Spotkanie audytorów wewnętrznych JSFP

Ministerstwo Finansów

Warszawa 28 luty 2013r

Kontrola zarządcza - budżet zadaniowy - bezpieczeństwo informacji

(powiązania i zagadnienia praktyczne w zarządzaniu jednostką)

Krzysztof Radecki , CGAP®

Kontrola zarządcza - budżet zadaniowy - bezpieczeństwo informacji

(powiązania i zagadnienia praktyczne w zarządzaniu jednostką)

Część I

- Kontrola zarządcza w jednostce jako narzędzie stymulacji realizacji planów działalności i budżetu zadaniowego
- Zasady funkcjonowania spójnego systemu kontroli zarządczej - ze szczególnym uwzględnieniem roli zarządzania ryzykiem w jednostce

Część II

- Praktyczna ocena ryzyka i sposób zarządzania ryzykiem z wykorzystaniem prostych narzędzi informatycznych - w powiązaniu z realizacją planów działalności jednostki
- Rola i miejsce oceny ryzyka bezpieczeństwa informacji w systemie kontroli zarządczej

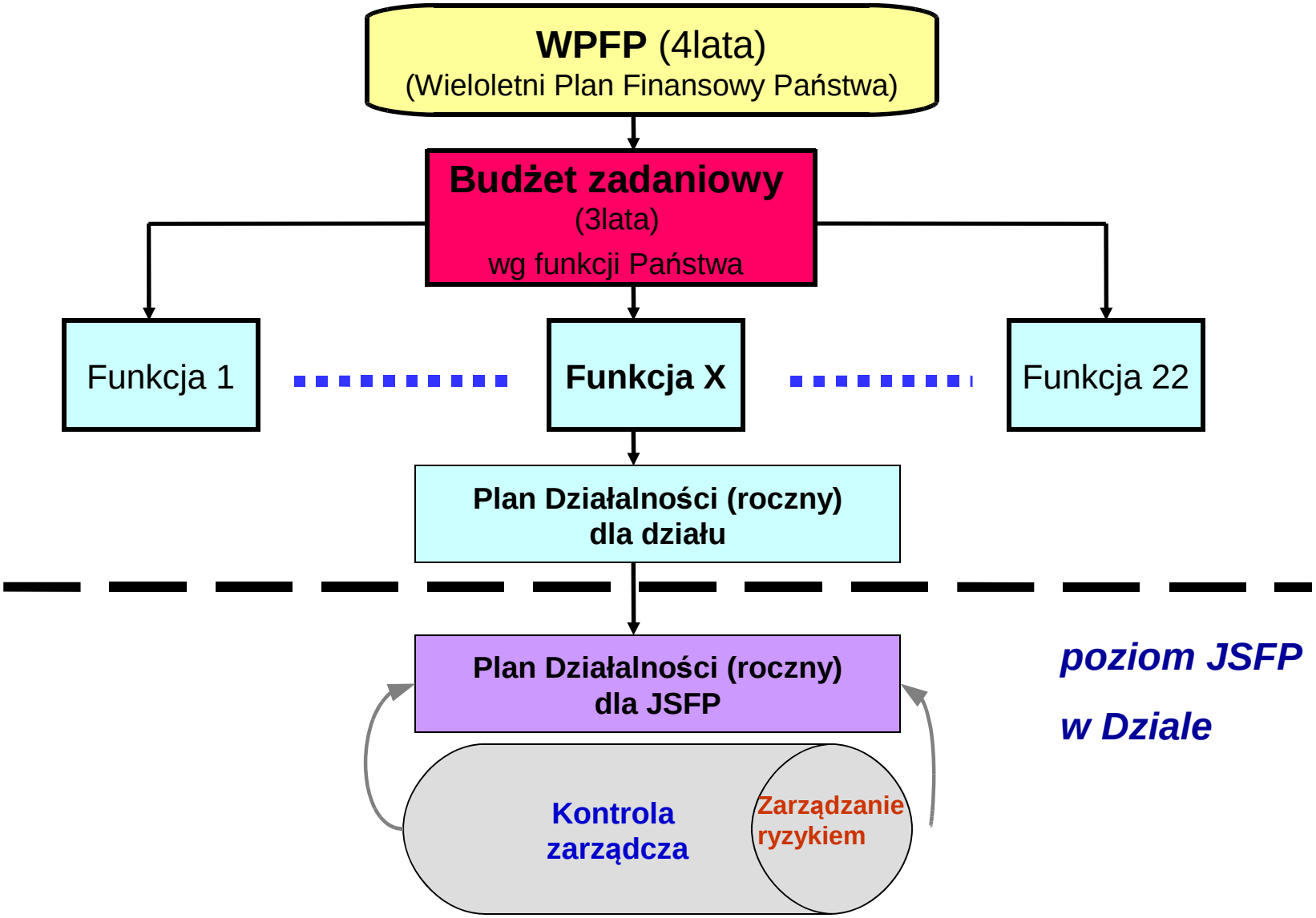
opracowanie: K.Radecki, CGAP®

Część I

kontrola zarządcza w jednostce jako narzędzie stymulacji realizacji planów działalności i budżetu zadaniowego

Miejsce kontroli zarządczej i zarządzania ryzykiem w układzie zadaniowym

Budżetu Państwa



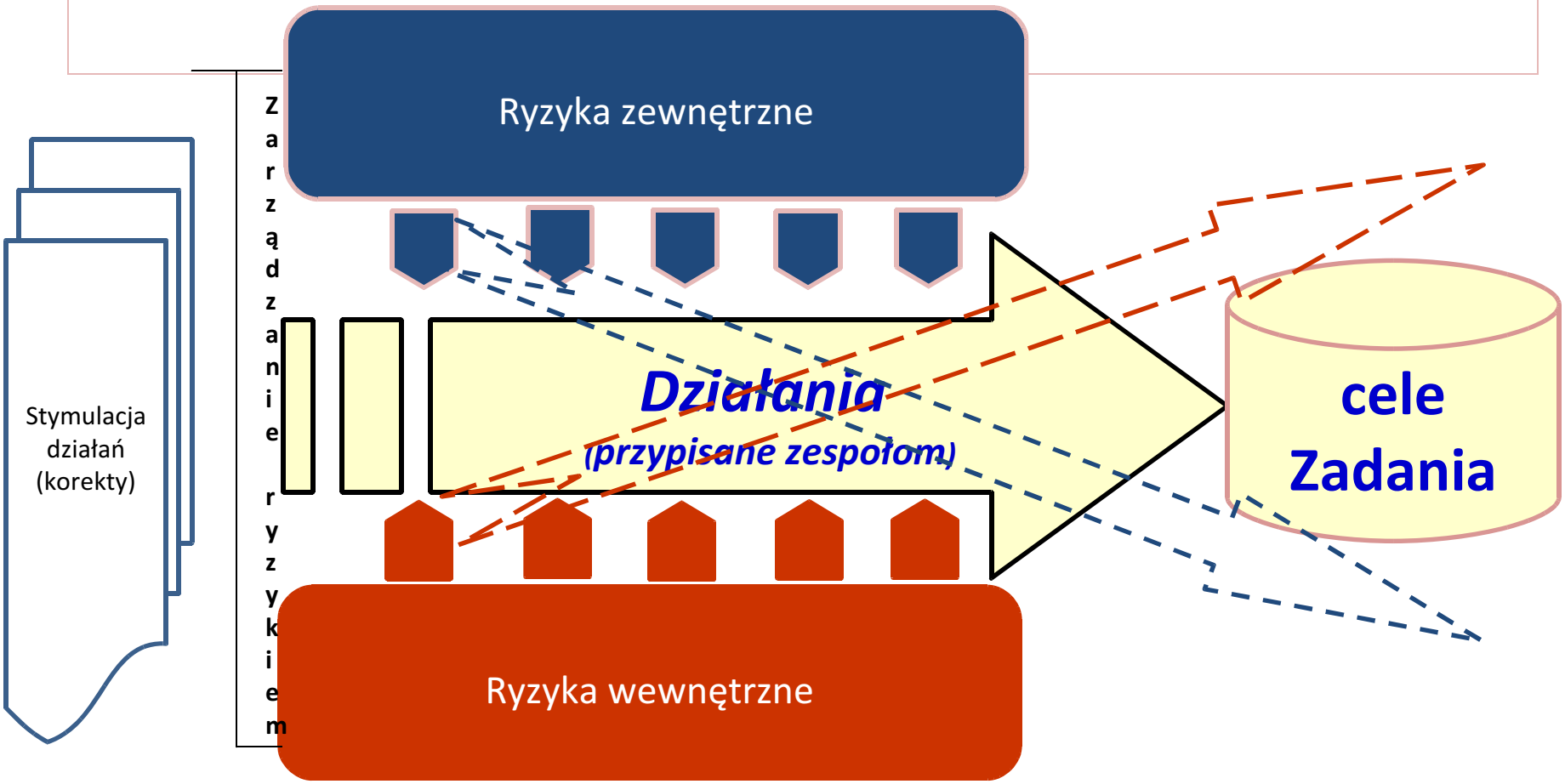
Opracowanie : K.Radecki© , CGAP®

Zarządzanie zadaniowe

Plan działalności

Opracowanie: Krzysztof Radecki , CGAP®

Istota formuły „Zarządzania zadaniowego”



Opracowanie: Krzysztof Radecki©, CGAP®

Sprawozdanie z wykonania planu działalności

Kontrola zarządzania

wg Maciariello (1994)

- **Narzędzie oceny i stymulowania realizacji zadań ,**
- **Oddziaływanie na zachowania zasobów organizacyjnych ,**
- **koordynacja, alokacja zasobów,**
- **motywacja i pomiar wyników.**

kontrola zarządcza *(**Art. 68.** 1. uofp)*

...Ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy

opracowanie: K.Radecki, CGAP®

Twórca i pionier w dziedzinie kontroli zarządzania

(*„kontroli zarządczej”*)

Prof.Anthony Robert N., członek Harvard Business School (HBS) *(zm. 1 XII 2006r)*

- **„Bob zrobił więcej niż ktokolwiek inny w zakresie wprowadzenia struktury pojęciowej kontroli zarządzania**.”
- W jego licznych publikacjach, często zadawał szczególnie ważne pytania : "***Kontrola zarządzania w przemyśle organizacji badawczych„ - na przykład jak zbadać problem pomiaru produkcji intelektualnej ?- zadanie znacznie trudniejsze niż pomiary bardziej konkretnych działań***.
- **W 1965 roku książka "Systemy planowania i kontroli*", stała się biblią na tym polu " Dla kolejnych pokoleń studentów HBS*** .
- Robert N.Anthony określał kontrolę zarządzania jako „...*proces , w którym menedżerowie mają wpływ na innych członków organizacji we wdrażaniu strategii organizacji*...”

Tłumaczenie: K.Redecki, CGAP®

Klasyczne podejście do kontroli zarządzania

Według Maciariello (1994)

kontrola zarządzania dotyczy:

- **koordynacji, alokacji zasobów,**
- **motywacji i pomiaru wyników.**
- **Praktyki zarządzania i kontroli projektu systemów kontroli zarządzania, wywodzącej się z wielu dyscyplin naukowych.**

Kontrola zarządzania jest to zarządzanie, które wymaga dużej ilości pomiarów i dlatego wiąże się to z dużym wkładem rachunkowości - zwłaszcza rachunkowości zarządczej.

kontrola zarządzania (management control)

(Definicja wg słownika biznesu – tł.wł.)

Wszystko, co menedżerowie realizują w sposób bezpośredni , podejmując decyzje dla osiągnięcia określonych celów zgodnie z ustalonym harmonogramem.

- "Kontrola zarządzania" - jej obecny charakter określił Robert N. Anthony (Otley, 1994)

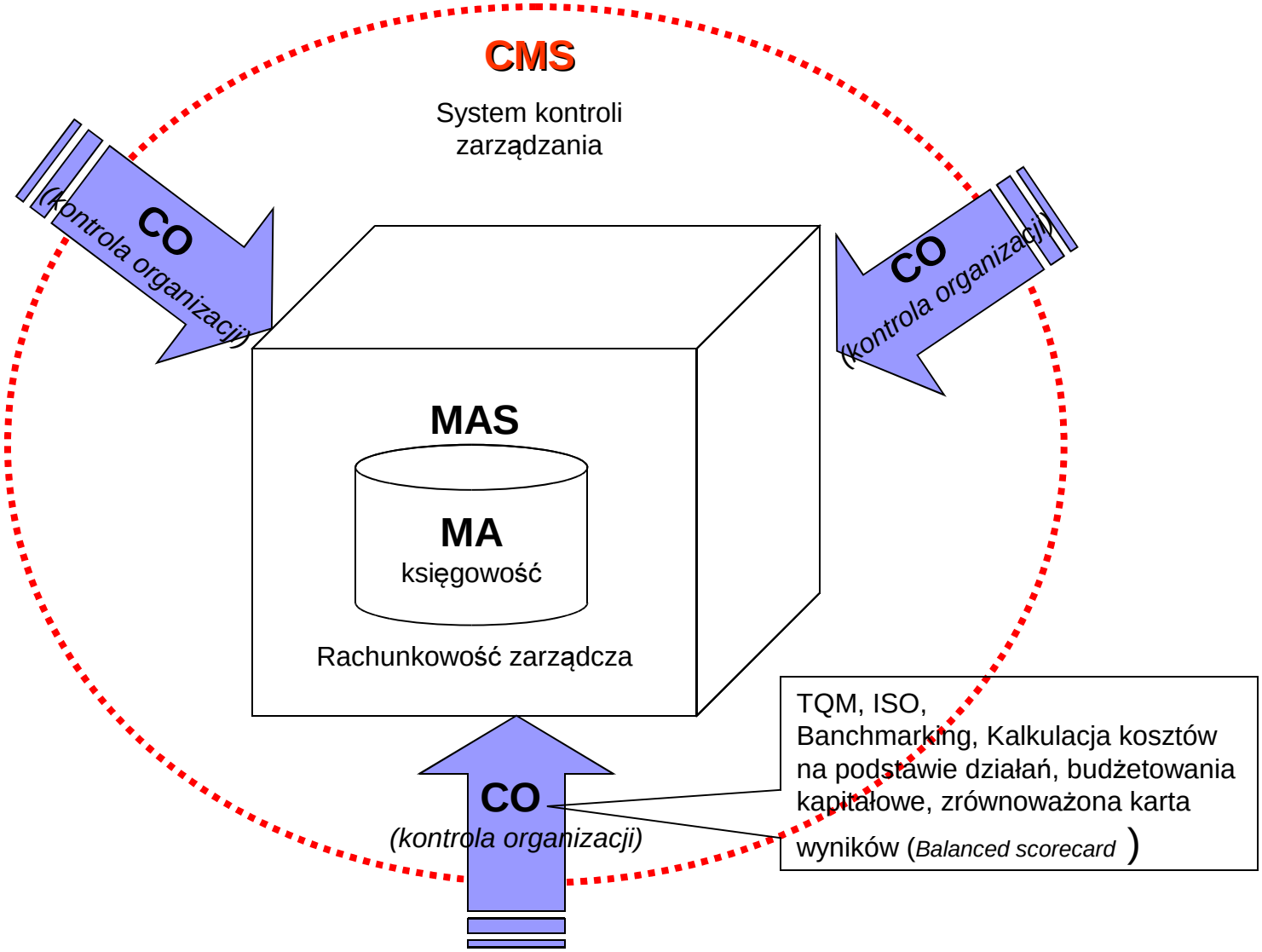
Systemy kontroli zarządzania - CMS (*)

- **Systemy kontroli zarządzania** (CMS) *to system, który zbiera i wykorzystuje informacje do oceny skuteczności różnych środków organizacyjnych jak ludzkie, fizyczne, finansowe, a także organizacyjne jako całość* ***z uwzględnieniem strategii organizacyjnych***.
- Wreszcie, **CMS** **wpływa na zachowanie zasobów organizacyjnych** do realizacji strategii organizacji.
- **CMS** może być formalny lub nieformalny.

(*) Anthony R. i Govindarajan, V.2007. Control Management Systems, Chicago, Mc-Graw Hill IRWIN.

Opracowanie i tł. :K. Radecki, CGAP®

Schematyczne ujęcie problematyki **Systemu Kontroli Zarządzania**



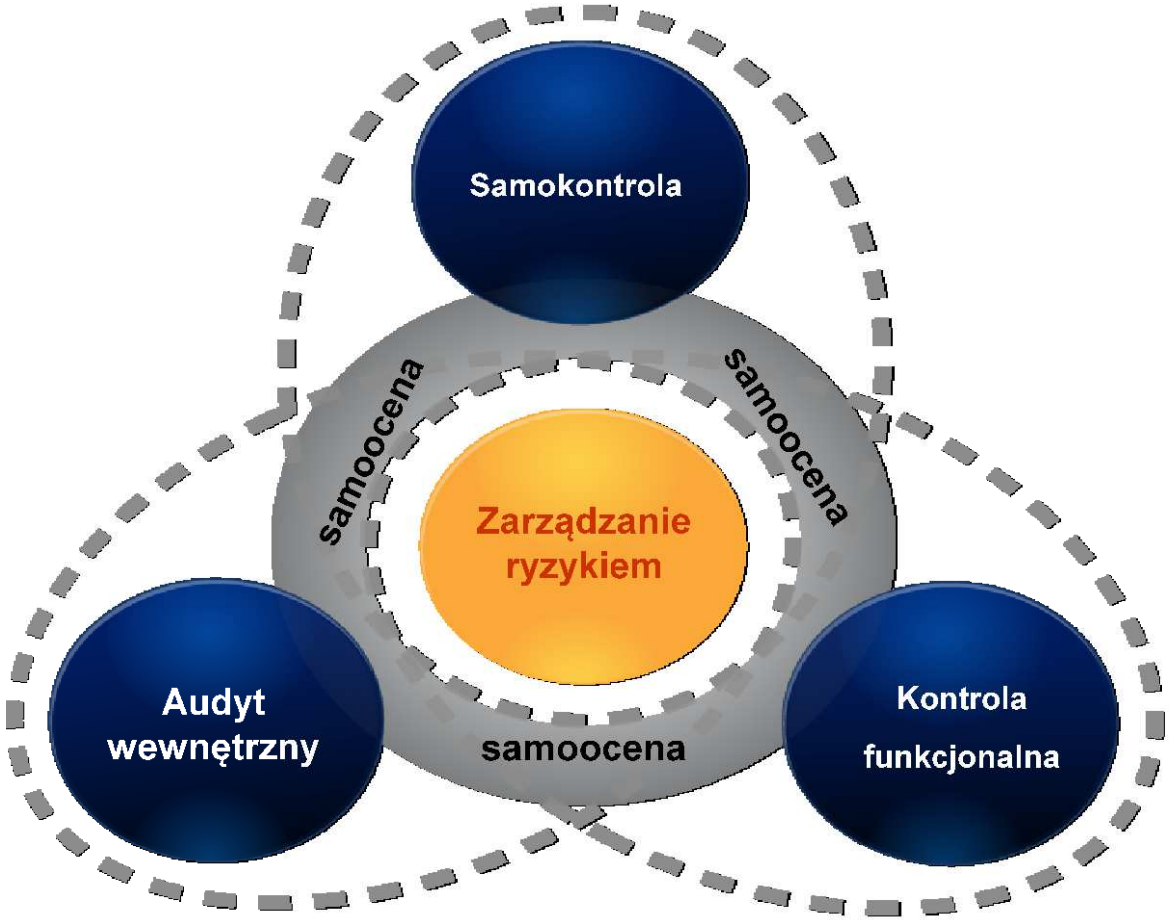
Opr.wł..K.Radecki - np. Chenhall, R., 2003. projekt systemu kontroli zarządzania w jej kontekście organizacyjnym

Część I

zasady funkcjonowania spójnego systemu kontroli zarządczej - ze szczególnym uwzględnieniem roli zarządzania ryzykiem w jednostce

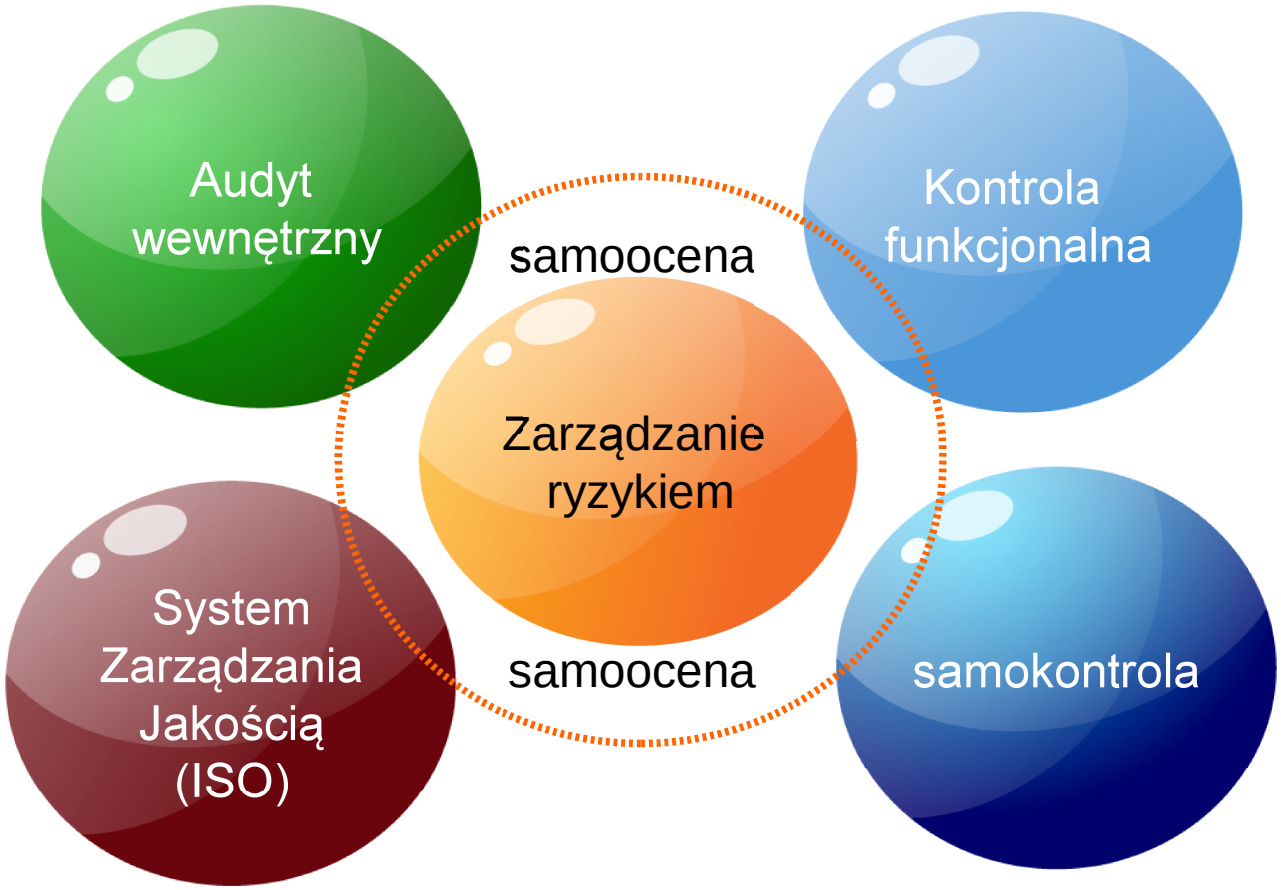
opracowanie: K.Radecki, CGAP®

Przykład 1 - systemu kontroli zarządczej (**Kontroli Zarządzania**)



K.Radecki© , CGAP®

Przykład 2 - systemu kontroli zarządczej (**Kontroli Zarządzania**)



Zakres zadań i obowiązków grupy ds. zarządzania ryzykiem

Skuteczna grupa ds. zarządzania ryzykiem funkcjonująca w organizacji może stanowić istotny (choć nie niezbędny) element procesu komunikacji zarządzania ryzykiem. Grupa taka posiada zazwyczaj jasno określony cel oraz zakres zadań i obowiązków, który obejmuje przegląd i uzgodnienie zmian w profilu ryzyka organizacji w oparciu o informacje własne i stron trzecich.

Grupa ds. zarządzania ryzykiem posiada odrębny zakres zadań i obowiązków i odpowiada za:

- przygotowanie zakresu zadań i obowiązków związanych z jej działalnością, we współpracy z kierownikiem jednostki/kierownictwem najwyższego szczebla ;
- uproszczenie i przegląd inicjatyw z zakresu zarządzania ryzykiem na szczeblu operacyjnym i strategicznym;
- sprawozdania dot. inicjatyw i działań z zakresu zarządzania ryzykiem oraz ich wyników;
- informowanie o zagadnieniach z zakresu zarządzania ryzykiem; oraz
- coroczny przegląd zakresu polityki zarządzania ryzykiem, by zapewnić jego stosowność do potrzeb organizacji.

W skład grupy ds. zarządzania ryzykiem wchodzi przedstawiciel(e) kierownika jednostki/kierownictwa najwyższego szczebla .

Źródło: podręcznik zarządzania ryzykiem w polskiej administracji publicznej (MF 2007)

Szacowanie ryzyka

Zazwyczaj liczbowe oceny punktowe oddziaływania i prawdopodobieństwa wystąpienia ryzyka mnoży się, by uzyskać łączną punktową ocenę ryzyka, np. jeśli ocena punktowa oddziaływania i prawdopodobieństwa wynosi 5 punktów, ocena ryzyka wynosi 25 tj. 5 X 5.

Uwaga:

Identyfikacja i analiza ryzyka to proces ciągły, a nie jednorazowe ćwiczenie. Za pierwszym razem, kompleksowa analiza z pewnością umożliwi wykrycie kilku rodzajów ryzyka, lecz w ciągu kilku tygodni lub miesięcy pojawią się nowe rodzaje ryzyka, a istniejące ryzyka ulegną zmianie.

Źródło: podręcznik zarządzania ryzykiem w polskiej administracji publicznej (MF 2007)

Skala oceny prawdopodobieństwa

Wartość	>0 do <= 10%	>10% <=25%	>25% <=45%	>45% <=70%	>70% <=100%
Opis	rzadkie	mało prawdopodobne	średnio prawdopodobne	prawdopodobne	prawie pewne lub pewne
Punktacja	**1**	**2**	**3**	**4**	**5**

Źródło: podręcznik zarządzania ryzykiem w polskiej administracji publicznej (MF 2007)

Tabela punktowa oddziaływania ryzyka (SKUTKU)

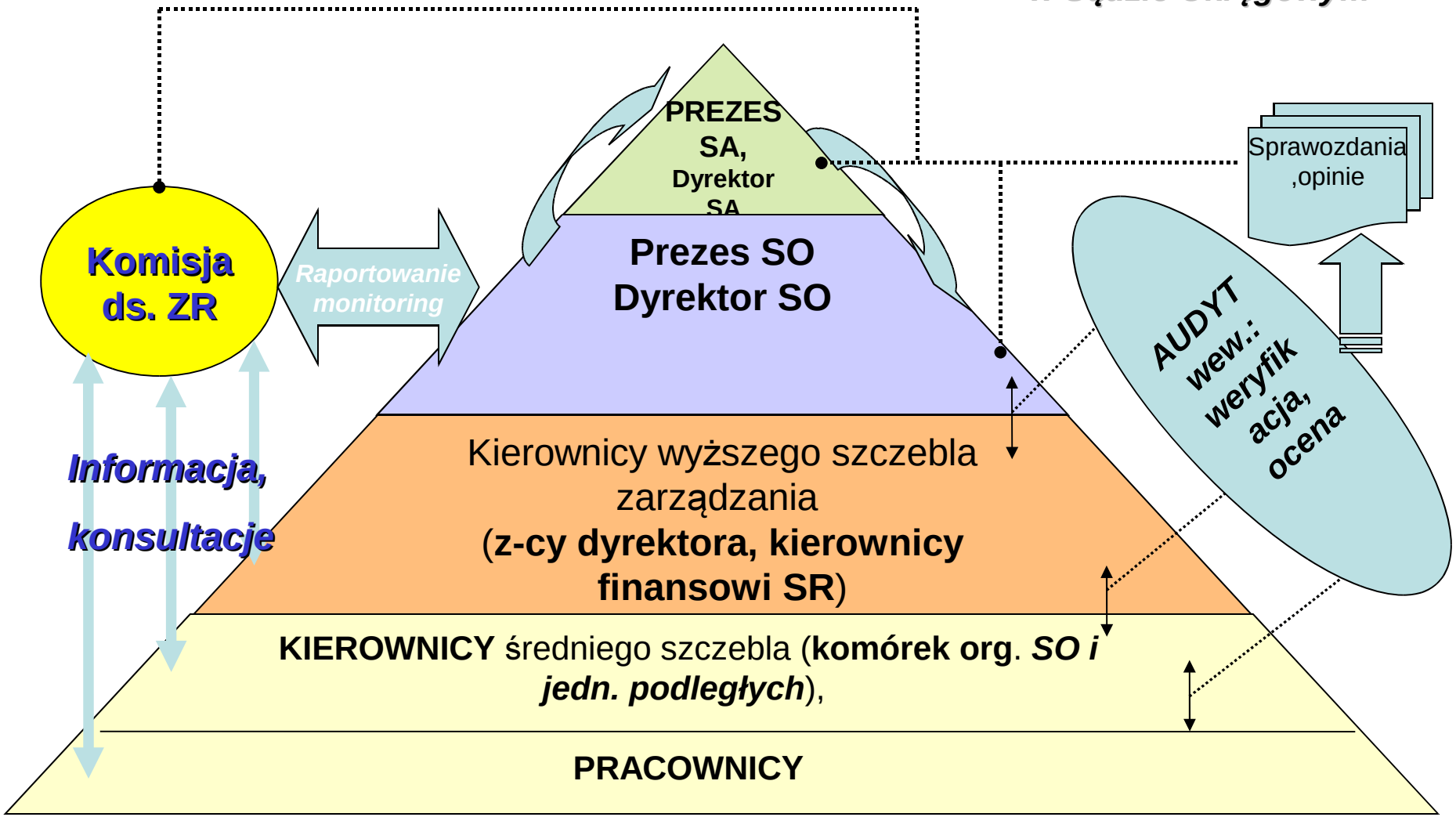
Punktacja	Opis	Kryteria			
		Finansowe	Organizacyjne	Ochrona zdrowia i bezpieczeństwa osób	Reputacja
5	Katastrofalne	Strata finansowa >500.000 PLN	Brak realizacji kluczowych celów	Utrata życia	Doniesienia prasowe w całym kraju
4	Poważne	Strata finansowa 100.000 PLN< 500.000 PLN	Brak realizacji kluczowego celu	Poważne obrażenia	Pewne informacje w mediach ogólnokrajowych
3	Średnie	Strata finansowa 10.000 PLN <100.000 PLN	Zakłócenia w działalności	Pewne obrażenia	Pewne informacje w mediach lokalnych lub regionalnych
2	Małe	Strata finansowa 1.000 PLN< 10.000	Niewielkie zakłócenia w działalności	Niewielkie obrażenia	Ograniczone informacje w mediach lokalnych lub regionalnych
1	Nieznaczne	Strata finansowa <1.000	Krótkotrwałe zakłócenia w działalności	minimalne obrażenia	Ubogie informacje w mediach lokalnych lub regionalnych

Źródło: podręcznik zarządzania ryzykiem w polskiej administracji publicznej (MF 2007)

Zarządzanie ryzykiem

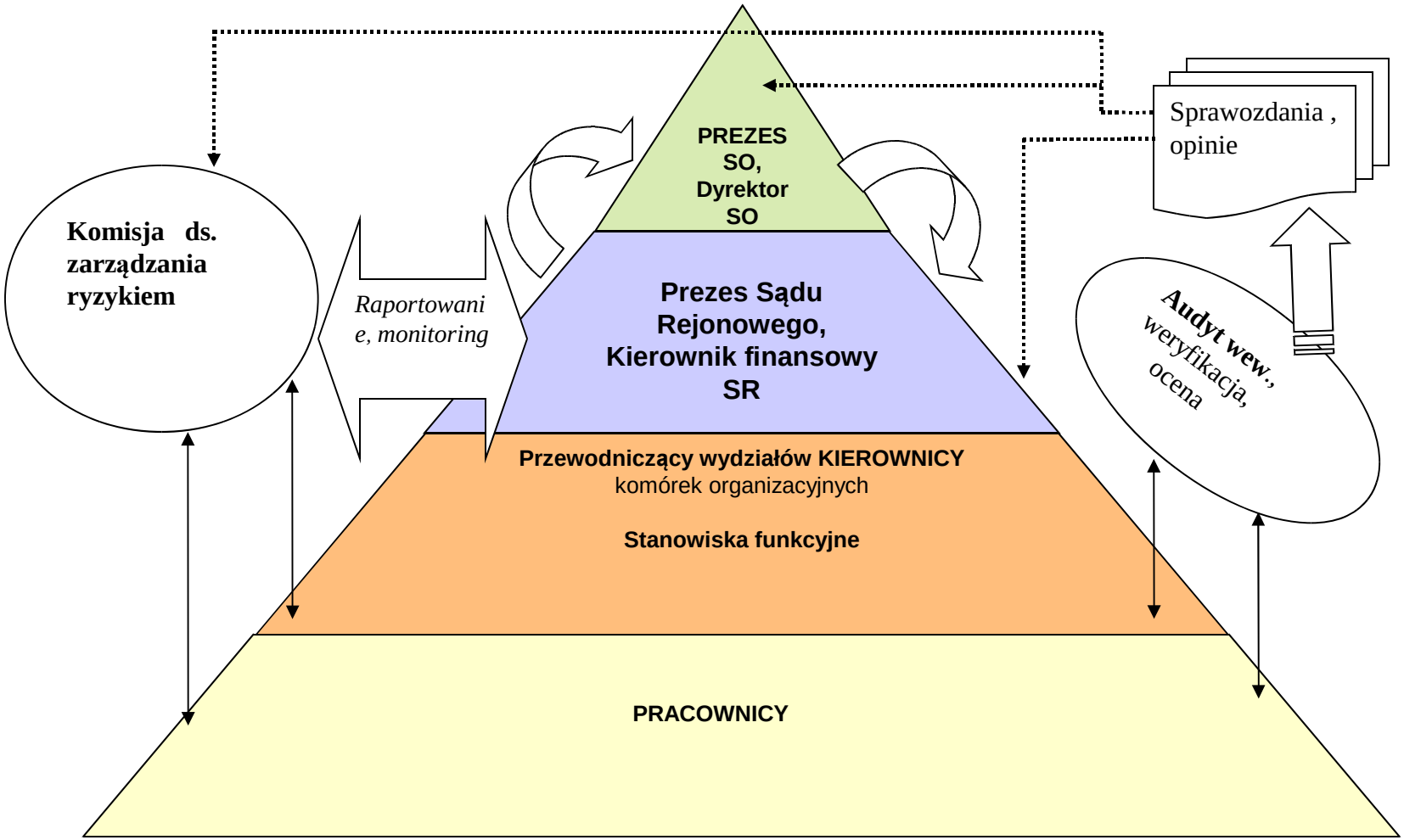
Modelowe podejście
uwzględniające specyfikę Jednostki

Model zarządzania ryzykiem w Sądzie Okręgowym



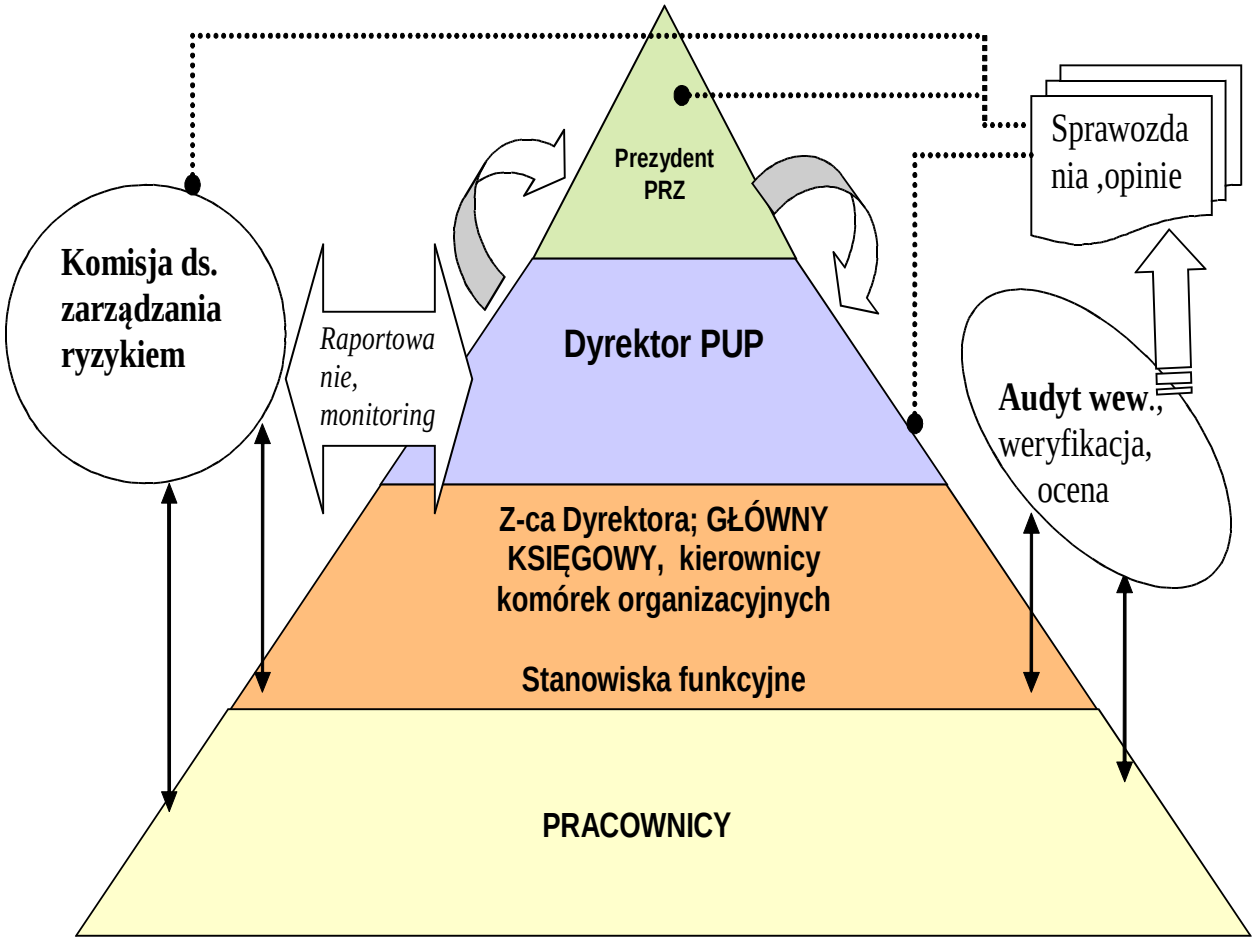
Opracowanie: Krzysztof Radecki, CGAP®

Schemat realizacji procesu zarządzania ryzykiem w Sądzie Rejonowym

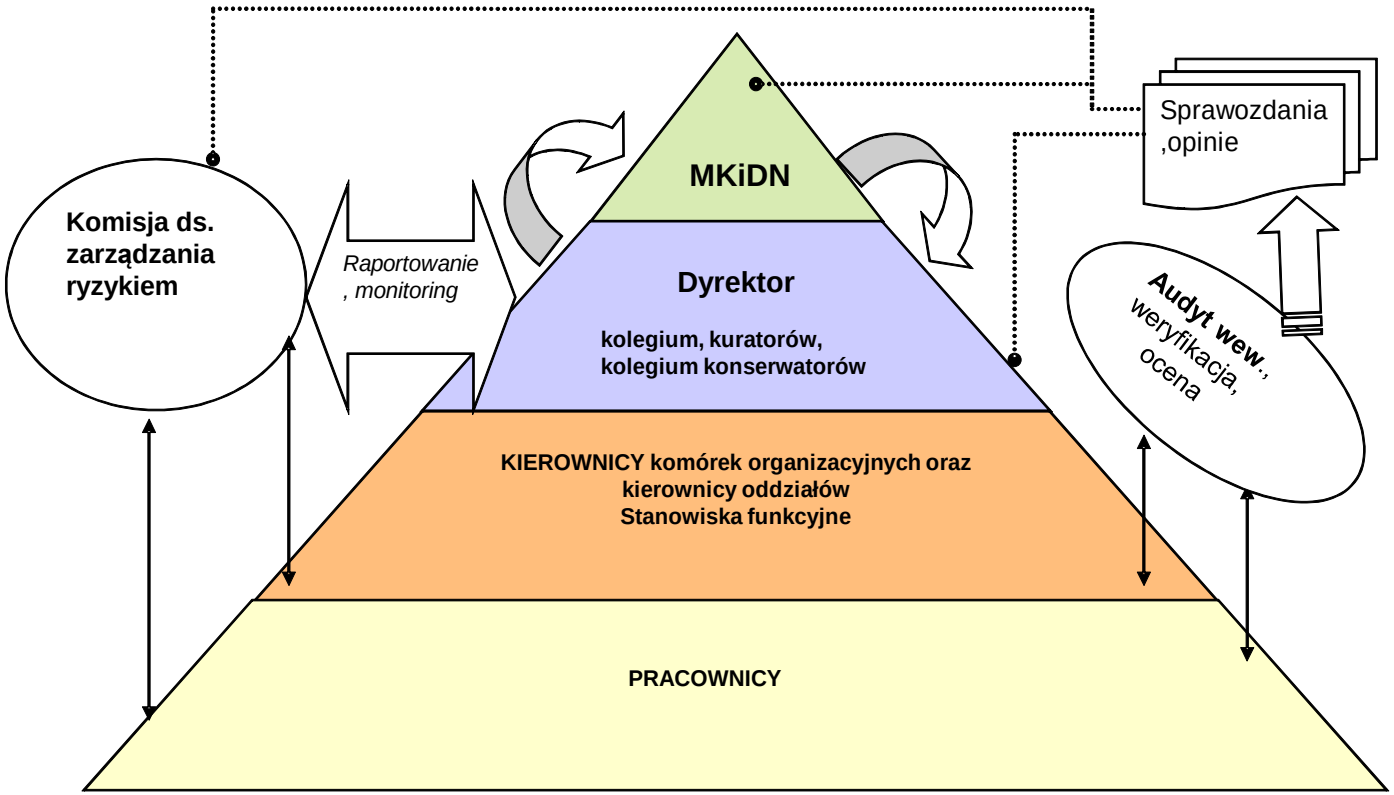


Opracowanie: Krzysztof Radecki, CGAP®

Schemat realizacji procesu zarządzania ryzykiem w Urzędzie Pracy



Model zarządzania ryzykiem w jednostce MKiDN



opracowanie: K.Radecki, CGAP®

Część II

praktyczna ocena ryzyka i sposób zarządzania ryzykiem z wykorzystaniem prostych narzędzi informatycznych - w powiązaniu z realizacją planów działalności jednostki

opracowanie: K.Radecki, CGAP®

ARKUSZ OCENY RYZYK dla jednostki org./Sądu(*) .....

kod jedn. Org.	symbol identyfikacyjny - Kategoria ryzyka (****)	ryzyka wg hierarchii istotności (***)	RYZYKO OPERACYJNE - krótki opis skutków	właściciel ryzyka	Prawgopodobieństwo na dzień oceny (1-5)	Skutek na dzień oceny (1-5)	Status ryzyka wg mapy ryzyka**	Funkcjonujące mechanizmy kontrolne (na dzień oceny) - opis
1	2	3	4	5	6	7	8	9

(*) niepotrzebne skreślić

(**)status ryzyka wg mapy

N	niskie
S	średnie
W	wysokie

(***)hierarchia istotności ryzyka

1- kluczowe o znaczeniu strategicznym, 2- poważne , ze wzgl. na realizowane zadania, 3 - istotne ze względu na zakres realizowanych zadań

(****)symbol identyfikacyjny - kategoria ryzyka

SWS - sprawowanie wymiaru sprawiedliwości

ZNS - zarządzanie należnościami sądu

ZWOT - zapewnienie warunków organizacyjno-technicznych funkcjonowania sądu

F - finansowe

O - organizacyjne

TT - techniczn-technologiczne

OZ - ochrona zasobów

CD - ciągłość działania

Opracowanie:Krzysztof Radecki©, CGAP®

TABELA POWIĄZAŃ - kategorii ryzyka oraz RYZYK *na poziomie operacyjnym*

Symbol identyfikacyjny kategorii ryzyka	kategoria ryzyka	podzadania wg planu działalności (czynniki ryzyka)	procesy wymagające nadzoru (miary oceny wg BZ/PD)	oczekiwane wartości mierników oceny realizacji procesów wg PD MS	RYZYKO OPERACYJNE ,które może mieć wpływ na realizację procesów
1	2	3	4	5	6
SWS	sprawowanie wymiaru sprawiedliwości	Zwiększanie sprawności postępowań sądowych	wskaźnik opanowania wpływu (odniesienie liczby spraw załatwionych przez sądy do liczby spraw wpływających)	103%	organizacja pracy orzeczniczej, obsada etatowa,
	sprawowanie wymiaru sprawiedliwości	ograniczanie poziomu zaległości sądowych	odsetek spraw rozpatrywanych przez sądy I instancji, w których czas trwania postępowania przekracza 12 miesięcy (odniesienie liczby spraw, w których czas trwania postępowania sądowego od dnia pierwszej rejestracji w sądzie I instancji do uprawomocnienia się sprawy/orzeczenia/wyroku w I instancji przekracza 12 miesięcy do liczby spraw uprawomocnionych w I instancji)	4.10%	kompetencje ; sprawność działania i komunikacja
	sprawowanie wymiaru sprawiedliwości	Ułatwianie dostępu obywateli do wymiaru sprawiedliwości	średni czas trwania postępowania w sprawach cywilnych, karnych i gospodarczych (z wyłączeniem spraw wieczystoksięgowych i rejestrowych) (w miesiącach)	1.6	monitorowanie czasu trwania postępowań
	sprawowanie wymiaru sprawiedliwości	Ułatwianie dostępu obywateli do wymiaru sprawiedliwości	odsetek spraw, w których uwzględniono skargi na naruszenie prawa strony do rozpoznania sprawy w postępowaniu sądowym bez nieuzasadnionej zwłoki	0.012%	zabezpieczenie: dokumentów, zbiorów informatyczne itp..
			odsetek obywateli pozytywnie oceniających pracę sądów	34%	zabezpieczenie dostępu do informacji, pieczęci itp..
ZWOT	zapewnienie warunków organizacyjnych i technicznych funkcjonowania sądu	wsparcie organizacyjno-techniczne działalności sądu	odniesienie liczby infokiosków zainstalowanych w sądach w danym roku do łącznej liczby infokiosków planowanych do zainstalowania w sądach	40%	zabezpieczenie obsługi informatycznej sądu
		wsparcie organizacyjno-techniczne działalności sądu	odniesienie liczby utworzonych w danym roku w sądach punktów obsługi interesantów do liczby punktów planowanych do utworzenia	100%	działalność remontowo-inwestycyjna
					realizacja zakupów , zamówień publicznych
ZNS	zrządzanie należnościami sądu	organizacja procesu monitorowania sytuacji dłużników			brak zastępstw w sekcji egzekucji (orzeczników i urzędników)
		czynności egzekucyjne			niedostateczna obsada kadrowa w sekcji egzekucji
		wsparcie techniczne obsługi dłużników sądu			niewydolność serwerów lub sieci w obsłudze aplikacji przeznaczonych do wsparcia procesu monitorowania sytuacji dłużników sądu
					problemy ze spójnością orzeczeń kar grzywien lub kosztów - brakiem możliwości stosowania kar zastępczych

O	**organizacyjne**	struktra organizacyjna (podleglość , zakres kompetencji)			brak precyzyjnego określenia zakresu kompetencji, odpowiedzialności i uprawnień
		współpraca pomiędzy komórkami organizacyjnymi			nieokreślone lub brak zasad współpracy pomiedzy komórkami organizacyjnymi jednostki
		podległość organizacyjna			niewłaściwa lub nieczytelna struktura organizacyjna jednostki
		kompetencje kierownictwa i pracowników funkcyjnych			niedostateczne (zbyt niskie) komptencje pracowników i osób funkcyjnych
		podział obowiązków i kompetenecji			nieadekwatny (nierównomierny) podział obowiązków i zadań
TT	**techniczno-technologiczne**	dostępność technologii			brak dostatecznych środków finansowych dot. zakupów lub wdrożenia rozwiązań techn-technolog.
		mozliwość spełnienia warunków techniczno-technologicznych jednostek organizacyjnych sądu			ograniczony zakres wsparcia techniczno-technologicznego w realizowanych projektach
		bariery technologiczne			brak odpowiedniej infrastruktuty technicznej w sądzie
F	**finansowe**	*ewidencja księgowa*			planowanie finansowe
		sprawozdawczość finansowa i budżetowa			terminowość i kompletność sprawozdań
		rozliczenia finansowe			poprawność kwalifikacji wydatków
		obsługa kasowo-bankowa			bezpieczeństwo obrotu gotówkowego
OZ	**ochrona zasobów**	*bezpieczeństwo systemów informatycznych i przetwarzania informacji*			nieodpowiednie warunki lokalizacji pomieszczenia serwerowni
		zabezpieczenie miejsc przetwarzania informacji wszelkiego rodzaju			brak określenia miejsca przechowywania kopii zapasowych zbiorów z serwerów (poza siedzibą jednostki)
		ochrona dostępu do miejsc składowania i przetwarzania dokumnetów sądowych i zbiorów infomacji wrażliwych			niedostateczne zabezpieczenie miejsc przechowywania informacji wrażliwych (nieodpowiednie zamki , brak kodowania dostępu etc.)

CD	**ciągłość działania**	*istnienie i przestrzeganie procedur awaryjnych*			brak tzw. alternatywnego źródła zasilania dla jednostki
		dostępność alternatywnego źródła zasilania			brak procedur zabezpieczenia kluczy, kodów dostępu do pomieszczeń z dokumentacją archiwalną i systemu powiadamiania o zdarzeniach nagłych
		testowanie procedur awaryjnych			brak ustalonych procedur awaryjnych w związku ze zdarzeniami losowymi oraz sposobu testowania tych procedur
		monitorowanie czasu wznowienia działalności wg ustalonego planu ciągłości działania			brak przyjęcia normy czasu wznowienia działania po ustaniu przyczyn powodujących przerwanie ciągłości działania jednostki oraz monitorowania tego czasu
ZL	**zasoby ludzkie**	*kompetencje kadr*			niedostatecznie wyszkolona kadra
		zakres wymienności stanowisk pracy (mobilności kadr)			zbyt mała wszechstronność pracowników - ograniczenia w zastępstwach
		jakość i częstotliwość szkoleń			zbyt mała częstotoliwość szkoleń, niedostosowanie zakresu szkoleń do potrzeb jednostki
		gotowość do podnoszenia kwalifikacji			ograniczona lub zbyt niska gotowość pracowników do samokształcenia lub uczestnictwa w szkoleniach

Kolumny 1 i 2 zawierają obowiązujący katalog kategorii ryzyk i ich symboli identyfikacyjnych (nie należy ich modyfikować i rozszerzać)
Kolumny 3,4,5 mają charakter informacyjny (pokazują odniesienie niektórych kategorii ryzyk do budżetu zadaniowego oraz opisują główne czynniki ryzyka w kategoriach mające również charakter ryzyk głównych o znaczeniu strategicznym dla sądu)
Kolumna 6 zawiera przykłady ryzyk w poszczególnych ustalonych kategoriach , na poziomie operacyjnym tj. komórek organizacyjnych sądu (można te zapisy uzupełniać wg własnej oceny ryzyka na poziomie komórki organizacyjnej)

Przykład tabeli powiązań dla Jednostki Ratownictwa Medycznego z certyfikacją ISO

TABELA POWIĄZAŃ - kategorii ryzyka oraz RYZYK *na poziomie operacyjnym*

Symbol identyfikacyjny kategorii ryzyka	kategoria ryzyka	podzadania wg planu działalności (czynniki ryzyka)	procesy wymagające nadzoru (miary oceny)	oczekiwane wartości mierników oceny realizacji procesów wg Planu Działania	Opis źródła powstawania RYZYKO OPERACYJNE ,które może mieć wpływ na realizację procesów
1	2	3	4	5	6
MPD	Planowanie dyżurów				
MPT	Pomoc doraźna i transport sanitarny				
ZZI	Zarządzanie infrastrukturą (nadzór nad środkami transportu)				
ZZI	Zarządzanie infrastrukturą (nadzór infrastruktury budowlanej, technicznej, informatycznej)				
ZSP	Sprzedaż				
ZAR	Reklamacje do dostawców				
ZKD	Kwalifikacje i ocena dostawców				
MRM	Ratownictwo medyczne	zabezpieczenie karetek wraz z wyposażeniem	dostosowanie dyspozytorni medycznej do realizacji kontraktu ;	ilość karetek od 43 do 53; ilość stanowisk dyspozytorskich - 4	
MAO	Ambulatoryjna opieka specjalistyczna				
ZAN	Analizy i rozliczenia				
HRM	Zarządzanie zasobami ludzkimi	kompetencje kadr, zakres wymienności stanowisk pracy (mobilności kadr),			niedostatecznie wyszkolona kadra, zbyt mała wszechstronność pracowników - ograniczenia w zastępstwach
HRR	Rekrutacja	zabezpieczenie odpowiedniej ilości pracowników z kwalifikacjami do obsady ambulansów i dyspozytorni medycznej		od 446 do 576	
HRS	Szkolenia	jakość i częstotliwość szkoleń, gotowość do podnoszenia kwalifikacji			zbyt mała częstotoliwość szkoleń, niedostosowanie zakresu szkoleń do potrzeb jednostki, ograniczona lub zbyt niska gotowość pracowników do samokształcenia lub uczestnictwa w szkoleniach
ZZO	Zarządzanie operacyjne	zabezpieczenie odpowiedniejilośći lokali (dyżurek) w rejonach - wg wymagań kontraktu; dostosowanie rozmieszczenia zespołów rat.med. Do planu Wojewody		ilość dyżurek - 10 (wg planu wojewody - 8)	

ZPR	Planowanie rzeczowo-finansowe				
ZAK	Zakupy materiałów i usług				
MTM	Pozostały transport medyczny i sanitarny				
MPOZ	Podstawowa opieka zdrowotna				
CRM	Zarządzanie relacjami z klientem				
O	**organizacyjne**	struktra organizacyjna (podległość , zakres kompetencji)			brak precyzyjnego określenia zakresu kompetencji, odpowiedzialności i uprawnień
		współpraca pomiędzy komórkami organizacyjnymi			nieokreślone lub brak zasad współpracy pomiedzy komórkami organizacyjnymi jednostki
		podległość organizacyjna			niewłaściwa lub nieczytelna struktura organizacyjna jednostki
		kompetencje kierownictwa i pracowników funkcyjnych			niedostateczne (zbyt niskie) komptencje pracowników i osób funkcyjnych
		podział obowiązków i kompetenecji			nieadekwatny (nierównomiemy) podział obowiązków i zadań
OZ	**ochrona zasobów**	*bezpieczeństwo systemów informatycznych i przetwarzania informacji*			nieodpowiednie warunki lokalizacji pomieszczenia serwerowni
		zabezpieczenie miejsc przetwarzania informacji wszelkiego rodzaju			brak określenia miejsca przechowywania kopii zapasowych zbiorów z serwerów (poza siedzibą jednostki)
		ochrona dostępu do miejsc składowania i przetwarzania dokumentów i zbiorów infomacji wrażliwych			niedostateczne zabezpieczenie miejsc przechowywania informacji wrażliwych (nieodpowiednie zamki , brak kodowania dostępu etc.)
CD	**ciągłość działania**	*istnienie i przestżeganie procedur awaryjnych*			brak tzw. alternatywnego źródła zasilania dla jednostki
		dostępność alternatywnego źródła zasilania			brak procedur zabezpieczenia kluczy, kodów dostępu do pomieszczeń z dokumentacją archiwalną i systemu powiadamiania o zdarzeniach nagłych
		testowanie procedur awaryjnych			brak ustalonych procedur awaryjnych w związku ze zdarzeniami losowymi oraz sposobu testowania tych procedur
		monitorowanie czasu wznowienia działalności wg ustalonego planu ciągłości działania			brak przyjęcia normy czasu wznowienia działania po ustaniu przyczyn powodujących przerwanie ciągłości działania jednostki oraz monitorowania tego czasu

Przykład tabeli powiązań dla ZPiSdN

TABELA POWIĄZAŃ - kategorii ryzyka oraz RYZYK *na poziomie operacyjnym dla ZPiSdN*

Symbol identyfikacyjny kategorii ryzyka	kategoria ryzyka	podzadania wg planu działalności (czynniki ryzyka)	procesy wymagające nadzoru (miary oceny wg BZ/PD)	oczekiwane wartości mierników oceny realizacji procesów wg PD MS	Opis źródła powstawania RYZYKO OPERACYJNE ,które może mieć wpływ na realizację procesów
1	2	3	4	5	6
PW	przyjęcie wychowanków	Skuteczna resocjalizacja wychowanków zakładów poprawczych i schronisk dla nieletnich	powrotność wychowanków zakładów poprawczych na drogę przestępstwa	55%	brak odpowiedniej : opinii o wychowanku,badań , wywiadu; niewłaściwe rozpoznanie psychologiczne: nieodpowiednie umieszczenie nieletniego w grupie (izba przejsciowa-grupa wychowawcza)
Szk	działaność szkoły w procesie resocjalizacji	Skuteczna resocjalizacja wychowanków zakładów poprawczych i schronisk dla nieletnich	Przygotowywanie nieletnich do samodzielnego funkcjonowania w społeczeństwie poprzez wyposażanie w umiejętności przydatne na rynku pracy w ramach nowoczesnych i praktycznych kursów zawodowych		motywacja do osiągania lepszych wyników w nauce; wzaorce nauki i wychowania ; współzawodnictwo w nauce.
Int	działaność internatu w procesie resocjalizacji	Skuteczna resocjalizacja wychowanków zakładów poprawczych i schronisk dla nieletnich	liczba wychowanków zakładów poprawczych i schronisk dla nieletnich przeszkolonych w ramach kursów zawodowych w danym roku	500	peroblem w zaresie indywidualnego doboru programu resocjalizacyjnego;
Zdk	działalność zespołu diagnostyczno-kon. W procesie resocjalizacji	Skuteczna resocjalizacja wychowanków zakładów poprawczych i schronisk dla nieletnich	Przygotowanie ram prawnych dla tworzenia i prowadzenia hosteli dla nieletnich przez organizacje społeczne, co pozwoli na zwiększenie miejsc w tego rodzaju placówkach, stanowiących pożądaną formę probacji i odgrywających istotną rolę w procesie usamodzielniania się nieletnich		problem w zakresie doboru indywidulanego programu resocjalizacyjnego; problem doboru zakresu, kierunku i formy nauczania, kształcenia zawodowego, jakimi wychowanek ma zostać objęty
Slzdr	działaność służby zdrowia w procesie resocjalizacji	Skuteczna resocjalizacja wychowanków zakładów poprawczych i schronisk dla nieletnich			możliwosci właściwej diagnostyki uzależnień i chorób o podłoży psychicznym; promocja zdrowia psychicznego i zapobieganiu zaburzeniom psychicznym, zapewnienie osobom z zaburzeniami psychicznymi wielostronnej i powszechnie dostępnej opieki zdrowotnej oraz innych form opieki i pomocy niezbędnych do życia w środowisku rodzinnym i społecznym oraz kształtowaniu wobec osób z zaburzeniami psychicznymi właściwych postaw społecznych, a zwłaszcza zrozumienia, tolerancji, życzliwości, a także przeciwdziałania ich dyskryminacji.

O	**organizacyjne**	struktra organizacyjna (podległość , zakres kompetencji)			brak precyzyjnego określenia zakresu kompetencji, odpowiedzialności i uprawnień
		współpraca pomiędzy komórkami organizacyjnymi			nieokreślone lub brak zasad współpracy pomiedzy komórkami organizacyjnymi jednostki
		podległość organizacyjna			niewłaściwa lub nieczytelna struktura organizacyjna jednostki
		kompetencje kierownictwa i pracowników funkcyjnych			niedostateczne (zbyt niskie) komptencje pracowników i osób funkcyjnych
		podział obowiązków i kompetenecji			nieadekwatny (nierównomiemy) podział obowiązków i zadań
TT	**techniczno-technologiczne**	dostępność technologii			brak dostatecznych środków finansowych dot. zakupów lub wdrożenia rozwiązań techn-technolog.
		mozliwość spełnienia warunków techniczno-technologicznych jednostek organizacyjnych sądu			ograniczony zakres wsparcia techniczno-technologicznego w realizowanych projektach
		bariery technologiczne			brak odpowiedniej infrastruktuty technicznej w sądzie
F	**finansowe**	*ewidencja księgowa*			planowanie finansowe
		sprawozdawczość finansowa i budżetowa			terminowość i kompletność sprawozdań
		rozliczenia finansowe			poprawność kwalifikacji wydatków
		obsługa kasowo-bankowa			bezpieczeństwo obrotu gotówkowego
OZ	**ochrona zasobów**	*bezpieczeństwo systemów informatycznych i przetwarzania informacji*			nieodpowiednie warunki lokalizacji pomieszczenia serwerowni
		zabezpieczenie miejsc przetwarzania informacji wszelkiego rodzaju			brak określenia miejsca przechowywania kopii zapasowych zbiorów z serwerów (poza siedzibą jednostki)
		ochrona dostępu do miejsc składowania i przetwarzania dokumnetów sądowych i zbiorów infomacji wrażliwych			niedostateczne zabezpieczenie miejsc przechowywania informacji wrażliwych (nieodpowiednie zamki , brak kodowania dostępu etc.)
CD	**ciągłość działania**	*istnienie i przestżeganie procedur awaryjnych*			brak tzw. alternatywnego źródła zasilania dla jednostki
		dostępność alternatywnego źródła zasilania			brak procedur zabezpieczenia kluczy, kodów dostępu do pomieszczeń z dokumentacją archiwalną i systemu powiadamiania o zdarzeniach nagłych
		testowanie procedur awaryjnych			brak ustalonych procedur awaryjnych w związku ze zdarzeniami losowymi oraz sposobu testowania tych procedur
		monitorowanie czasu wznowienia działalności wg ustalonego planu ciągłości działania			brak przyjęcia normy czasu wznowienia działania po ustaniu przyczyn powodujących przerwanie ciągłości działania jednostki oraz monitorowania tego czasu
ŻL	**zasoby ludzkie**	*kompetencje kadr*			niedostatecznie wyszkolona kadra
		zakres wymienności stanowisk pracy (mobilności kadr)			zbyt mała wszechstronność pracowników - ograniczenia w zastępstwach
		jakość i częstotliwość szkoleń			zbyt mała częstotoliwość szkoleń, niedostosowanie zakresu szkoleń do potrzeb jednostki
		gotowość do podnoszenia kwalifikacji			ograniczona lub zbyt niska gotowość pracowników do samokształcenia lub uczestnictwa w szkoleniach

Opracowanie:Krzysztof Radecki©, CGAP®

Przykład tabeli powiązań dla jednostki MKiDN

TABELA POWIĄZAŃ - kategorii ryzyka oraz RYZYK na poziomie operacyjnym

kategoria ryzyka	podzadania wg budżetu zadaniowego - planu działalności (czynniki ryzyka)	procesy wymagające nadzoru (miary oceny wg BZ)	Opis źródła powstawania RYZYKO OPERACYJNE ,które może mieć wpływ na realizację procesów
1	2	3	4
Arch - archiwizacja	Utrzymywanie muzeów	Gromadzenie, bezpieczne przechowywanie i udostępnianie zbiorów muzealnych	brak właściwego zabezpieczenia zbiorów pod względem ochrony fizycznej, przechowywanie w nadmiernie zagęszczonych magazynach lub w sposób grożący ich zniszczeniem albo uszkodzeniem
Inw i wyp - inwentaryzacja i wypożyczenia	Zachowanie, utrzymanie i zagospodarowanie zabytków	Poprawa stanu zachowania zabytków ruchomych i nieruchomych	zaległości i nieprawidłowości w ewidencjonowaniu muzealiów, nieprzestrzeganie obowiązku przeprowadzania okresowych inwentaryzacji zbiorów, nie przestrzeganie obowiązujących przepisów prawnych określających warunki, sposób i tryb przenoszenia muzealiów; zaniechania sporządzania protokółów zdawczo-odbiorczych, stwierdzających przeniesienie zabytku; brak: dokładnego opisu wypożyczonego obiektu, kart katalogu naukowego, dokumentacji wizualnej, oceny konserwatorskiej, określenia wymaganych warunków przechowywania; zaległości lub nieprawidłowości w ewidencjonowaniu muzealiów.
GiZ - galerie i zbiory	Upowszechnianie i promocja kultury polskiej	Rozwój i upowszechnianie kultury poprzez działania edukacyjne	ograniczone środki na działalność wystawienniczą, znaczne uszczuplenie zbiorów (tematyczne); brak odpowiednich przepisów dotyczących muzealiów przejętych przez państwo polskie po II wojnie światowej i przekazanych do muzeów, w stosunku do których byli właściciele mogą zgłaszać roszczenia o zwrot.
Kons - konserwacja	Działalność wystawiennicza	Rozwój i upowszechnianie kultury polskiej poprzez działalność wystawienniczą	brak okresowego opracowywania harmonogramów prac konserwatorskich, brak odpowiednich materiałów do konserwacji, znaczna skala uszkodzeń wymagająca długotrwałych zabiegów konserwatorskich, prowadzenie prac konserwatorskich w zbyt ograniczonym zakresie

Opracowanie:Krzysztof Radecki©, CGAP®

Rejestr i ocena ryzyka

dla

Data aktualizacji:

							Ocena ryzyka								
kod jedn. Org.	ryzyka wg hierarchii istotności	Kategoria ryzyka *	RYZYKO OPERACYJNE / skutkl	Własciciel ryzyka	Status (oddziaływanie wg mapy ryzyka) **	Prawgopodobieństwo na dzień oceny (1-5)	Skutek na dzień oceny (1-5)	Funkcjonujące mechanizmy kontrolne (na dzień oceny) - opis	Prawdopodobieństwo faktyczne *** - tj po zastosowaniu mechanizmuu kontrolnego	Skutek po zastosowaniu mechanizmu kontrolnego	priorytet kierownictwa (0,1,2,3)	Końcowa ocena poziomu ryzyka (%) faktycznego**** (10*11+12)	Wymagane działania	Termin realizacji, osoba odpowiedzialna
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0.00	0	0				0.00%		
0	0	0	0	0	0	0.00	0	0				0.00%		
0	0	0	0	0	0	0.00	0	0				0.00%		

dane przenoszone automatycznie z arkusza oceny ryzyka

*** kategoria ryzyka -**

SWS - sprawowanie wymiaru sprawiedliwości
ZNS - zarządzanie należnościami sądu
ZWOT - zapewnienie warunków organizacyjno-technicznych funkcjonowania sądu
F - finansowe
O - organizacyjne
TT - techniczn-technologiczne
OZ - ochrona zasobów
CD - ciągłość działania
ZL - zasoby ludzkie

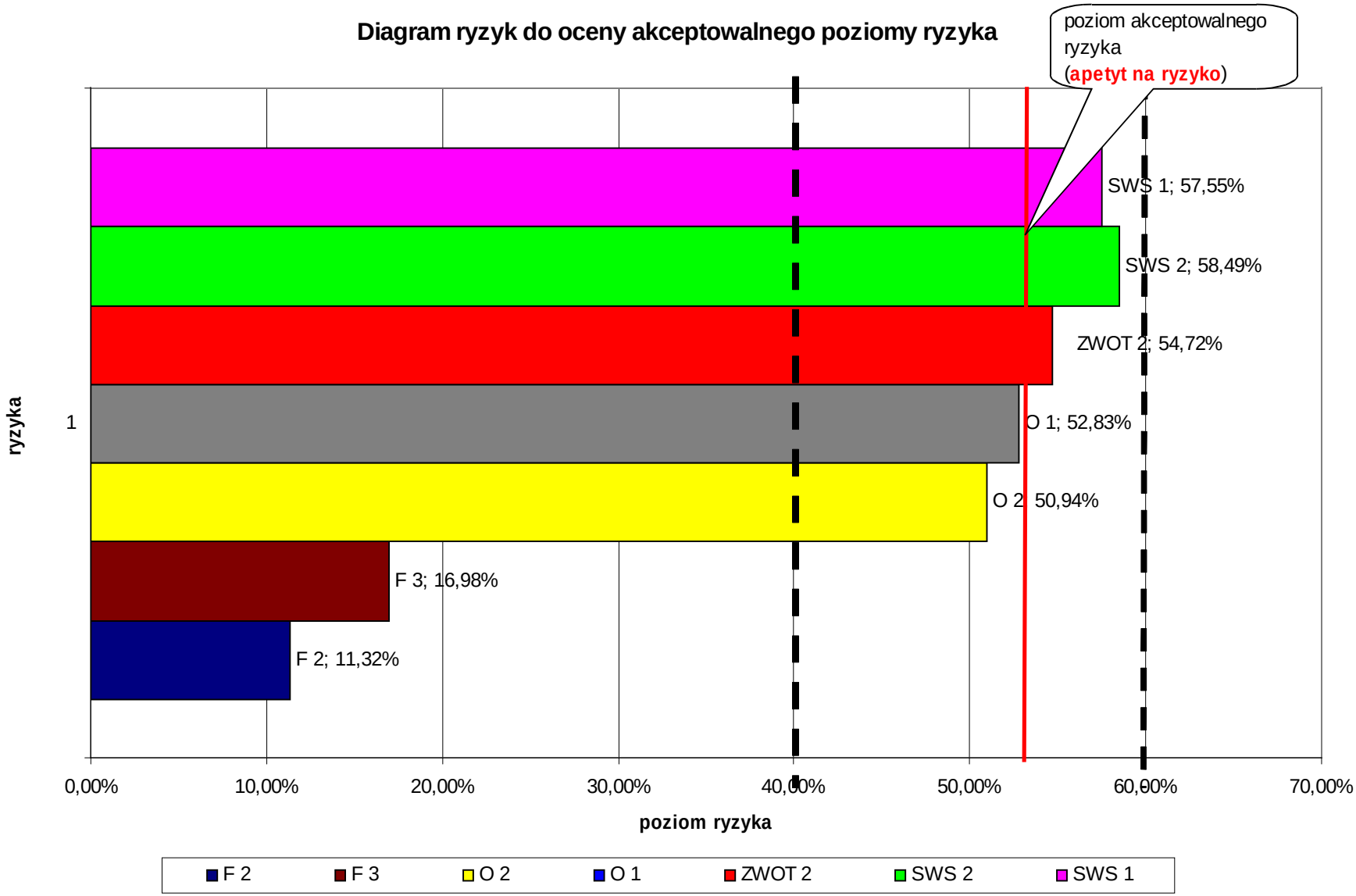
** ***status*** W- Wysokie, S - średnie, N-niskie

*** ***Prawdopodobieństwo faktyczne*** - ocenione wg skali ocen prawdopodobieństwa: od 1 do 5

**** ***końcowa ocena ryzyka*** - zawiera element priorytetu kierownictwa (apetytu na ryzyko)

poziom ryzyka	*(ocena końcowa)*
Niski (N)	<40%
Średni (S)	>40% - ≤60%
Wysoki (W)	>60%

- Ostatecznej oceny i kwalifikacji ryzyka dokonuje Kierownik Jednostki, uwzględniając opinie i oceny prezentowane przez Komisję ds.ZR
- Wyniki tej oceny ryzyka mogą zostać przedstawione ,dla celów decyzyjnych, w formie diagramu ryzyk dla Jednostki – celem określenia „poziomu ryzyka akceptowalnego”



Opracowanie:Krzysztof Radecki©, CGAP®

Role : Kierownika jednostki i audytu wewnętrznego.

- **Kierownik Jednostki** , we współpracy **z Komisją ds. ZR**, określa jakie działania zostaną podjęte w procesie ZR, informuje osoby odpowiedzialne za realizację zadań obarczonych znacznym ryzykiem o działaniach jakie są zobowiązane podjąć w celu ograniczenia ryzyka.
- **Audytor wewnętrzny** ocenia działanie ustanowionych mechanizmów kontrolnych w trakcie realizacji zadań zapewniających i doradczych.
- **Audyt wewnętrzny sporządza raport roczny nt. działania systemu KZ**, która zawiera informację o stwierdzonych słabościach w ustanowionych mechanizmach kontrolnych, nowych, potencjalnych ryzykach, zagregowanych wynikach kontroli zewnętrznych lub innych przeglądów dokonywanych w jednostce, a także o innych problemach związanych z systemem KZ. ***Adresatem raportu jest Kierownik Jednostki i Przewodniczący Komisji ds. ZR***.

Elementy dokumentowania KZ
na poziomie jednostki

- **OŚWIADCZENIE PÓŁROCZNE O STANIE REALIZACJI ZADAŃ W OBSZARZE KONTROLI ZARZĄDCZEJ**
- **ARKUSZ SAMOOCENY SYSTEMU KONTROLI ZARZĄDCZEJ**

OŚWIADCZENIE O STANIE REALIZACJI ZADAŃW OBSZARZE KONTROLI ZARZĄDCZEJ

za okres od :……. do :……

zgodnie z obowiązującym regulaminem kontroli zarządczej oraz przyjętym modelem zarządzania ryzykiem w sądzie ……
(zarządzenie nr …… z dnia ……. Prezesa Sądu ……)

lp	zagadnienie	Treść deklaracji	uwagi
1	Dokonałem oceny funkcjonowania systemu kontroli zarządczej w obszarze który nadzoruję i stwierdziłem następujące nieprawidłowości :		
2	Wprowadziłem następujące mechanizmy (działania) korygujące funkcjonowanie systemu kontroli zarządczej w nadzorowanym obszarze:		
3	W sposób systematyczny prowadzona jest kontrola funkcjonalna i samokontrola wg ustalonego planu kontroli w nadzorowanym przeze mnie obszarze:		
4	Stwierdzone nieprawidłowości i uchybienia w przeprowadzonych kontrolach funkcjonalnych i procesie samokontroli:		
5(*)	Zalecenia pokontrolne przekazane podległym pracownikom (w ramach kontroli funkcjonalnej):		

(*) nie dotyczy stanowisk samodzielnych

(**)niepotrzebne skreślić

Realizacja zaleceń pokontrolnych zostanie poddana ocenie w okresie :

System kontroli zarządczej w nadzorowanym przeze mnie obszarze jest / jest ale z zastrzeżeniami ** : rzetelny, adekwatny do zakresu zadań realizowanych w podległym mi obszarze.

Zastrzeżenia dotyczą :

data, podpis: ……..

Kierownik komórki org.

Przew. wydziału/Stan.samodzielne

Arkusz samooceny KZ w Sądzie

dla komórki org./wydziału/stanowiska(*)

lp	zagadnienie	tak	nie	uwagi
1	Czy kwalifikacje pracowników (poziom wiedzy, umiejętności i doświadczenie) w Pani/Pana komórce/jednostce organizacyjnej odpowiadają realizowanym przez nich zadaniom?			
2	Czy organizowane są szkolenia dla pracowników celem podwyższenia ich kwalifikacji niezbędnych do wykonywania zadań?			
3	Jakie obejmują stanowiska i częstotliwość szkoleń – opisać.			
4	Czy dokonywane są wewnętrzne oceny pracowników?			
5	Czy struktura organizacyjna jest adekwatna do charakteru działalności Pani/Pana komórki/jednostki?			
6	Czy pracownicy zapoznawani są z regulaminami/zarządzeniami oraz zmianami wprowadzanymi do nich?			
7	Czy wszyscy pracownicy posiadają aktualne zakresy zadań, w których określono zakres obowiązków, odpowiedzialności i uprawnień?			
8	Czy zakres uprawnień powierzonych poszczególnym kierownikom / pracownikom jest precyzyjnie określony, odpowiedni do wagi podejmowanych decyzji i ryzyka z nimi związanego?			
9	Czy upoważnienia są aktualizowane, w miarę zachodzących potrzeb (np. w przypadku zmian wprowadzonych przepisami prawa)? Jeśli nie, opisać dlaczego			
10	Czy w Pani/Pana komórce/jednostce prowadzony jest bieżący monitoring / ocena realizacji zadań za pomocą: mierzalnych wskaźników, precyzyjnie zdefiniowanych kryteriów. Jeśli tak opisać jakich, jeśli nie opisać dlaczego.			

Część II

rola i miejsce oceny ryzyka bezpieczeństwa informacji w systemie kontroli zarządczej.

opracowanie: K.Radecki, CGAP®

Istotne zmiany w systemie KZ jakie powinny być wprowadzone w związku z wprowadzeniem SZBI

- Wskazane jest rozszerzenie kompetencji Zespołu ds. zarządzania ryzykiem;
- Zespół ds. zarządzania ryzykiem powinien być przekształcony w „Zespół ds koordynacji bezpieczeństwa informacji i zarządzania ryzykiem”;
- Wyniki analizy ryzyka bezpieczeństwa informacji ,którą na bieżąco wykonywać powinien Kierownik OI/Informatyk oraz ABI , powinny być przekazywane do Zespołu jw. w celu włączenia tych informacji do wspólnego rejestru ryzyk sądu.

Zasady nadrzędne zarządzania bezpieczeństwem informacji

W Sądzie ..... stosowana jest zasada odpowiedzialności za bezpieczeństwo informacji wszystkich członków kierownictwa.

Schemat organizacji zarządzania bezpieczeństwem informacji w Sądzie stanowi załącznik nr 2 do niniejszego opracowania.

Za wyznaczanie kierunków działań w zakresie rozwoju bezpieczeństwa informacji oraz udzielanie wsparcia w zakresie podejmowanych inicjatyw w obszarze bezpieczeństwa informacji, zarówno przez pracowników jak i kierowników poszczególnych komórek / jednostek organizacyjnych – odpowiedzialny jest Zespół ds. koordynacji bezpieczeństwa informacji i zarządzania ryzykiem (zwany dalej ZESPOŁEM) .

Prezes Sądu lub wyznaczony przez niego Wiceprezes przewodniczy pracom ZESPOŁU

W skład ZESPOŁU oprócz Prezesa Sądu (lub Wiceprezesa) wchodzą:

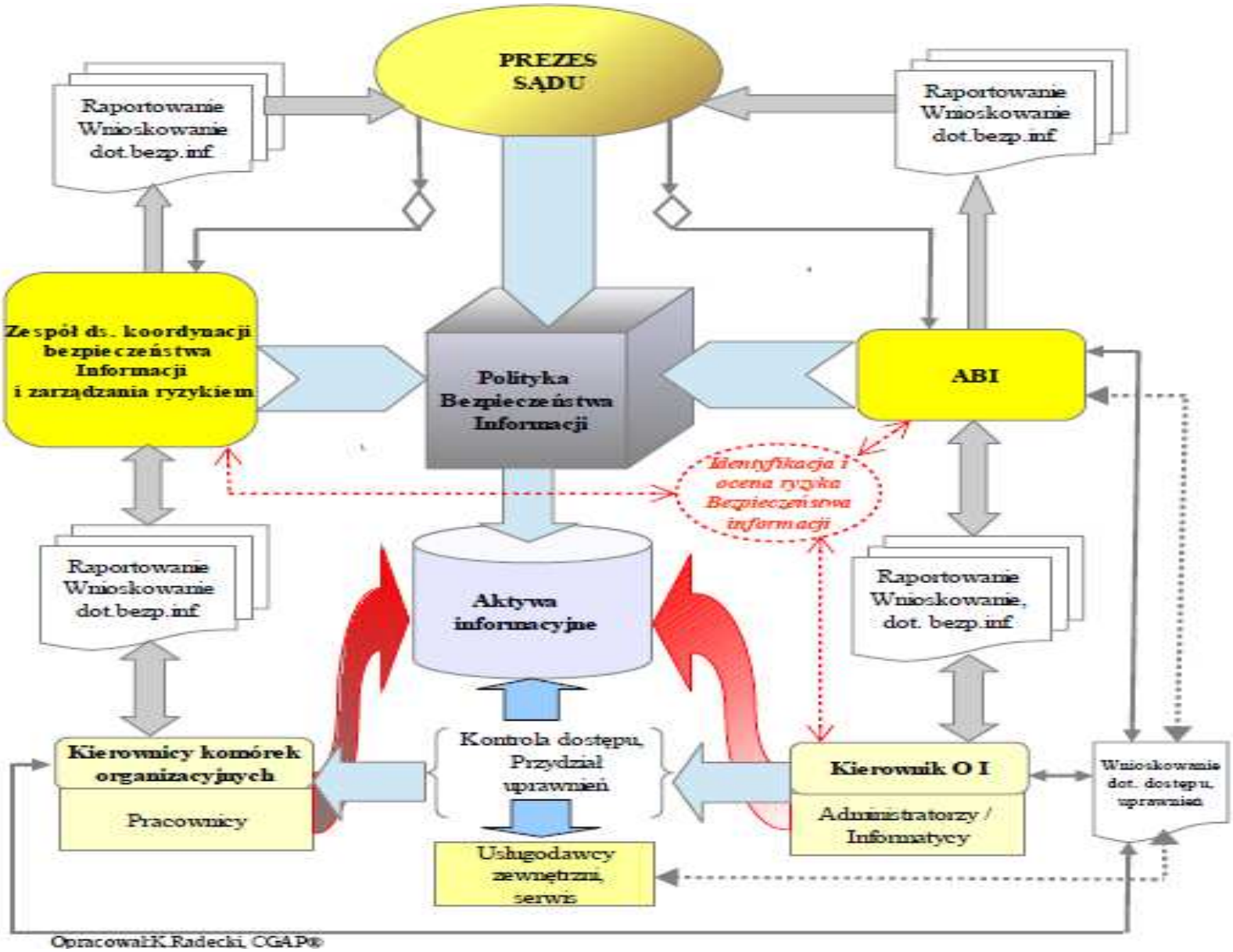
Administrator bezpieczeństwa informacji

Kierownik Oddziału Informatycznego

oraz przedstawiciele wybranych komórek organizacyjnych sądu (tj.: wydziałów , oddziałów, stanowisk samodzielnych), które pełnią kluczowe role w organizacji jednostki.

Pełny skład Zespołu i jego przewodniczącego powołuje odrębnym zarządzeniem Prezes Sądu.

Schemat organizacji zarządzania bezpieczeństwem informacji w Sądzie



Przykład - SCHEMATU FUNKCJONOWANIA PBI

POLITYKA BEZPIECZENSTWA INFORMACJI
W ……

Postanowienia ogólne

Zasady funkcjonowania polityki bezpieczenstwa informacji

Ogólne i szczególne obowiazki w odniesieniu do zarzadzania bezpieczenstwem informacji

Dokumenty uzupelniajace polityke bezpieczenstwa informacji

REGULAMINY, INSTRUKCJE I PROCEDURY

- Regulamin organizacji bezpieczenstwa i ochrony przetwarzania informacji

- Regulamin organizacji stanowiska pracy Administratora Bezpieczenstwa informacji
- Plan ciaglosci dzialania

- Instrukcja postepowania w sytuacji naruszenia ochrony informacji
- Instrukcja zabezpieczenia miejsc przetwarzania i gromadzenia informacji
- Instrukcja zarzadzania procesami przekazywania informacji
- Instrukcja uzytkowania systemu informatycznego i internetu w jednostce

- Procedura zarzadzania prawami dostepu do zasobów informatycznych systemów sieciowych jednostki
- Procedura wykonywania kopii zapasowych

Opracowanie: Krzysztof Radecki, CGAP®

Regulamin organizacji stanowiska pracy
Administratora Bezpieczeństwa Informacji. ***(przykład***)

Osoba pełniąca funkcję **Administratora Bezpieczeństwa Informacji** (ABI) **podlega bezpośrednio Kierownikowi Jednostki** .
ABI jest odpowiedzialny za nadzór we wdrożeniu , modyfikacji i aktualizacji polityki bezpieczeństwa (tworzenie i opiniowanie różnych instrukcji, regulaminów, procedur, dokumentacji).

ABI wspólnie z kierownikami komórek/jednostek organizacyjnych prowadzi działania szkoleniowe w zakresie wdrożenia i upowszechnienia znajomości polityki bezpieczeństwa informacji w Jednostce. Po zakończeniu prac wdrożeniowych prowadzi stałe działania weryfikujące stosowanie PBI oraz w razie konieczności podejmuje stosowne działania o charakterze restrykcyjnym (w ramach obowiązujących przepisów w tym zakresie, w tym szczególnie określone obowiązującymi normami i zasadami opisanymi w PBI).

W tworzenia świadomości wśród pracowników Jednostki o potrzebie znajomości i stosowania zasad bezpieczeństwa informacji określonych w PBI , **Administrator Bezpieczeństwa Informacji inspiruje organizację permanentnych szkoleń wszystkich pracowników Jednosrtki** , pamiętając o nadrzędnej zasadzie w strategii zarządzania bezpieczeństwem informacji, tzn. „wiedza = bezpieczeństwo”.

Administrator Bezpieczeństwa Informacji musi mieć świadomość istnienia wewnętrznej bariery psychicznej akceptowalności użytkowników systemu informatycznego (tzn. „widzą potrzebę istnienia ABI, ale... lepiej, żeby nie patrzył im na ręce!”).

ABI powinien dbać o to , ażeby polityki bezpieczeństwa nie była zbiorem dokumentów zbyt szczegółowych i niezrozumiałych dla przeciętnego odbiorcy, ponieważ będzie to stwarzać konieczność zbyt częstej aktualizacji tego dokumentu co może powodować poważną barierę organizacyjną – w myśl zasady , kto i kiedy ma to robić?.

Opracowanie: Krzysztof Radecki, CGAP®

Niezbędne cechy psychologiczne ABI to: precyzja w działaniu, spokój w sytuacjach stresowych, brak roztargnienia, podzielność uwagi, skrupulatność, umiejętność kojarzenia pozornie odległych faktów.

Niezbędne są narzędzia do monitorowania sieci, łamania haseł i wykrywania oraz łatania dziur systemowych. Narzędzia te ABI powinien używać zawsze w obecności administratora systemów informatycznych lub indywidualnie, ale po uprzedzeniu administratora.

Przy współpracy ze służbami informatycznymi Jednostki należy brać pod uwagę to, że może być kilku administratorów systemowych/aplikacji (od systemów sieciowych, od aplikacji etc.) pomimo, że w Jednostce jest osoba nadzorująca ich pracę – Koordynator Służby Informatycznej , **ABI powinien w swej pracy podejmować bezpośrednią współpracę z każdym z administratorów** .

ABI w szczególnie ważnych zastosowaniach systemów, **powinien rozważyć konieczność dokonywania zewnętrznego audytu bezpieczeństwa informacji w okresach 2-3 letnich**.

Funkcje ABI może pełnić jednocześnie Pełnomocnikiem ochrony informacji niejawnej. Połączenie tych funkcji jest możliwe z uwagi na brak kolizji w tej kwestii pomiędzy ustawami UODO i UOIN.

ABI powinien współdziałać z innymi służbami Jednostki odpowiedzialnymi za ochronę i bezpieczeństwo informacji w tym z : służbami zajmującymi się ochroną fizyczną i techniczną, służbami ochrony informacji tj. w szczególności służbą informatyczną Jednostki. Działania tych służb i ABI powinny być komplementarne.

Dużą ostrożność należy zachować przy serwisie (w szczególności zdalnym) systemów informatycznych firm z zewnątrz, które nadzorują i pielęgnują sprzęt oraz oprogramowanie. **ABI powinien opiniować w tym przypadku umowy zawierane z tymi firmami** (przed ich formalnym podpisaniem) , pod względem ich zgodności z zasadami, opisanymi w PBI,

wykonywania tych czynności.

Opracowanie: Krzysztof Radecki, CGAP®

PRZYKŁAD , raportu składanego przez komórkę IT

RAPORT
dla ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI
W SPRAWIE USUNIĘCIA SKUTKÓW NARUSZENIA OCHRONY INFORMACJI

1. **Zgłaszający informację (imię, nazwisko, stanowisko służbowe):**

   ……..

2. **Informacje szczegółowe:**

Rodzaj naruszenia ochrony informacji	Skutki naruszenia ochrony informacji	Termin i sposób usunięcia skutków naruszenia ochrony informacji.

3. **Wykaz dokumentów dodatkowych załączonych do raportu, potwierdzających usunięcie skutków naruszenia ochrony informacji** *(notatki służbowe, protokoły, ekspertyzy, etc.)***:**

4. **Wnioski** (propozycje działań eliminujących tego typu zagrożenia w przyszłości):

data i podpis zgłaszającego: data i podpis ABI:

PRZYKŁAD , raportu składanego przez Kierownika komórki IT

RAPORT
dla Administratora bezpieczeństwa informacji
W SPRAWIE NARUSZENIA OCHRONY INFORMACJI

1. **Zgłaszający informację (imię, nazwisko, stanowisko służbowe):**

   .....

2. **Informacje szczegółowe:**

Rodzaj naruszenia ochrony informacji	Data stwierdzenia	Dokładny opis okoliczności	Skutki naruszenia ochrony informacji
Próba nielegalnego dostępu do informacji (logowania,kopiowania , usunięcia etc.)			
Utrata/uszkodzenie danych w wyniku zainfekowania systemu np. poprzez dostęp intruza z sieci wewnętrznej lub zewnętrznej			
Uszkodzenie/ naruszenie ochrony fizycznej dostępu do informacji			
Uszkodzenie/ naruszenie ochrony programowej dostępu do informacji			
Inne przypadki			

3. **Wykaz dokumentów dodatkowych załączonych do raportu, potwierdzających naruszenie ochrony informacji** (wydruk logów, zrzuty ekranów, inne):
4. **Termin i sposób usunięcia skutków naruszenia ochrony informacji**

5. **Wnioski (propozycje działań eliminujących tego typu zagrożenia w przyszłości):**

data i podpis zgłaszającego: data i podpis ABI

PRZYKŁAD , raportu składanego przez Kierowników komórek org.

RAPORT
dla Zespołu ds. koordynacji bezpieczeństwa informacji i zarządzania ryzykiem
W SPRAWIE NARUSZENIA OCHRONY INFORMACJI

1. Zgłaszający informację (imię, nazwisko, stanowisko służbowe):

.....

2. Informacje szczegółowe:

Rodzaj naruszenia ochrony informacji	Data stwierdzenia	Dokładny opis okoliczności	Skutki naruszenia ochrony informacji
Utrata/uszkodzenie danych			
Brak możliwości logowania w systemie			
Awaria systemu operacyjnego (Windows itp.)			
Brak możliwości wydruków			
Inne przypadki			

3. Wykaz dokumentów dodatkowych załączonych do raportu, potwierdzających naruszenie ochrony informacji (wydruki, zrzuty ekranów, inne):

4. Termin i sposób usunięcia skutków naruszenia ochrony informacji

5. Wnioski (propozycje działań eliminujących tego typu zagrożenia w przyszłości):

data i podpis zgłaszającego: data i podpis ABI:

REJESTR (incydentów – zdarzeń)

tj. zgłoszonych awarii w działaniu : *Sprzętu komputerowego, aplikacji (systemu)* ***i innych naruszeń ochrony bezpieczeństwa informacji***

w roku ……

Lp	Imię i nazwisko osoby zgłaszającej (komórka organizacyjna)	***Data zgłoszenia***	***Krótki opis charakteru awarii*** (np. formularza zgłoszeniowego)	***Osoba przyjmująca*** — odpowiedzialna za usunięcie awarii	***Wstępny termin usunięcia awarii*** (np. formularza zgłoszeniowego)	***Zakres prac(czynności)*** — podjętych w ramach usunięcia awarii	*Data zakończenia prac* (usunięcia awarii)	***Podpis osoby weryfikującej wykonanie prac*** (kierownika zespołu)

opracowanie: K.Radecki, CGAP®

Zezwolenie stałe (S) – tymczasowe(T) (*) **nr.....**

Pani/Pan. .....

(imię i nazwisko, stanowisko, komórka organizacyjna , nazwa firmy)

upoważniona/-y jest w dniu ./ na okres ..... do wyniesienia – wniesienia (*) poza/na teren(*)

jednostki …… …… sprzętu komputerowego .....

marki ..... nr seryjny .....

w celu .....

(podać cel wynoszenia - wnoszenia sprzętu komputerowego)

.....

data, podpis Kierownika jednostki lub
Koordynatora Służby Informatycznej

(*) niepotrzebne skreślić

opracowanie: K.Radecki, CGAP®

EWIDENCJA
wydanych <u>zezwoleń stałych</u> na wnoszenie i wynoszenie sprzętu komputerowego

Lp	*Imię i nazwisko* osoby wynoszącej - wnoszącej sprzęt komputerowy	Nr dowodu osobistego	Jednostka /komórka organizacyjna	*Data* wydania zezwolenia	Numer zezwolenia	Rodzaj sprzętu komputerowego / marka i numer seryjny/	Określenie celu wynoszenia - wnoszenia sprzętu komputerowego	Podpis osoby wydającej zezwolenie

opracowanie: K.Radecki, CGAP®

REJESTR
wnoszenia – wynoszenia sprzętu komputerowego na/poza teren jednostki

Lp	*Imię i nazwisko* osoby wynoszącej - wnoszącej sprzęt komputerowy	*Nr dowodu osobistego*	*Nazwa jednostki /komórki org.*	Data wydania zezwolenia	Numer zezwolenia	Rodzaj sprzętu komputerowego / marka i numer seryjny /	Określenie celu wynoszenia – wnoszenia sprzętu komputerowego	Data i Podpis pracownika ochrony

opracowanie: K.Radecki, CGAP®

12 zasad bezpieczeństwa informacji (*)

1. Skup się na celach biznesowych (głównych celach organizacji)
2. Zapewnij odpowiednią jakość i wartość informacji dla interesariuszy
3. Uzyskaj zgodność z odpowiednimi wymogami prawnymi i innymi regulacjami
4. Zapewnij aktualne i dokładne informacje na temat spełnienia wymagań bezpieczeństwa
5. **Dokonuj oceny obecnych i przyszłych zagrożeń informatycznych**
6. Promuj ciągłą poprawę bezpieczeństwa informacji
7. **Przyjmij podejście oparte na ryzyku**, (w odniesieniu do bezpieczeństwa informacji)
8. Chroń informacje niejawne
9. **Skoncentruj się na krytycznych aplikacjach biznesowych (aplikacjach organizacji)**
10. Rozwijaj systemy z zachowaniem bezpieczeństwa
11. Działaj w sposób profesjonalny i etyczny
12. Sprzyjaj rozwojowi pozytywnej kultury bezpieczeństwa

(*) *na podstawie materiałów: ISF, ISACA® i (ISC)2®* *tłumaczenie: K.Radecki, CGAP®*

Podsumowanie rozważań nt.Kontroli zarządczej

1. Jej nadrzędnym celem jest stymulacja realizacji planów działalności;
2. Nie istnieje bez spójnego , udokumentowanego, prowadzonego w sposób ciągły i doskonalonego - zarządzania ryzykiem ;
3. Zarządzanie ryzykiem w obszarze bezpieczeństwa informacji , jest nieodłącznym elementem systemu kontroli zarządczej;
4. KZ – powinna być sformalizowana i udokumentowana, *choć może też mieć charakter nie formalny* ;
5. System KZ obejmuje wszystkie obszary aktywności w jednostce ;
6. Sprawny system KZ wraz z oceną i zarządzaniem ryzykiem w jednostce , umożliwia skuteczną realizację celów organizacji – zarówno strategicznych jak i operacyjnych;
7. Za ustanowienie adekwatnego i skutecznego systemu KZ w jednostce – odpowiada Kierownik jednostki .

opracowanie: K.Radecki, CGAP®

Dziękuję za uwagę