

# SEMINARIA EDUKACYJNE

**WSPÓLNIE**

**dla rynku**



Urząd Regulacji  
Energetyki i  
Gospodarki  
Elektryczną

kdpw



## **Kompleksowy system zarządzania ryzykiem operacyjnym w instytucji finansowej średniej wielkości**

**Andrzej Bajszczak, Dyrektor Biura Bezpieczeństwa KDPW S.A.**

**Rafał Rudzki, Biuro Bezpieczeństwa KDPW S.A.**

*Warszawa, 29 października 2009 roku*

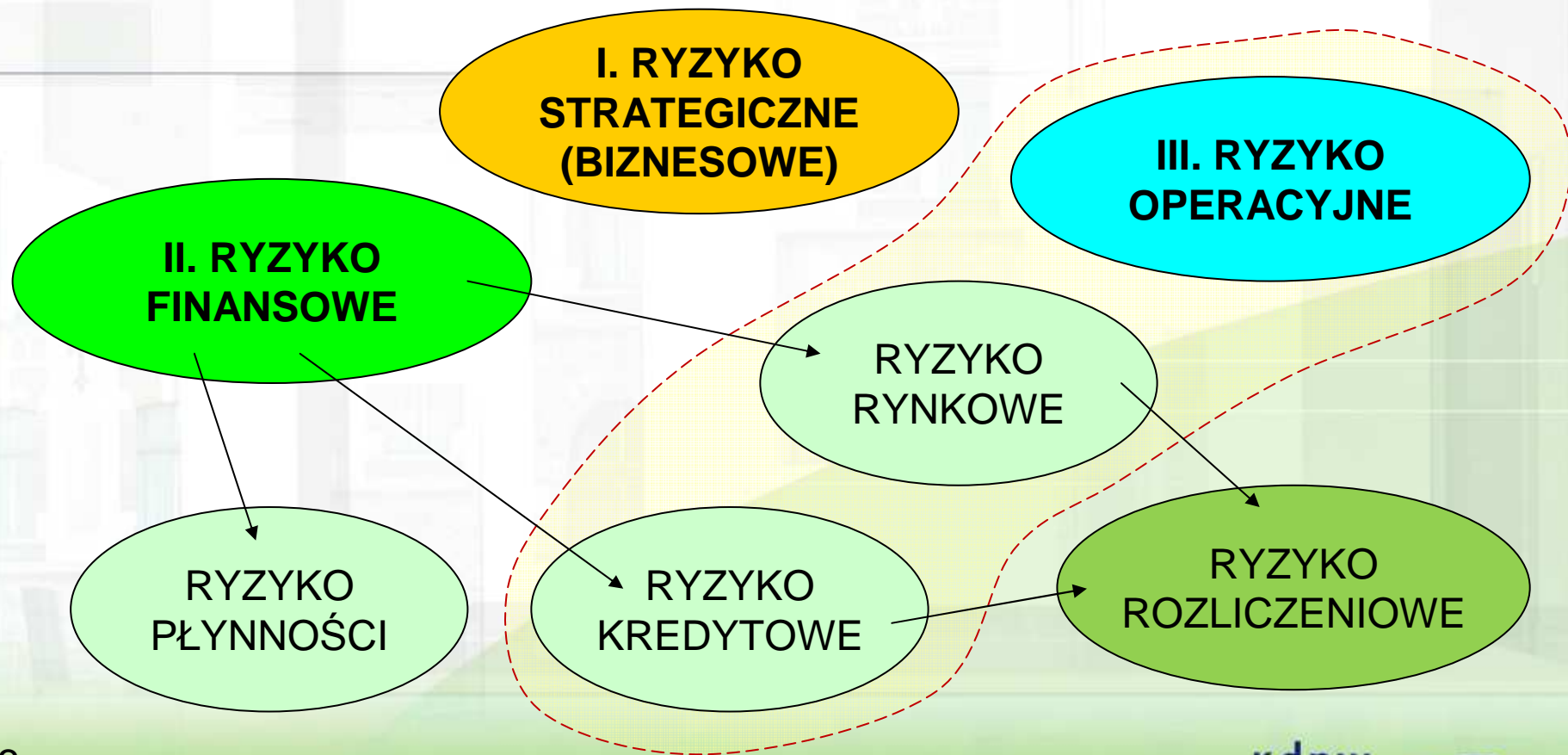
kdpw 

## PODEJŚCIE PRAGMATYCZNE

- Kluczowa idea przy budowaniu kompleksowego systemu zarządzania ryzykiem operacyjnym w **instytucji średniej wielkości to pragmatyzm.**
- Podejście pragmatyczne, wymuszone w mniejszych firmach przez ograniczone środki, może stanowić przy okazji **inspirację dla dużych instytucji finansowych.**

# Ryzyko operacyjne w instytucji średniej wielkości

## RYZYZKO W INSTYTUCJI FINANSOWEJ



# Ryzyko operacyjne w instytucji średniej wielkości

## ZASOBY ZARZĄDZANE W ORGANIZACJI



# Ryzyko operacyjne w instytucji średniej wielkości

## ZASOBY ZARZĄDZANE W ORGANIZACJI c.d.



# Ryzyko operacyjne w instytucji średniej wielkości

## PODZIAŁ KOMPETENCJI



# Ryzyko operacyjne w instytucji średniej wielkości

## AUDYT WEWNĘTRZNY

- Audyt wewnętrzny **powinien powstrzymać się** od następujących czynności:
  - brania odpowiedzialności za proces zarządzania ryzykiem operacyjnym,
  - podejmowania decyzji zarządczych co do wyboru środków ograniczania ryzyka,
  - określania poziomu apetytu na ryzyko.
- W związku z powyższym, audyt wewnętrzny **nie powinien** pełnić funkcji komórki ds. zarządzania ryzykiem.

# Ryzyko operacyjne w instytucji średniej wielkości

## COMPLIANCE

- Zgodnie z obowiązującą definicją ryzyka operacyjnego (Bazylea II / CRD), obejmuje ono **ryzyko prawne**.
- Zgodnie z dyrektywą MiFID, nie musi stanowić zagrożenia dla niezależnego funkcjonowania **zarządzania ryzykiem i nadzoru zgodności z prawem** fakt, iż obie te funkcje należą do obowiązków tej samej osoby (na przeszkodzie może jednak stać kwestia odpowiednich kompetencji merytorycznych danej osoby).

# Ryzyko operacyjne w instytucji średniej wielkości

## PROCES ZARZĄDZANIA RYZYKIEM (OPERACYJNYM)

- Identyfikacja ryzyka

- Pomiar ryzyka



W miejsce niepewności pojawia się rozkład prawdopodobieństwa lub coś o zbliżonym charakterze.

- Monitoring ryzyka

- Kontrola ryzyka

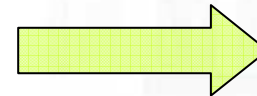
Należy podkreślić, że nie ma to jednak wiele wspólnego z prognozowaniem przyszłych wydarzeń.

# Ryzyko operacyjne w instytucji średniej wielkości

## NIEPEWNOŚĆ A RYZYKO

Pon.	1	2	2	1	0
Wt.	1	1	2	1	0
Śr.	0	0	0	2	1
Czw.	0	2	1	1	2
Pt.	1	1	2	1	1

↑ NIEPEWNOŚĆ ↑



0	24%	25%
1	48%	50%
2	28%	25%
...	?	-

↑ RYZYKO ↑

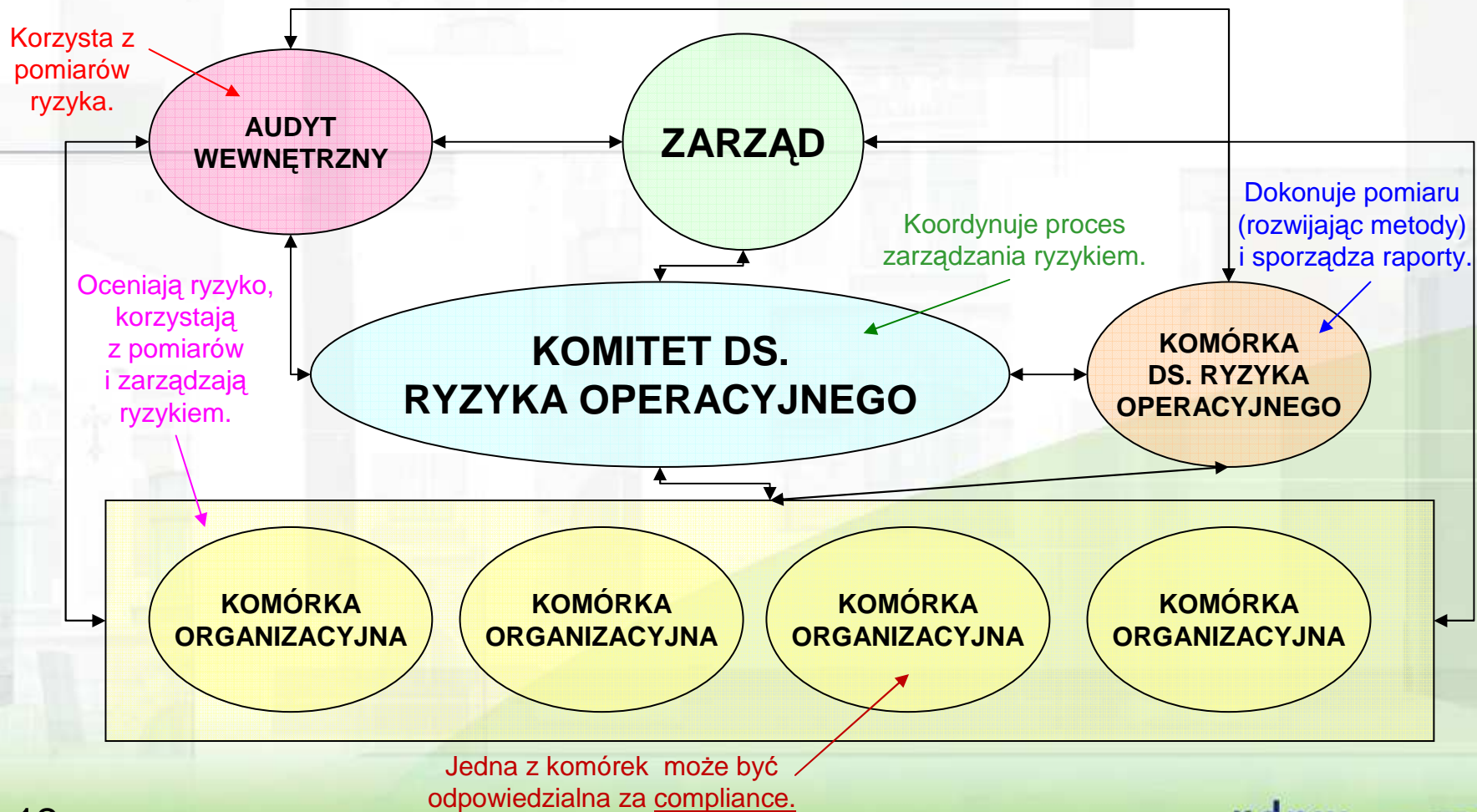
**Ryzyko to niepewność mierzalna.**

## STRUKTURA ORGANIZACYJNA

- **Komórka** ds. ryzyka (operacyjnego) lub **menadżer** ds. ryzyka (operacyjnego) – odpowiedzialność za ogólne funkcjonowanie systemu, w szczególności za **pomiar**.
- **Komitet** ds. ryzyka (operacyjnego) – praktyczna **koordynacja** w ramach działań **zarządczych**.
- **Eksperci** oceniający ryzyko, **korespondenci** zgłaszający incydenty bądź zagrożenia, **odbiorcy raportów** z pomiaru ryzyka.

# Ryzyko operacyjne w instytucji średniej wielkości

## STRUKTURA ORGANIZACYJNA c.d.



## OPIS SYSTEMU ZARZĄDZANIA RYZYZKIEM OPERACYJNYM

- Ogólna **polityka** zarządzania ryzykiem operacyjnym – nadrzędny dokument definiujący **koncepcję systemu**, strukturę organizacyjną, etc.; odsyłający do szczegółowych procedur.
- Szczegółowe **procedury** opisujące stosowane **metody pomiaru** ryzyka operacyjnego, sposób raportowania, kryteria podejmowania działań zarządczych, etc.

## POMIAR RYZYKA - ŹRÓDŁA

- **Dane o rzeczywistych stratach (incydentach):** wewnętrzne oraz zewnętrzne (z innych instytucji).
- **Kluczowe wskaźniki ryzyka (KRI)** – miary ilościowe pośrednio odzwierciedlające poziom ryzyka.
- **Samocena ryzyka (RSA)** oraz **scenariusze strat** (uzupełnienie danych o rzeczywistych stratach).

# Ryzyko operacyjne w instytucji średniej wielkości

## REJESTR ZDARZEŃ RYZYKA OPERACYJNEGO (KDPW)

OpRisk - Rejestr Zdarzeń Ryzyka Operacyjnego - Microsoft Internet Explorer

Plik Edycja Widok Ulubione Narzędzia Pomoc

Wstecz Wyszukaj Ulubione

Adres http://oprisk/opriskrz.php?page=RZPR

kdpw OpRisk Rejestr Zdarzeń Ryzyka Operacyjnego

Strona startowa Przeglądanie rejestru Zgłoszenie do rejestru Strona główna OpRisk Administracja

Rejestr zdarzeń >> Przeglądanie rejestru >>

Dział: == Filtr daty zdarzenia: Filtr treści opisów: Szukaj

Sortowanie - kliknij w nazwę kolumny P - przeglądanie szczegółowe H - historia zmian M - modyfikacja D - duplikacja G - grupa

Id. zdarz.	Grupa	Dział	Data zdarz.	Proces Biznesowy	Czynnik ryzyka	Pow.	Opis zdarzenia	Strata poten.	Strata rzecz.	Data zglosz.	Operacje
------------	-------	-------	-------------	------------------	----------------	------	----------------	---------------	---------------	--------------	----------

Gotowe Zaufane witryny

## REJESTR ZDARZEŃ - SUGESTIE

- Rejestr zdarzeń (strat) jest **niezbędnym elementem** systemu zarządzania ryzykiem operacyjnym także wtedy, gdy nie będzie przeprowadzane modelowanie rozkładu strat w oparciu o dane wewnętrzne.
- Dobrze jest przeznaczyć na potrzeby rejestru zdarzeń zcentralizowaną **bazę danych**.


# Ryzyko operacyjne w instytucji średniej wielkości

## REJESTR ZAGROŻEŃ RYZYKA OPERACYJNEGO (KDPW)

OpRisk - Rejestr Zdarzeń Ryzyka Operacyjnego - Windows Internet Explorer

http://oprisk/opriskrz.php?page=RZPZ

OpRisk - Rejestr Zdarzeń Ryzyka O...

**kdpw**  **OpRisk**  
Rejestr Zdarzeń Ryzyka Operacyjnego

Start Przekładanie zdarzeń Nowe zdarzenie Zagrozenia Strona główna OpRisk Administracja

Rejestr zdarzeń >> Zgłaszanie i przeglądanie zagrożeń >>

Skrócony opis:

Pełny opis:

Proces biznesowy: Nieokreślony

Poważność: 0

Zapis do rejestru zagrożeń

P - pełny opis K - podjęte kroki M - modyfikacja U - usunięcie

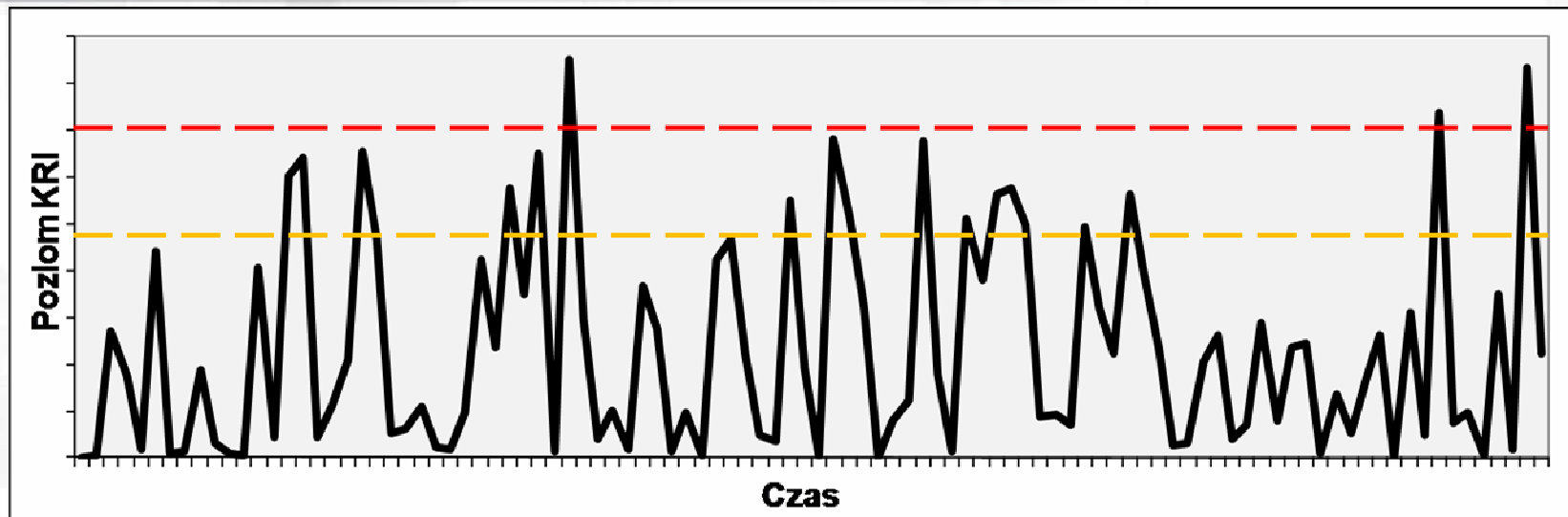
Identyfikator	Skrócony opis	Proces biznesowy	Czynnik ryzyka	Pow.	Data i czas	Autor	Status	Operacje

http://oprisk/opriskrz.php?page=RZPZ

Zaufane witryny 100%

# Ryzyko operacyjne w instytucji średniej wielkości

## KLUCZOWE WSKAŹNIKI RYZYKA



# Ryzyko operacyjne w instytucji średniej wielkości

## KRI - SUGESTIE

- Zapewnienie maksymalnego stopnia **zautomatyzowania** procesu pozyskiwania danych i kalkulacji wskaźników.
- Konieczna **korelacja** (oraz zrozumiały dla wszystkich **związek**) między wyliczonym poziomem danego wskaźnika a określonym czynnikiem ryzyka operacyjnego.

# Ryzyko operacyjne w instytucji średniej wielkości

## KRI – SUGESTIE c.d.

- Konieczność określenia **poziomów tolerancji** dla danego wskaźnika (np. dwa poziomy: żółty i czerwony).
- Włączenie kluczowych wskaźników ryzyka w **proces oceny** ryzyka operacyjnego nie jest trywialną kwestią. Proponowanym rozwiązaniem jest **konwersja** wyliczeń KRI na oszacowania częstotliwości i poważności ryzyka.

# Ryzyko operacyjne w instytucji średniej wielkości

## ANKIETA RYZYKA OPERACYJNEGO (KDPW)

OpRisk - Model Pomiaru Ryzyka Operacyjnego - Microsoft Internet Explorer

Plik Edycja Widok Ulubione Narzędzia Pomoc

Wstecz Wyszukaj Ulubione

Adres http://oprisk/opriskpr.php?page=PRAO&sbpg=QSTP

Przejdź Łącza

kdpw OpRisk  
Model Pomiaru Ryzyka Operacyjnego

Strona startowa Ankieta OpRisk Analizy ryzyka Raporty Strona główna OpRisk Administracja

Pomiar ryzyka >> Ankieta OpRisk >>

Powrót >>

[ANKIETA RYZYKA OPERACYJNEGO \(PRACOWNIK\), data pomiaru: 2008-08-31](#)

W ANKIECIE POZOSTAŁY NIWYPELNIONE POLA

- Częstotliwość  
 - Poważność

Tabele ocen >>

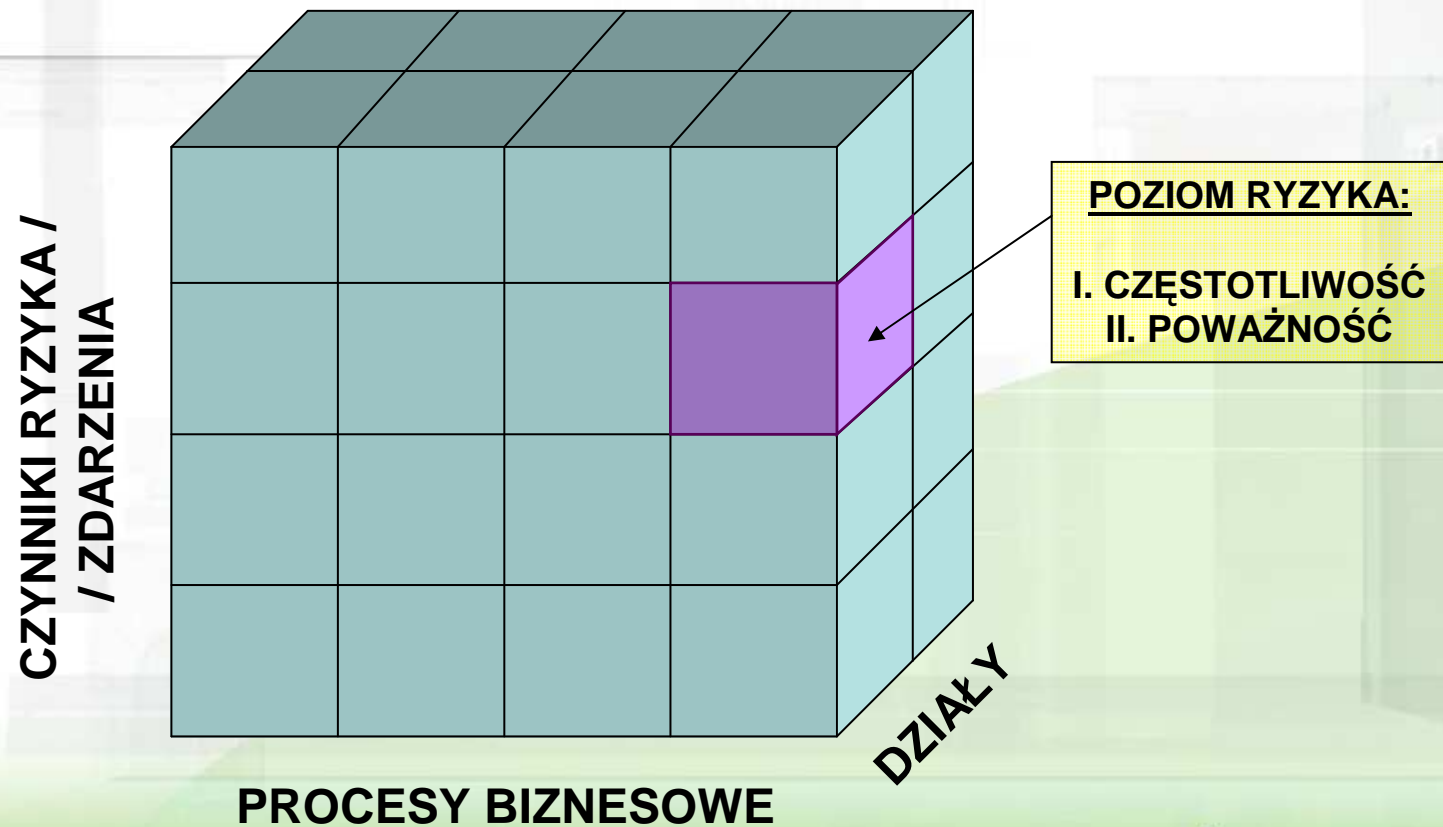
Procesy biznesowe >>

	2.1	3.1	3.2	4.1	6.1	6.3	6.4	7.3	8.1	
Czynniki w procesach										Czynniki w procesach
Czynniki w procesach										Czynniki w procesach

Zaufane witryny

# Ryzyko operacyjne w instytucji średniej wielkości

## SAMOCENA RYZYKA – - OGÓLNY MODEL (KDPW)



# Ryzyko operacyjne w instytucji średniej wielkości

## SKALA DLA OCENY CZĘSTOTLIWOŚCI I POWAŻNOŚCI RYZYKA (KDPW)

Wartość	Częstotliwość	Poważność
0	Czynnik wykluczony	
1	co 25 lat i rzadziej	znikome znaczenie
2	co 5 – 25 lat	ocena pośrednia
3	co 2 - 5 lat	mało poważne
4	co 2 lata – co pół roku	ocena pośrednia
5	co pół roku – co kwartał	średnio poważne
6	co kwartał – co miesiąc	ocena pośrednia
7	co miesiąc – co 2 tygodnie	ocena pośrednia
8	co 1 – 2 tygodnie	bardzo poważne
9	co tydzień – co 2 dni	ocena pośrednia
10	co 2 dni i częściej	skrajnie poważne

## SAMOOCENA RYZYKA – PROBLEMY

- Uznaniowa ocena ryzyka ma charakter wysoce **subiektywny**. Eksperti najczęściej przeszacowują część ryzyk, część zaś niedoszacowują (iluzja pewności).
- Istnieje zagrożenie, iż oceny ryzyka będą **nierzetelne** bądź nawet świadomie **zmanipulowane**.

## SAMOCENA RYZYKA - SUGESTIE

- Z uwagi na **heterogeniczny** charakter ryzyka operacyjnego, system samooceny ryzyka musi opierać się na **ekspertach** z wielu dziedzin (finanse, prawo, informatyka, etc.).
- Model oceny ryzyka musi być **zrozumiały** dla użytkowników i powinien charakteryzować się ograniczonym poziomem szczegółowości.

# Ryzyko operacyjne w instytucji średniej wielkości

## SAMOOCENA RYZYKA – SUGESTIE c.d.

- Dobrze jest **zautomatyzować** proces zbierania ocen (prosta aplikacja intranetowa bądź przynajmniej wystandardyzowane arkusze kalkulacyjne).
- Analiza **dynamiki** ryzyka znacznie bardziej pożyteczna niż opieranie się na oszacowanej wysokości ryzyka.

## SAMOOCENY RYZYKA - KORZYŚCI

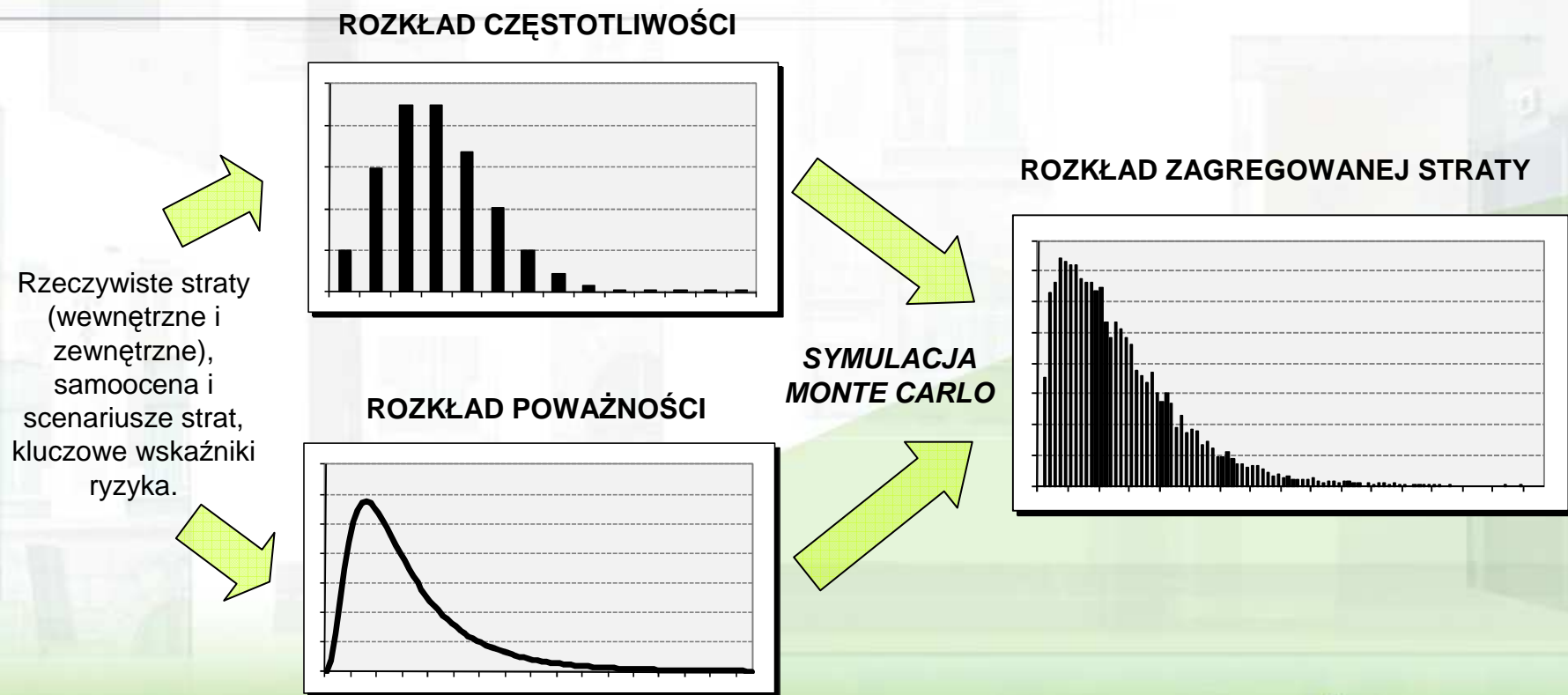
- Możliwość oceny ryzyka wystąpienia incydentów charakteryzujących się **niską częstotliwością i wysoką poważnością**, co trudno uzyskać jest poprzez kalkulację kluczowych wskaźników ryzyka bądź analizę rzeczywistych zdarzeń.
- Wzrost **świadomości ryzyka** wśród pracowników organizacji, co może wspierać naturalne mechanizmy kontroli wewnętrznej.

## POMIAR RYZYKA - WYNIKI

- Modelowanie **rozkładu** zagregowanych strat i wyznaczenie miary **VaR** (wartość narażona na ryzyko).
- Podsumowanie wyników pomiaru na **mapach** ryzyka.
- Metody **opisowe** wzbogacone o proste statystyki.

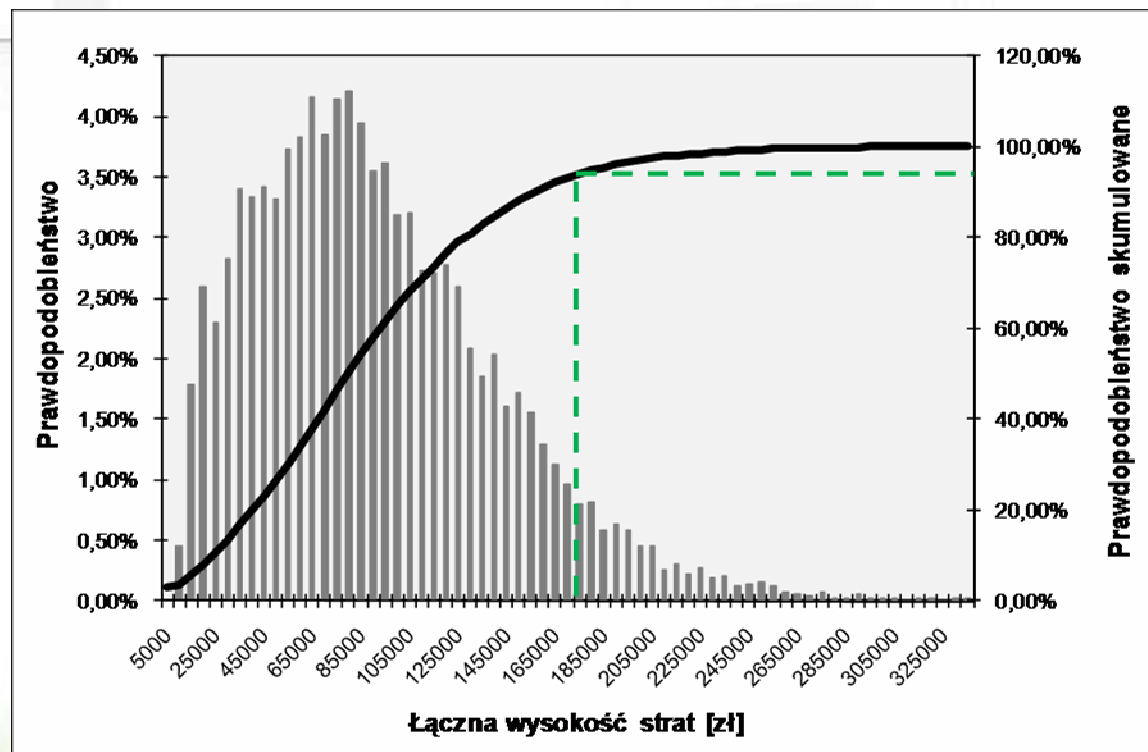
# Ryzyko operacyjne w instytucji średniej wielkości

## MODELOWANIE ROZKŁADU ZAGREGOWANYCH STRAT



# Ryzyko operacyjne w instytucji średniej wielkości

## ROZKŁAD ZAGREGOWANYCH STRAT I JEGO DYSTRYBUANTA



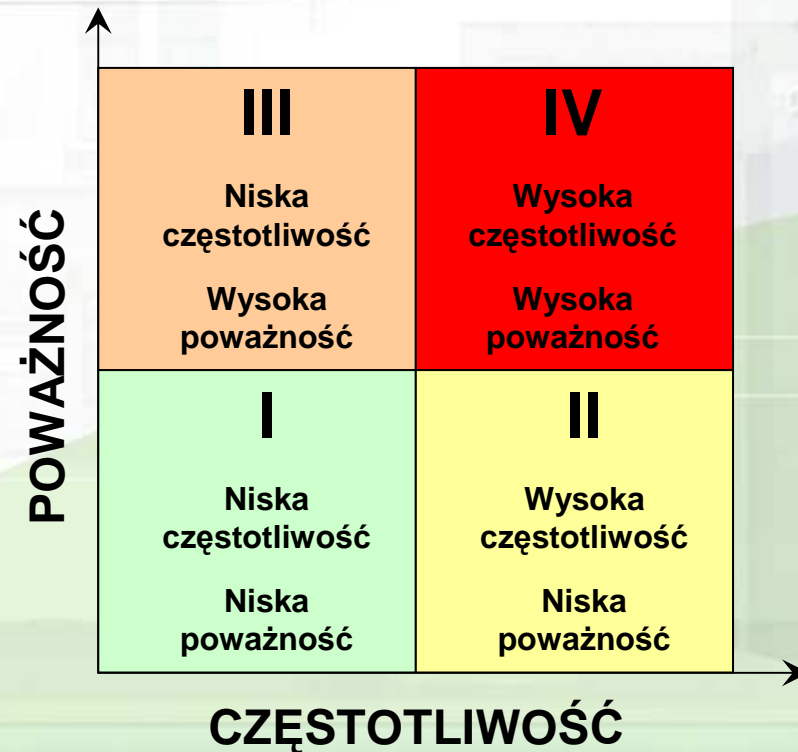
# Ryzyko operacyjne w instytucji średniej wielkości

## MAPY RYZYKA OPERACYJNEGO (KDPW)

### MACIERZ / TABELA RYZYKA

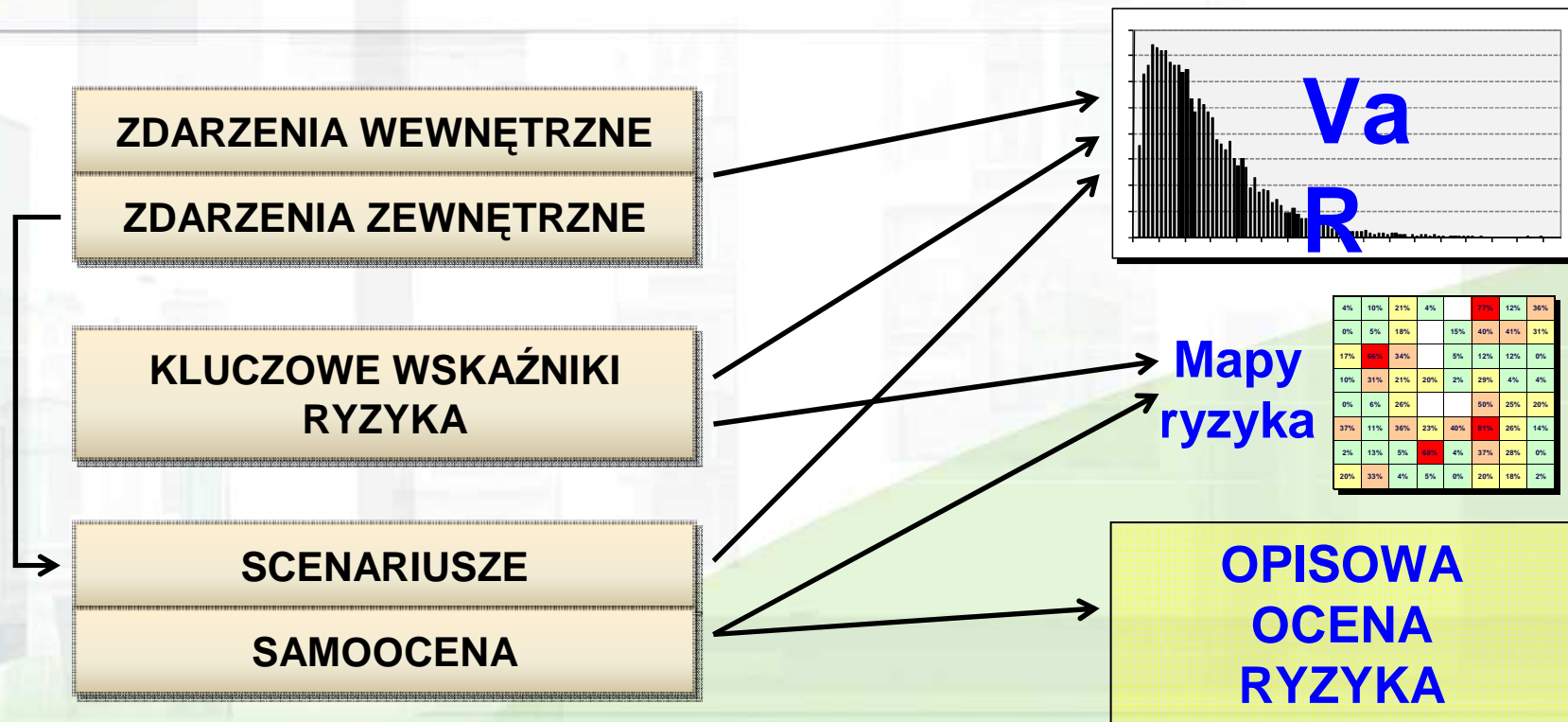
CZYNNIKI RYZYKA / ZDARZENIA	4%	10%	21%	4%		77%	12%	36%
	0%	5%	18%		15%	40%	41%	31%
	17%	66%	34%		5%	12%	12%	0%
	10%	31%	21%	20%	2%	29%	4%	4%
	0%	6%	26%			50%	25%	20%
	37%	11%	36%	23%	40%	81%	26%	14%
	2%	13%	5%	68%	4%	37%	28%	0%
	20%	33%	4%	5%	0%	20%	18%	2%
	PROCESY BIZNESOWE							

### MAPA RYZYKA



# Ryzyko operacyjne w instytucji średniej wielkości

## POMIAR RYZYKA - - ŹRÓDŁA I WYNIKI



## RAPORTOWANIE

- Dostarczenie kierownictwu **przekrojowej analizy** szeregu potencjalnych zagrożeń w całej organizacji, pozwalającej na identyfikację słabych punktów i określenie na tej podstawie priorytetowych działań w zakresie kontrolowania ryzyka (spojrzenie z „lotu ptaka”).
- Unikanie **przesadnej złożoności** (podejście „*pojedynczej strony*”).

## RAPORTOWANIE c.d.

- Należy skupić uwagę na zjawiskach **odbiegających od normy**, unikając powtarzania w kolejnych raportach tych samych stwierdzeń.
- Raporty muszą być **czytelne i zrozumiałe** nie tylko dla specjalistów zaangażowanych w rozwijanie metod pomiaru ryzyka operacyjnego w danej instytucji.

# Ryzyko operacyjne w instytucji średniej wielkości

## SYSTEM ZARZĄDZANIA RYZYKIEM OPERACYJNYM – SUGESTIE c.d.

- **Nigdy nie zaczynamy** budowy systemu zarządzania ryzykiem operacyjnym **od zera**. Określony system już istnieje, tylko nie jest uporządkowany i najprawdopodobniej brak w nim elementów formalnego pomiaru.
- Wdrożony system nigdy nie przestaje się **rozwijać** i powinien podlegać ciągłym **udoskonaleniom**. System może wystartować w bardzo prostej wersji.

# Ryzyko operacyjne w instytucji średniej wielkości

## SYSTEM ZARZĄDZANIA RYZYKIEM OPERACYJNYM – SUGESTIE c.d. [2]

- Konieczny jest skuteczny **dialog** osób odpowiedzialnych za system **z zarządem firmy**.
- System powinien zawierać elementy zapewniające stały monitoring pozwalający na **niezwłoczną reakcję** w określonych sytuacjach.
- System powinien **ewoluować** wraz ze **zmianami** zachodzącymi w firmie. Proces wprowadzania zmian powinien zaś **respektować profil ryzyka**.

# Ryzyko operacyjne w instytucji średniej wielkości

## SYSTEM ZARZĄDZANIA RYZYKIEM OPERACYJNYM – SUGESTIE c.d. [3]

- Przyjęte rozwiązania w zakresie pomiaru ryzyka powinny stanowić **optymalną mieszankę** metod opartych na **subiektywnej** samoocenie oraz **obiektywnej** kalkulacji (kluczowe wskaźniki ryzyka, modelowanie rozkładu strat).
- Ponieważ **każdy pracownik de facto zarządza ryzykiem operacyjnym**, fundamentalne znaczenie posiada budowanie kultury korporacyjnej opartej o **świadomość ryzyka**.

# Ryzyko operacyjne w instytucji średniej wielkości

## SYSTEM ZARZĄDZANIA RYZYKIEM OPERACYJNYM – SUGESTIE c.d. [4]

- Zarządzanie ryzykiem operacyjnym to złożony proces, który w dużej mierze musi pozostać **rozproszony** nawet w mniejszej organizacji. **Centralizacji** podlegać może wyłącznie **pomiar i analiza** ryzyka.
- **Synergę** w zarządzaniu ryzykiem operacyjnym zapewni **efektywna harmonizacja** różnych elementów składających się na system.

# Ryzyko operacyjne w instytucji średniej wielkości

## NA STYKU RÓŻNYCH RODZAJÓW RYZYKA

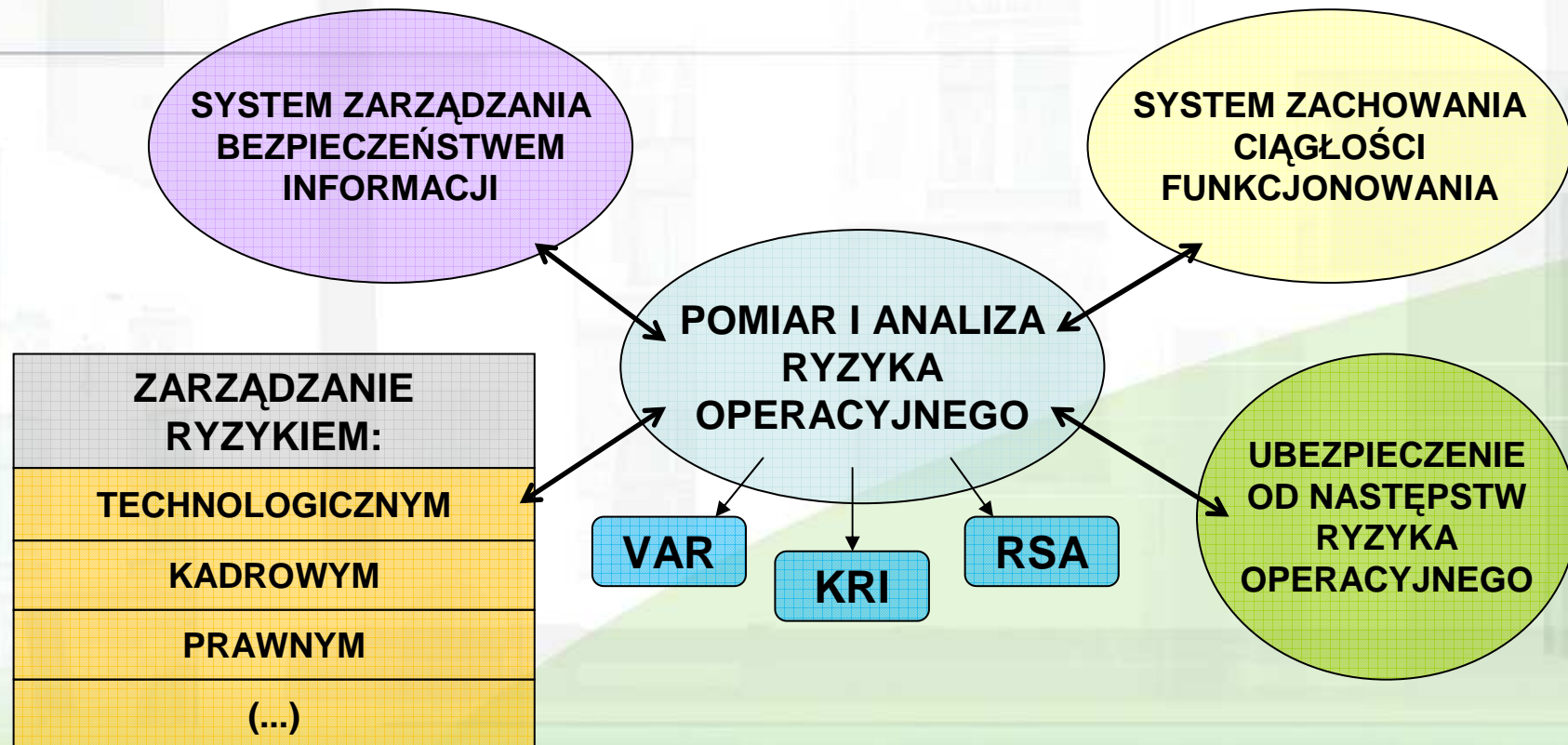
- Często występują **interakcje** między incydentami zaklasyfikowanymi do różnych rodzajów ryzyka (w szczególności **rynkowego, kredytowego i operacyjnego**).
- W przypadku **sporów o przynależność** danego incydentu istnieje obawa, że zostanie odrzucony przez wszystkich odpowiedzialnych za poszczególne rodzaje ryzyka i ostatecznie **sprawa zostanie zignorowana**.

# Ryzyko operacyjne w instytucji średniej wielkości NA STYKU RÓŻNYCH RODZAJÓW RYZYKA c.d.

- W instytucji, która **nie alokuje kapitału** w oparciu o metody zgodne z **AMA**, analiza w ramach zarządzania ryzykiem operacyjnym incydentu przynależnego raczej do **innego rodzaju ryzyka**, **nie stanowi** szczególnego **błędu** w sztuce.
- Za idealne rozwiązanie można by uznać prawdziwie **zintegrowany** system zarządzania **wszystkimi rodzajami ryzyka**. Z drugiej strony integracja różnych kategorii ryzyka operacyjnego już stanowi duże wyzwanie.

# Ryzyko operacyjne w instytucji średniej wielkości

## KOMPLEKSOWY SYSTEM ZARZĄDZANIA RYZYKIEM OPERACYJNYM



# Ryzyko operacyjne w instytucji średniej wielkości

## System Zarządzania Bezpieczeństwem Informacji (1)

- Informacja jest znaczącym aktywem KDPW S.A.
- Jakość pracy KDPW S.A. zależy w dużej mierze od ciągłej dostępności określonych informacji
- Utrata dostępności, integralności oraz poufności informacji może spowodować straty finansowe, konsekwencje prawne, a tym samym wpłynąć na wizerunek spółki
- Bezpieczeństwo informacji w KDPW S.A. ma podstawowe znaczenie dla utrzymania zgodności działań operacyjnych z właściwymi przepisami prawa oraz regulacjami wewnętrznymi
- Ryzyko technologiczne i bezpieczeństwo informacji to różne sprawy

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zarządzania Bezpieczeństwem Informacji (2)

- SZBI stanowi uzupełnienie systemu zarządzania ryzykiem operacyjnym w KDPW S.A.
- Polityka Bezpieczeństwa Informacji w KDPW S.A. to zespół dokumentów:
  - systematyzujący kwestie związane z bezpieczeństwem informacji w KDPW S.A.;
  - określający model tworzenia i zarządzania skutecznym SZBI w KDPW S.A. obejmującego obszary bezpieczeństwa teleinformatycznego, osobowego, prawnego oraz fizycznego;
  - wspierający osiągnięcie zgodności ze standardami oraz dobrymi praktykami, w szczególności ISO 2700x.

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zarządzania Bezpieczeństwem Informacji (3)

- Zasady PBI mają zastosowanie w stosunku do:
  - wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie,
  - wszystkich informacji w postaci dokumentów papierowych i elektronicznych, administrowanych przez KDPW S.A.,
  - wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są i/lub będą informacje podlegające ochronie,
  - wszystkich urządzeń przetwarzania informacji i nośników informacji, zawierających informacje podlegające ochronie,
  - wszystkich lokalizacji – budynków i pomieszczeń, w których są przetwarzane informacje podlegające ochronie.

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zarządzania Bezpieczeństwem Informacji (4)

### ■ Podejście procesowe

Zarządzanie SZBI w KDPW S.A. polega na „podejściu procesowym” do zagadnień bezpieczeństwa informacji zgodnie z modelem „Planuj – Wykonuj - Sprawdzaj - Działaj”, określającym korelacje pomiędzy procesami:

- zrozumienia wymagań bezpieczeństwa informacji oraz ustanowienia zasad i celów bezpieczeństwa informacji;
- wdrożenia i eksploatacji zabezpieczeń w celu zarządzania ryzykiem bezpieczeństwa informacji w kontekście całkowitego ryzyka biznesowego organizacji;
- monitorowania i przeglądu wydajności oraz skuteczności SZBI;
- ciągłego doskonalenia w oparciu o obiektywny pomiar.

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zarządzania Bezpieczeństwem Informacji (5)

- Dokumenty dot. bezpieczeństwa informacji w KDPW S.A. to m.in.:
  - Polityka Bezpieczeństwa Informacji;
  - Polityka Bezpieczeństwa Systemów Informatycznych;
  - Polityka Bezpieczeństwa Danych Osobowych;
  - Polityka Audytów Bezpieczeństwa Informacji;
  - Zasady i procedury dotyczące przetwarzania danych;
  - Regulacje dotyczące bezpieczeństwa fizycznego;
  - Statut Spółki oraz regulacje wewnętrzne z zakresu przedmiotu działalności (np. ponad 20 regulaminów);
  - oraz 26 regulacji zewnętrznych (ustawy, rozporządzenia).

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zarządzania Bezpieczeństwem Informacji (6)

- W KDPW S.A. zidentyfikowano 47 grup informacji chronionych.

Grupa informacji → Procesy biznesowe (ludzie, zasoby)

→ Proces macierzysty

→ Właściciel informacji

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zarządzania Bezpieczeństwem Informacji (7)

- Ocena ryzyka utraty atrybutów bezpieczeństwa (PID) dla informacji chronionych w KDPW S.A.:
  - 4-wymiarowa przestrzeń ryzyka (grupy informacji x atrybuty PID x procesy biznesowe x jednostki organizacyjne);
  - pomiary wg metody analogicznej do pomiarów poziomemu ryzyka operacyjnego;
  - pełna korelacja danych z Modelem Zarządzania Ryzykiem Operacyjnym;
  - pomiary 1 raz w roku, oraz przy znaczących zmianach;
  - wyniki w postaci map ryzyka analogicznych do map ryzyka operacyjnego;
  - wyniki uwzględniane w pomiarach ryzyka operacyjnego w kategorii ryzyka **Bezpieczeństwo danych i informacji**.

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zarządzania Bezpieczeństwem Informacji (8)

- CISO - Biuro Bezpieczeństwa
- Dział IT - ISM
- Szkolenia pracowników
- Portal edukacyjny PBI

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zachowania Ciągłości Funkcjonowania (1)

- W KDPW S.A. funkcjonuje System Zachowania Ciągłości Funkcjonowania mający na celu kompleksowe zarządzanie ciągłością działania poprzez przeciwdziałanie przerwom w działalności biznesowej oraz ochronę krytycznych procesów biznesowych przed skutkami rozległych awarii lub katastrof.

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zachowania Ciągłości Funkcjonowania (2)

- Świadomość potrzeby wśród kierownictwa i wszystkich pracowników
- To nie tylko sprawa działu IT – podejście procesowe
- Zbyt rozbudowany plan ciągłości działania nigdy nie zostanie przeczytany i w praktyce zastosowany
- Nie należy zajmować się niezliczoną ilością scenariuszy
- Uwzględnianie na bieżąco zmian zachodzących w organizacji

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zachowania Ciągłości Funkcjonowania (3)

### ZAŁOŻENIA OGÓLNE SZCF

- Przypadki zastosowania
- Procesy
- Czas odtworzenia działalności w Lokalizacji Zapasowej
- Czas przywrócenia działalności w siedzibie KDPW S.A.

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zachowania Ciągłości Funkcjonowania (4)

### DOKUMENTACJA SZCF

- Dokument Główny
- Procedury operacyjne jednostek organizacyjnych/procesów
- Plan Odtworzeniowy
- Procedury odtworzeniowe jednostek organizacyjnych/procesów

# Ryzyko operacyjne w instytucji średniej wielkości

## System Zachowania Ciągłości Funkcjonowania (5)

### ELEMENTY SZCF

- Sztab Antykryzysowy
- Lokalizacja Zapasowa
- Zespół Odtworzeniowy
- Grupa Operacyjna
- Procedury operacyjne
- Procedury odtworzeniowe jednostek organizacyjnych/  
procesów

# Ryzyko operacyjne w instytucji średniej wielkości

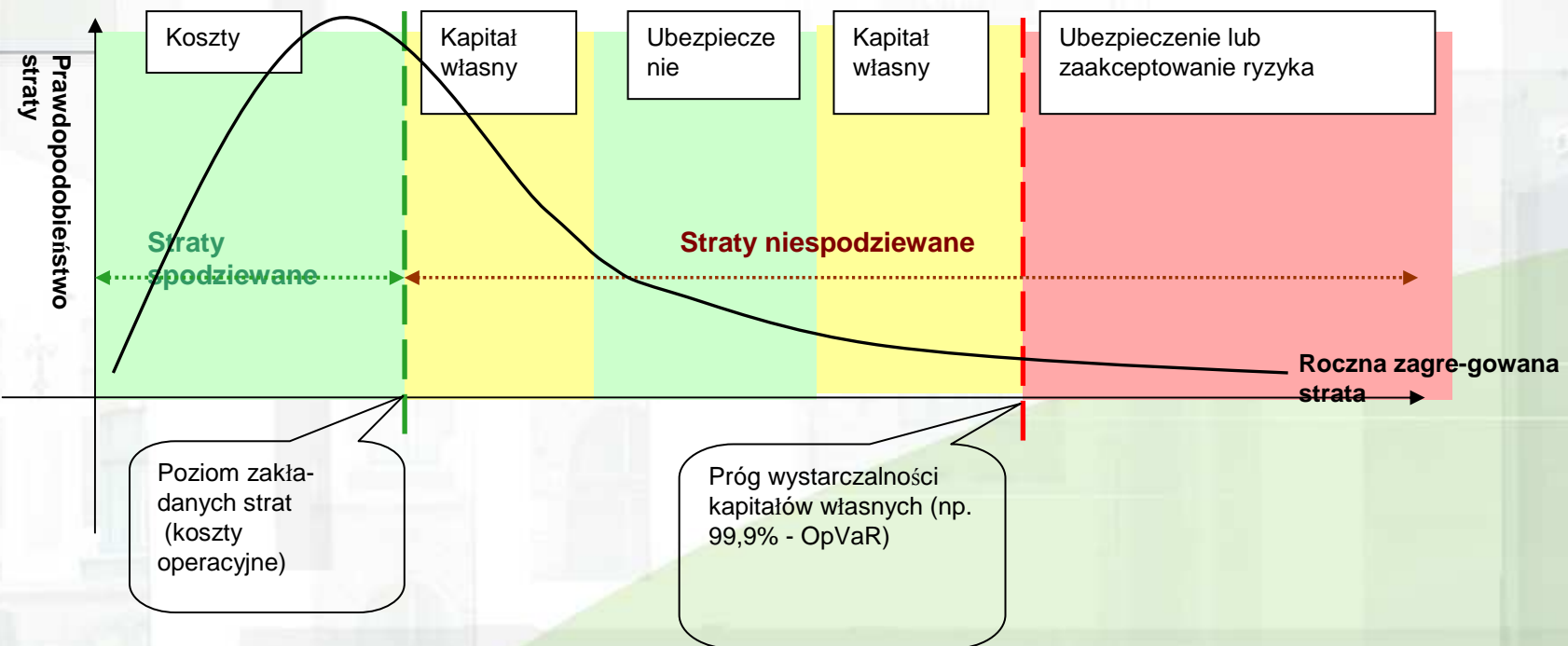
## System Zachowania Ciągłości Funkcjonowania (6)

### TESTY SYTUACJI KRYZYSOWYCH

- Testy zewnętrzne
- Testy wewnętrzne

# Ryzyko operacyjne w instytucji średniej wielkości

## Ubezpieczenie od ryzyka operacyjnego (1)



# Ryzyko operacyjne w instytucji średniej wielkości

## Ubezpieczenie od ryzyka operacyjnego (2)

- **Polisa BBB** - Nieuprawnione transakcje – tj. wszelkie transakcje dokonane przez pracowników KDPW S.A. środkami (instrumentami finansowymi, w tym papierami wartościowymi, i pieniędzmi) znajdującymi się na rachunkach KDPW S.A. oraz na rachunkach innych podmiotów, które to rachunki KDPW S.A. prowadzi lub, do których posiada dostęp (na podstawie stosownych pełnomocnictw) w związku z prowadzoną działalnością, o ile w wyniku takich transakcji doszło do utraty tych środków.
- **Polisa CC** - Biorąc pod uwagę specyfikę działania KDPW S.A., szczególnie z powodu wysokiego stopnia realizacji usług za pomocą systemu informatycznego, zasadnym uznano rozszerzenie zakresu ubezpieczenia o ryzyka związane z przestępstwami komputerowymi.

# Ryzyko operacyjne w instytucji średniej wielkości

## Ubezpieczenie od ryzyka operacyjnego (3)

- **Polisa PI** - Roszczenia cywilnoprawne osób trzecich – tj. roszczenia o zapłatę odszkodowania za szkody poniesione przez osoby trzecie w związku z działaniami KDPW S.A., w szczególności roszczenia kontrahentów KDPW S.A. związane ze szkodami, jakie ci kontrahenci ponieśli (w tym utracone korzyści) w wyniku niewykonania bądź nienależytego wykonania przez KDPW S.A. swoich obowiązków.

### Inne ubezpieczenia:

- Pełne ubezpieczenie majątkowe
- Ubezpieczenie OC (deliktowe).

## SZANSE DLA INSTYTUCJI ŚREDNIEJ WIELKOŚCI

- **Uniknięcie kosztów** budowy modeli alokacji kapitału zgodnych z AMA (I filar Bazylea II / CRD - zaawansowane metody pomiaru).
- Skupienie się na **optymalizacji procesów**, czyli faktycznym zarządzaniu ryzykiem, nie zaś na matematyce aktuarialnej (według krytyków Bazylei II / CRD **zbyt duży nacisk** kładziony jest na wyliczanie minimalnego **wymogu kapitałowego**).

# Ryzyko operacyjne w instytucji średniej wielkości

## SZANSE DLA INSTYTUCJI ŚREDNIEJ WIELKOŚCI c.d.

- Łatwiejsza **harmonizacja** różnych elementów szeroko pojętego systemu zarządzania ryzykiem operacyjnym.
- **Uniknięcie pułapek** związanych z negatywnym wpływem wdrażanych rozwiązań na **efektywność działania** instytucji.
- Łatwiejsze wdrożenie kultury korporacyjnej opartej o **świadomość ryzyka**.

# Ryzyko operacyjne w instytucji średniej wielkości

***DZIĘKUJEMY ZA UWAGĘ***

**ANDRZEJ BAJSZCZAK**

Dyrektor Biura Bezpieczeństwa

KDPW S.A.

tel. +48 22 KDPW 447

[andrzej.bajszczak@kdpw.pl](mailto:andrzej.bajszczak@kdpw.pl)

**RAFAŁ RUDZKI**

Biuro Bezpieczeństwa

KDPW S.A.

tel. +48 22 KDPW 476

[rafal.rudzki@kdpw.pl](mailto:rafal.rudzki@kdpw.pl)