Rejestry ryzyk
8. Mapa ryzyka – zbiorczy rejestr ryzyk
9. Powiązania rejestrów ryzyk z zadaniami, programami i zasobami informacyjnymi
10. Monitorowanie, raportowanie i zarządzanie ryzykiem
11. Przykłady prezentacji rejestrów ryzyk

Szczegółowy opis elementów procesu zarządzania ryzykiem:

1. Przyjęty zakres i systematyka dla zarządzania ryzykiem:

Proces zarządzania ryzykiem docelowo powinien objąć wszystkie istotne obszary tj. nie tylko ryzyka operacyjne związane z zadaniami budżetowymi i dostarczanymi produktami, ale także ryzyka strategiczne (brak realizacji celów długoterminowych), z których część wiąże się z realizacją programów wieloletnich oraz ryzyka związane z bezpieczeństwem informacji.
W każdym z obszarów należy określić tryb postępowania oraz sposób prowadzenia rejestru ryzyk.

2. Diagnoza, analiza potrzeb w zakresie zarządzania ryzykiem

Diagnoza potrzeb w zakresie zarządzania ryzykiem winna w pierwszym rzędzie zidentyfikować obszary, od których należy zacząć. Dla JST używających budżetowania zadaniowego naturalnym pierwszym obszarem są zadania budżetowe i ich produkty. Dla nich to w pierwszym rzędzie należy zidentyfikować potrzeby w zakresie zarządzania ryzykiem.
Następnie jeśli JST posiada programy wieloletnie z zapisanymi klarownie celami strategicznymi wraz z miarami rzeczą naturalną będzie wdrożenie zarządzania ryzykiem w obszarze programów.
Gdy JST posiada zdefiniowaną metodykę zarządzania projektami to ona zapewne także stawia wymagania w zakresie zarządzania ryzykami projektowymi, więc ten obszar także nie może być pominięty.
Diagnozując obszary warto także rozważyć ryzyka strategiczne związane osiąganiem wskaźników i trendami związanymi z wieloletnim planowaniem finansowym jak np. nadwyżka operacyjna, czy dynamika wzrostu wydatków bieżących.
Jeśli JST posiada (a powinna) system zarządzania bezpieczeństwem informacji elementem niezbędnym będzie także zarządzanie ryzykiem w tym obszarze.
W każdym z obszarów, który zostanie objęty procesem należy określić tryb postępowania obejmujący wszystkie etapy ujęte w cyklu Deminga, zapewniając tym samym ciągły proces doskonalenia.
Jest rzeczą zupełnie naturalną, że wdrożenie procesu zarządzania ryzykiem jeśli ma przynieść oczekiwane skutki będzie wymagało kilku lat i powinno być dokonywane stopniowo. Kolejność obejmowania zarządzaniem ryzykiem poszczególnych obszarów zależeć winna od stanu systemu zarządzania w danej JST i preferencji najwyższego kierownictwa.

3. Rodzaje, trypy postępowania w różnych obszarach

W zależności od diagnozy i zakresu , który chcemy objąć zarządzaniem ryzykiem można wyróżnić różne obszary i określić dla nich odpowiednie tryby postępowania:

3.1. Przykład 1. Przyjmując 5 obszarów można dokonać podziału jak w tabelce poniżej i dla każdego z obszarów zaproponować odpowiedni tryb postępowania. Przykład czynności dla poszczególnych trybów przedstawiono poniżej.

Symbol	Obszar zarządzania ryzykiem	Rodzaj ryzyk	Perspektywa czasowa	Właściciel
ZB	Zadania budżetowe	operacyjne	roczna	Koordynator zadania
PS	Programy sektorowe	operacyjne i strategiczne	Kilkuletnia (4-5 lat)	Koordynator programu
INFO	Bezpieczeństwo Informacji	operacyjne	roczna	Właściciel zasobów
PR	Projekty	projektowe	czas życia projektu	Kierownik projektu
STR	Cele długoterminowe	strategiczne	Wieloletnia (powyżej 5 lat)	Najwyższe kierownictwo

Poniżej przedstawiono czynności wykonywane przez właścicieli ryzyk w kolejnych czterech etapach cyklu Deminga (z pominięciem obszaru projektów, który zwykle opisany jest w metodyce zarządzania projektami):

ETAP I – PLANUJ (*działanie dla osiągnięcia celu****)***

ZB - W fazie przygotowania planów działań, każdy z koordynatorów zadań budżetowych dla wszystkich istotnych (lub najważniejszych) (=duża ilość klientów, duży koszt wytworzenia, ważne dla społeczności itp.) produktów (usług) identyfikuje i ocenia ryzyka niezrealizowania celów (zazwyczaj ilość i jakość produktów) i decyduje o stosowaniu mechanizmów kontrolnych oraz ustala (wybiera, definiuje) wskaźniki, które pozwolą na bieżące śledzenie stanu materializowania się wybranych ryzyk. Dla produktów krytycznych koordynatorzy winni uwzględnić także ryzyka towarzyszące wystąpieniu stanów nadzwyczajnych (klęski żywiołowe, zagrożenia terrorystyczne itp.) oraz przygotować plany ciągłości działania.

BI – Właściciele zasobów używanych do przetwarzania informacji identyfikują i oceniają ryzyka związane z zasobami, które są w ich gestii, biorąc pod uwagę zagrożenia i podatności oraz w zakresie ryzyk istotnych (poważnych) poprawiają lub planują zmianę zabezpieczeń (mechanizmów kontrolnych). Dla zasobów krytycznych właściciele winni uwzględnić także ryzyka towarzyszące wystąpieniu stanów nadzwyczajnych (klęski żywiołowe, zagrożenia terrorystyczne itp.) oraz przygotować plany odtworzeniowe.

PS – Formułując bądź aktualizując program wieloletni (strategiczny, sektorowy) koordynator programu powinien zawrzeć w nim informacje o zidentyfikowanych ryzykach niepowodzenia (nieosiągnięcia założonych celów), ich ocenie oraz przewidywanych mechanizmach zabezpieczających (kontrolnych).

STR – Identyfikacja i ocena ryzyk strategicznych dokonywana winna być dokonywana przez najwyższe kierownictwo (ewentualnie przez „risk manager'a", jeśli kierownik jednostki utworzyła taką funkcję/stanowisko). Poza tym niezależną ocenę najważniejszych ryzyk przedstawia także kierownik audytu wewnętrznego. Po zapoznaniu się z oceną/ocenami kierownik jednostki poleca przygotowanie propozycji reakcji na przedstawione w raporcie najważniejsze ryzyka. Przygotowane plany działań wraz z planami finansowania Prezydent Miasta zatwierdza i przekazuje do realizacji.

ETAP II – WYKONAJ *(to co zaplanowałeś**)***

ZB, BI, PS – Koordynując Program operacyjny, zarządzając zespołem w trakcie realizacji Zadania budżetowego, kierując projektem, czy nadzorując i udostępniając zasoby informacyjne koordynator, kierownik lub właściciel wdraża zaplanowane rozwiązania i bieżąco śledzi osiągane wyniki monitorując skuteczność zastosowanych zabezpieczeń (mechanizmów).

STR - Podobne obowiązki ciążą na wyznaczonych realizatorach planów działań zatwierdzonych przez kierownika jednostki w wyniku dyskusji nad analizą ryzyk strategicznych.

ETAP III – SPRAWDŹ (*czy rezultat jest zadowalający i dokonaj oceny**)***

ZB, PS – W odpowiednich odstępach czasu koordynator programu (zwykle raz w roku) i zadania (co najmniej raz na pół roku) dokonuje oceny postępu w realizacji celów i skuteczności systemu kontroli, prócz oceny własnej korzysta z wyników różnego rodzaju niezależnych od niego działań zapewniających (audyt wewnętrzny oraz ewentualnie audity ISO 9001, ISO14001 i 27001, kontrole, inne)

BI – Właściciel aktywa (zasobu) bieżąco monitoruje, sprawdza i analizuje stan zabezpieczeń najważniejszych zasobów, weryfikuje skuteczność systemu kontroli, prócz oceny własnej korzysta z wyników różnego rodzaju niezależnych od niego działań zapewniających (audyt wewnętrzny, audity ISO 9001, ISO 14001 i 27001, kontrole, inne)

STR – Przeglądu stanu ryzyk strategicznych dokonuje kierownik jednostki raz w roku lub w razie potrzeby częściej i wtedy plany działań są korygowane.

ETAP IV – POPRAW (*zmodyfikuj rozwiązanie na podstawie dokonanej oceny**)***

ZB, BI, PS, STR – W zależności od wyników monitorowania, przeglądów oraz audytów koordynatorzy, właściciele zasobów oraz realizatorzy planów dla zmniejszenia zagrożeń strategicznych wprowadzają modyfikacje i udoskonalenia poprawiające skuteczność systemu kontroli, a w razie potrzeby przedstawiają kierownictwu wnioski o sfinansowanie zmian, jeśli konieczna poprawa systemu wymaga nakładów finansowych lub innych zasobów.

3.2 Przykład 2. Innym sposobem jest: zbudowanie struktury procesu zarządzania ryzykiem (ZR) na 3 podstawowych poziomach:

a. poziom strategiczny tj. dla wizji i celów strategicznych - ryzyka strategiczne będą badane w powiązaniu z rejestrem ryzyka operacyjnego Miasta,
b. poziom operacyjny, tj. zarządzanie ryzykiem w Urzędzie i m.j.o.
   - identyfikowanie ryzyk do procesów / zadań / projektów (w tym m.in. BI)
c. poziom zarządczy, tj. zatwierdzanie / akceptacja ryzyk operacyjnych przez Prezydenta Miasta, a następnie przekazanie rejestru ryzyk Miasta do Audytu Wewnętrznego w celu nadania priorytetu do planu audytu.

Efektem końcowym powinno być zatem powstanie 3 podstawowych informacji zarządczych w procesie zarządzania ryzykiem:
- rejestr ryzyka operacyjnego Miasta,
- rejestr ryzyka strategicznego,
- wskazanie ryzyk priorytetowych - w celu wyodrębnienia obszarów zagrożeń istotnych dla Audytu Wewnętrznego.

Po etapie wdrożenia powyższego sposobu i ukształtowaniu kultury zarządzania ryzykiem, można rozważyć dalszą modyfikację / udoskonalenie procesu zarządzania ryzykiem poprzez m.in. wyodrębnienie z poziomu operacyjnego - jako osobnego obszaru - poziomu BI.

4. Cel procesu zarządzania ryzykiem

W opisie procesu zarządzania ryzykiem warto zdefiniować jego cel. W proponowanym modelu przyjęto, że celem procesu jest zapewnienie, że dla wszystkich ważnych działań bieżących i zamierzeń długoterminowych podejmowanych w JST zidentyfikowano najważniejsze ryzyka i wdrożono odpowiednie działania (dla redukcji ryzyk lub inne) tak, aby prawdopodobieństwo uzyskania zaplanowanych rezultatów było jak największe.

Proces ten winien także zapewnić najwyższemu kierownictwu:
- istotne informacje o aktualnym stanie oceny ryzyk przez ich właścicieli oraz
- bieżący dostęp do danych, które wskazują na poziom zagrożeń.

5. Odpowiedzialność

W ramach zadań budżetowych oraz programów wieloletnich odpowiedzialność za identyfikowanie, ocenę i reakcję na ryzyka warto przypisać bezpośrednio koordynatorom zadania lub programu. Gdy zadanie jest projektowe ryzyka należą do kierownika projektu.
Ryzyka zadań, programów i projektów wiążą się zazwyczaj z nieosiągnięciem celów lub nadmiernymi odchyleniami od planu.
W przypadku ryzyk związanych z bezpieczeństwem informacji odpowiedzialność za ocenę ryzyka i decyzję w sprawie rodzaju zabezpieczeń powinien ponosić właściciel, a odpowiedzialność za stosowanie ustalonych przez właściciela zabezpieczeń spoczywa na użytkowniku bezpośrednim, gdy nie jest nim właściciel.
Można w organizacji powołać zespół ds. BI, którego zadaniem będzie wsparcie w ocenie ryzyk i ustalaniu rodzajów zabezpieczeń.
Odpowiedzialność za ryzyka strategiczne spoczywa bezpośrednio na najwyższym kierownictwie i ono też ustalić powinno zakres informacji niezbędny dla zarządzania tymi ryzykami. Osoby wyznaczone do ich dostarczania winny odpowiadać za wiarygodność i terminowość przekazywania danych oraz analiz.
Monitorowanie ryzyk w postaci bieżącej obserwacji wskaźników, które dostarczają na ten temat informacji to w pierwszym rzędzie odpowiedzialność właścicieli. Jeśli istnieje w organizacji komórka monitorowania to ona także może zostać obciążona odpowiedzialnością za informowanie najwyższego kierownictwa o pojawiających się zagrożeniach.
Badania materializowania się ryzyk to z kolei odpowiedzialność audytorów. Badania te winni niezależnie od kierownictwa planować i realizować audytorzy wewnętrzni. Dobrą praktyką w zakresie badań ryzyk jest podporządkowanie wynikom analizy ryzyka audytorów wewnętrznych także planów auditów w ramach zgodności z normami dotyczącymi systemu zarządzania np. jakością ISO 9001, środowiskiem ISO 14001, czy bezpieczeństwem informacji ISO 27001.

6. Mierniki i wskaźniki dla monitorowania ryzyk

W ramach planowania zadań budżetowych definiując mierniki i wskaźniki warto wziąć pod uwagę także :
- jakie ryzyka zagrażają osiągnięciu zaplanowanych rezultatów

- czy istnieją dane, których gromadzenie mogłoby dostarczyć ważnej z punktu w/w ryzyk informacji

- czy gromadzenie tej informacji jest z ekonomicznego punktu widzenia uzasadnione

Po rozważeniu powyższego w razie potrzeby warto uzupełnić rejestr wskaźników i ew. mierników o te dodatkowe miary.

Podobne rozważanie warto przeprowadzić dla innych trybów postępowania, szczególnie, gdy dane istotne z punktu widzenia oceny zagrożeń są łatwo dostępne w JST lub jej otoczeniu.

7. Rejestry ryzyk

Dla każdego z trybów postępowania należy określić format rejestru ryzyk oraz zdefiniować zasady jego prowadzenia.
Przykładowe formy rejestrów ryzyka przedstawiono w tabelkach poniżej
Ważnym elementem prowadzenia rejestru ryzyk dla zadań jest możliwość agregowania i podsumowywania informacji dla najwyższego kierownictwa.
Można w tym celu sporządzić słowniki kategorii ryzyk, ryzyk oraz produktów i wszystkie definiowane przez właścicieli ryzyka przyporządkowywać do określonych wcześniej grup. Utrzymanie nazw właścicieli ułatwia komunikację z nimi, a przyporządkowanie do kategorii daje możliwość agregowania zarówno ocen jak i wyników badań w ich obrębie.
Rejestry ryzyk winny zawierać następujące informacje:

- ryzyka związane z produktami zidentyfikowane przez właścicieli wraz z aktualną i historyczna oceną

- niezależną ocenę audytu wewnętrznego dla każdego z ryzyka ocenionego przez właściciela powyżej poziomu umiarkowanego oraz dla ryzyk, które audyt ocenia powyżej umiarkowanego

- wyniki badań ryzyka (aktualne i historyczne) otrzymane przez audyt wewnętrzny lub audit ISO 9001 lub 27001

Innym sposobem zapisu / udokumentowania wyników przeprowadzonej analizy ryzyka może być tworzenie trzech typów rejestrów:

- rejestr ryzyk wydziału (lub jednostki), którego aktualizacja dokonywana jest co najmniej raz na kwartał podczas przeglądów jakości, lub o ile system informatyczny na to pozwala na bieżąco

- rejestr ryzyk strategicznych (aktualizacja wg opracowania dotyczącego monitoringu Strategii)

- rejestr ryzyk Miasta - sporządzany na podstawie rejestrów ryzyk poszczególnych wydziałów i jednostek miejskich oraz rejestru ryzyk strategicznych, co najmniej raz w roku lub o ile system informatyczny na to pozwala na bieżąco

Rejestry powyższe zawierają informacje dotyczące zidentyfikowanych ryzyk wraz z ich parametrami określającymi:
- proces / zadanie / projekt, w którym zidentyfikowano ryzyko/a,
- właściciela ryzyka,
- ocenę ryzyka,
- informacje o reakcji na ryzyko – wskazanie działań zaradczych i terminu ich wdrożenia.

- rejestr obszarów ryzyka sporządzany przez audyt wewnętrzny (na podstawie rejestru ryzyk Miasta audyt wewnętrzny dokonuje identyfikacji i oceny obszarów ryzyk, a następnie tworzy plan audytów)

Rejestry winny być prowadzone w formie pozwalającej na ich bieżącą aktualizację, dokonywanie syntezy oraz prezentację podsumowań dla kadry kierowniczej.

8. Mapa ryzyka – zbiorczy rejestr ryzyk

Na podstawie rejestrów ryzyk prowadzonych w różnych obszarach (zadania, programy, projekty, bezpieczeństwo informacji oraz ryzyk strategicznych) warto dokonać syntezy w postaci jednego zbioru, który sprowadza ryzyka pochodzące z różnych obszarów do „wspólnego mianownika" (uszeregowując je wg takiej samej skali - np. 4 stopniowej.
(niskie, umiarkowane, poważne, krytyczne)
(Tu skala)
Operacja „sprowadzania do jednej skali" może zostać dokonana w zasadzie tylko przy udziale najwyższego kierownictwa, posiadającego swoją ocenę łączną pozwalającą porównywać oceny z różnych obszarów.
Jeśli w Kierownik utworzył stanowisko „risk manager'a" to osoba zajmująca je powinna mieć także orientację pozwalającą na dokonanie takiej wstępnej oceny i zaprezentowanie jej szefowi.
Niezależną ocenę dotycząca uszeregowania ryzyk z różnych obszarów i oceny w jednej skali powinien także przeprowadzić audyt wewnętrzny.
Ryzyka poważne i krytyczne pochodzące ze wszystkich obszarów objętych zarządzaniem ryzykiem wraz z ocenami „risk manager'a" oraz audytu wewnętrznego mogą zostać zebrane w postaci wspólnego rejestru i wraz ze wskaźnikami obrazującymi ich stan powinny być bacznie obserwowane w pierwszym rzędzie przez ich właścicieli oraz przez najwyższe kierownictwo. W przypadku istotnych zmian właściciele winni informować o nich kierownictwo niezwłocznie.
Prowadzenie, aktualizację i dokonywanie podsumowań w zakresie rejestrów ryzyk i mapy zbiorczej znacznie ułatwi oprogramowanie wspomagające zarządzanie ryzykiem powiązane z hurtownią danych.

9. Powiązania rejestrów ryzyk z zadaniami, programami i zasobami informacyjnymi

Ponieważ oceny i badania dotyczące ryzyk są istotną informacją zarządczą i muszą być związane z innymi elementami i informacjami w systemie zarządzania, więc warto aby:
a. Ryzyka dotyczące zadań budżetowych były bezpośrednio powiązane z systemem planowania zadań (wtedy właściciel dokonuje identyfikacji i oceny poziomu ryzyka), a

dalej z monitorowaniem postępu w ich realizacji, gdy obserwacja postępu i wartości wskaźników pozwala mu śledzić poziom materializowania się ryzyka i reagować.

b. Ryzyka dotyczące programów wieloletnich były z nimi analizowane, bo wiążą się głownie z niepowodzeniem w osiągnięciu planowanych zmian wartości wskaźników strategicznych.

c. Ryzyka z obszaru bezpieczeństwa informacji najlepiej w JST powiązać bezpośrednio z ewidencją zasobów informacyjnych, odpowiedzialność za zasoby bowiem połączona jest z odpowiedzialnością za ocenę ryzyka i zabezpieczenia.

Ponieważ:
- informacje o planowaniu oraz realizacji programów i zadań znajdują się w hurtowni danych,
- ewidencja zasobów prowadzona jest zazwyczaj w formie elektronicznej, więc łatwo można ją do hurtowni dostarczyć,

przewidziano, że moduł zarządzania ryzykiem podobnie jak planowanie zadań zostanie przygotowany wspólnie z budową hurtowni danych, tak, aby wykorzystać jej funkcjonalność do prezentacji i analiz w tym obszarze.

10. Monitorowanie, raportowanie i zarządzanie ryzykiem

Monitorowanie ryzyk i raportowanie zachodzących zmian jest kluczowym warunkiem „szybkiego reagowania" a więc dostarczenia przez system zarządzania ryzykiem wartości dodanej dla organizacji.
Zorganizowanie procesu jak przedstawiono wyżej zapewnia, że każde z ryzyk ma właściciela i jego odpowiedzialnością jest w pierwszym rzędzie monitorowanie i reagowanie na zmiany. Jeśli ryzyko rośnie i właściciel nie ma w dyspozycji środków, które pozwolą je ograniczyć do zaakceptowanego wcześniej przez decydentów poziomu powinien informację tę eskalować na wyższy poziom zarządzania, przedstawiając raport z propozycjami działań.
W razie potrzeby informacja winna zostać przedstawiona najwyższemu kierownictwu, które powinno podjąć i udokumentować decyzję o zaakceptowaniu ryzyka lub polecić wdrożenie dodatkowych działań dla jego ograniczenia.
W zakresie ryzyk strategicznych kierownictwo bezpośrednio winno wyznaczyć osoby w organizacji, które ryzyka te będą obserwować i w razie potrzeby będą przedstawiać w tej sprawie informacje i ewentualne wnioski.

11. Przykłady prezentacji rejestrów ryzyk

A. Przykład zawartości rejestru ryzyk w obszarze bezpieczeństwa informacji przy wykonywaniu analizy ryzyka ukierunkowanej na zasoby informacyjne JST.

a. Kategoria zasobu
b. Opis, lokalizacja lub nr ewidencyjny pojedynczego aktywa lub ich grupy
c. Właściciel zasobu
d. Użytkownik zasobu
e. Opis zagrożenia – ryzyko

f. Opis podatności
g. Wartość zasobu
h. Opis zabezpieczeń
i. Ocena zagrożenia
j. Ocena podatności
k. Ocena skutku
l. Ocena ryzyka wg algorytmu
m. Ocena ryzyka w skali 1-7
n. Wynik weryfikacji istnienia zabezpieczeń
o. Wynik oceny skuteczności zabezpieczeń
p. Ocena ryzyka po badaniu
q. Reakcja właściciela

B. Przykład zawartości rejestru ryzyk w JST – mapa ryzyka

a. Obszar ryzyka
b. Komórka organizacyjna urzędu lub jednostka
c. Numer i nazwa zadania budżetowego
d. Nazwa produktu wg właściciela
e. Symbol procesu, w ramach którego produkt jest wytwarzany
f. Typ produktu wg słownika
g. Nazwa ryzyka wg właściciela
h. Kategoria ryzyka wg słownika
i. Nazwa typu ryzyka wg słownika
j. Ocena ryzyka wg właściciela
k. Ocena ryzyka wg audytorów
l. Rodzaj wykonywanych badań (audyt wewnętrzny, audit ISO, kontrole,..)
m. Wynik badań w skali 1-3

C. Przykład zawartości raportu prezentującego wybrane/najważniejsze wskaźniki strategiczne:

a. Dziedzina
b. Poddziedzina (obszar)
c. Nazwa wskaźnika
d. Wartość oczekiwana lub oczekiwany kierunek zmian
e. Wartości historyczne (np. dla ostatnich 5 lat)
f. Wartość aktualna
g. Komentarz kierownika komórki odpowiedzialnej
h. Propozycja reakcji – kierownik pionu

D. Przykład zawartości raportu prezentującego wybrane/najważniejsze wskaźniki operacyjne:

a. Dziedzina
b. Poddziedzina (obszar)
c. Komórka organizacyjna urzędu lub jednostka
d. Program sektorowy (jeśli zadanie jest objęte jakimś programem)
e. Zadanie budżetowe
f. Nazwa wskaźnika osiągnięcia celu operacyjnego

g. Wartość oczekiwana lub oczekiwany kierunek zmian
h. Wartości historyczne (np. dla ostatnich 5 lat)
i. Wartość aktualna
j. Komentarz kierownika komórki odpowiedzialnej
k. Propozycja reakcji – kierownik pionu.