Deloitte.

PIU
Polska Izba Ubezpieczeń

Ocena zarządzania ryzykiem i rola audytu wewnętrznego w świetle nowych wymogów wypłacalności – Solvency II

Seminarium Polskiej Izby Ubezpieczeń
6 grudnia 2011

Agenda

Ocena systemu zarządzania ryzykiem i kontroli wewnętrznej przez audyt wewnętrzny

1. Zintegrowany system zarządzania ryzykiem
2. Właściwy podział ról i odpowiedzialności
3. Organizacja procesu zarządzania ryzykiem operacyjnym w kontekście wymogów ORSA
4. Wymagania oraz oczekiwania wobec audytu wewnętrznego w kontekście ORSA
5. Koncepcja funkcji zgodności zintegrowanej z ryzykiem – Metodyka Deloitte
6. Przełożenie wyników zadań audytowych na całościową ocenę systemu zarządzania ryzykiem i kontroli wewnętrznej

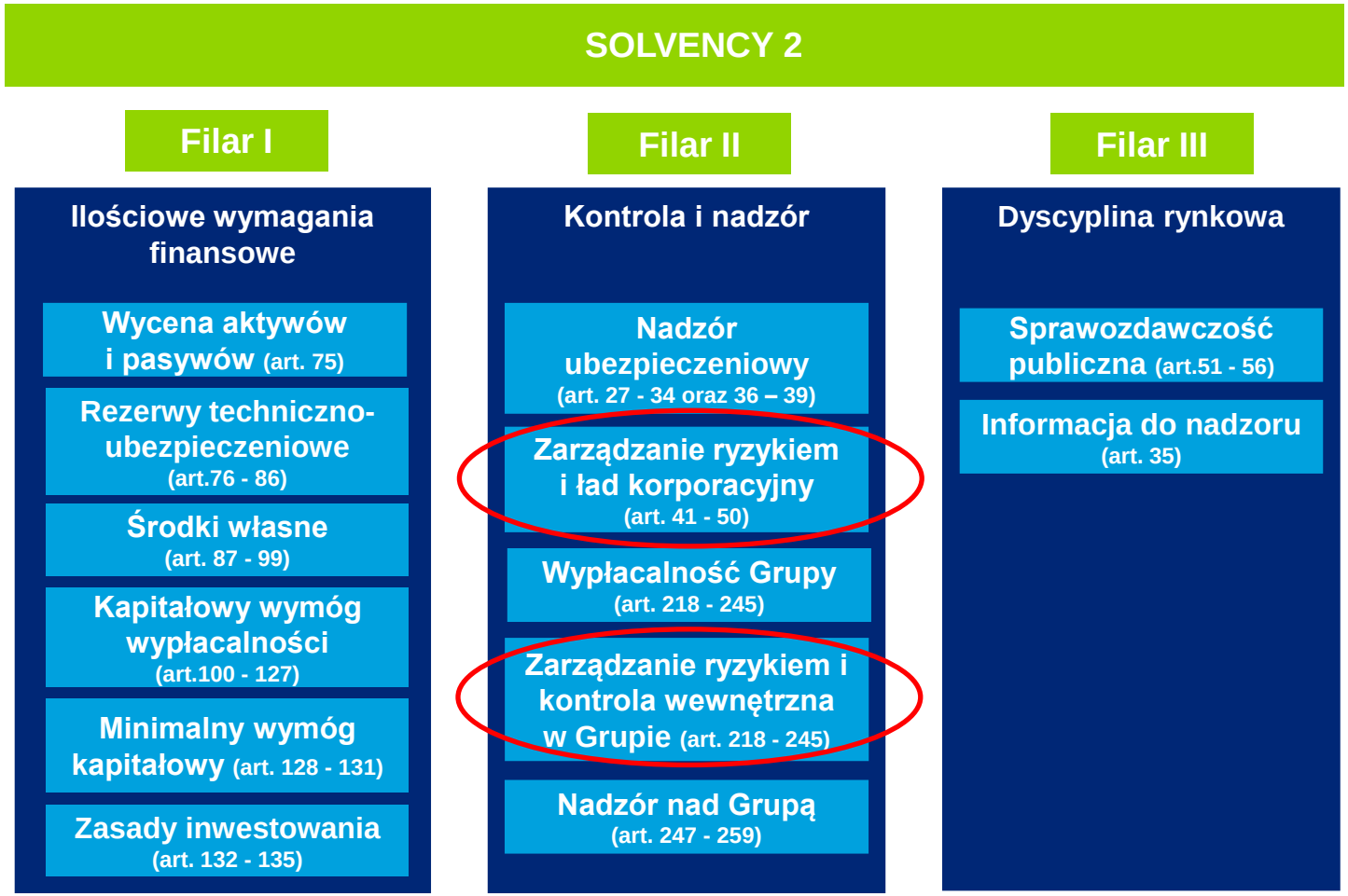
Solvency II i rola audytu wewnętrznego

1. Umiejscowienie i rola audytu wewnętrznego w ramach systemu zarządzania zakładem ubezpieczeniowym
2. Wymogi regulacyjne wobec audytu wewnętrznego
3. Dobre praktyki – oczekiwania wobec audytu wewnętrznego
4. Nowe zadania audytu wewnętrznego
5. Koncepcja audytu wewnętrznego zintegrowanego z ryzykiem – Metodyka Deloitte

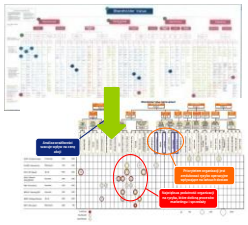
Ocena systemu zarządzania ryzykiem i kontroli wewnętrznej przez audyt wewnętrzny

Zintegrowany system zarządzania ryzykiem

Trzy filary wymogów

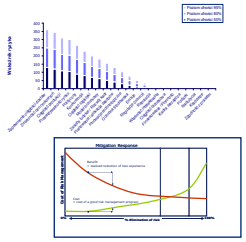


Zintegrowany system zarządzania ryzykiem (ORSA)



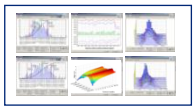
- Cele strategiczne
- Cele operacyjne
- Cele finansowe (KPI)
- Czynniki wartości
- Projekty strategiczne
- Skłonność do ryzyka
- Tolerancja ryzyka
- Środowisko (kultura, struktura, kompetencje, wartości)

- Bieżący monitoring
- Raportowanie trendów
- Eskalacja
- Ocena / optymalizacja



- Świadomość
- Szkolenia
- Komunikacja o ryzykach

- Analiza procesów
- Benchmarking
- Analiza strat
- Analiza incydentów
- Analiza czynników
- Scenariusze / zdarzenia
- Współzależności
- Korelacje
- Definiowanie scenariuszy
- Kategoryzacja zdarzeń



- Ocena wpływu
- Ocena podatności i prawdopodobieństwa
- Nadanie priorytetów
- Wybór ryzyk kluczowych

Ryzyka nie uwzględnione w filarze 1

Unikanie
- Zaniechanie działań
- Sprzedaż aktywów
- Ograniczenie skali

Minimalizacja
- Zmiana organizacji
- Zmiana procesu
- Monitor. i kontrola

Transfer
- Ubezpieczenie
- Joint venture/alians
- Outsourcing

Akceptacja
- Celowe podejmowanie
- Pełna akceptacja
- Plany awaryjne

Identyfikacja i ocena/pomiar powinna obejmować wszystkie ryzyka związane z działalnością w szczególności :

- Ryzyko strategiczne,
- Ryzyko utraty reputacji.

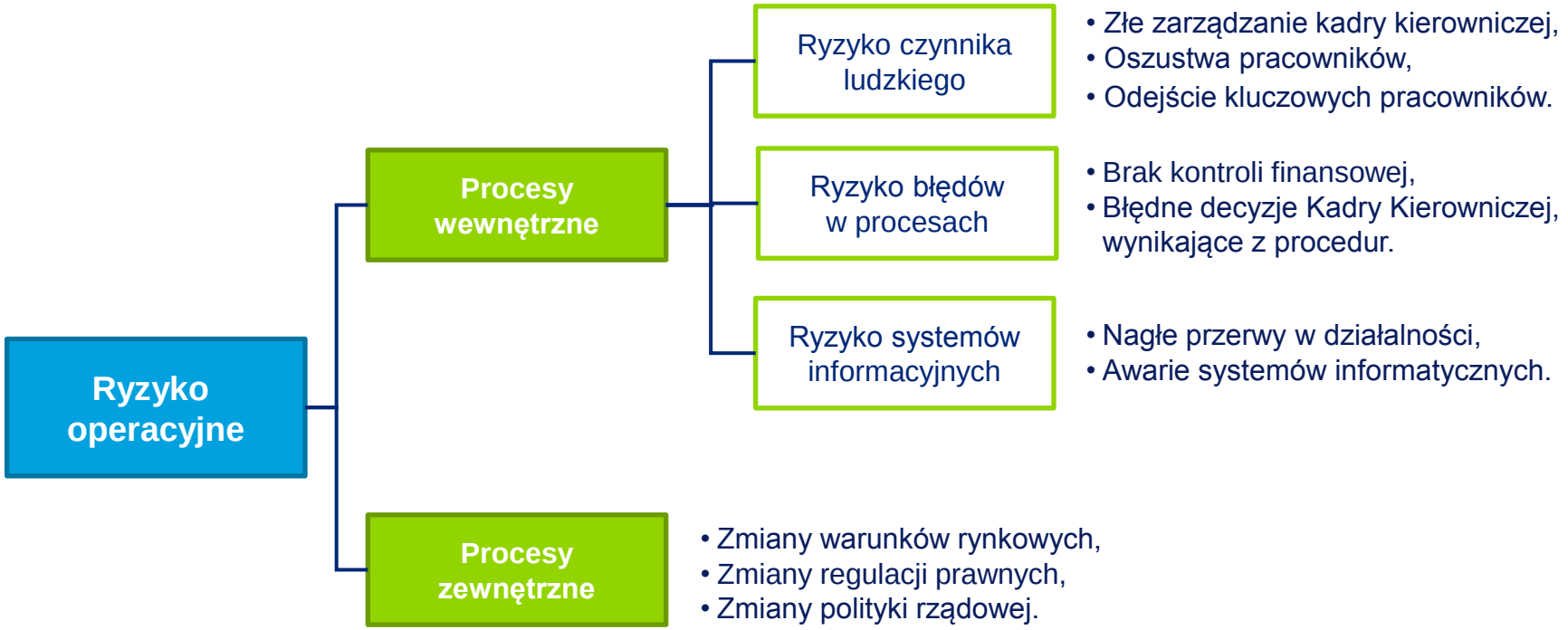
Wsparcie IT w procesie ORSA

Zarządzanie ryzykiem operacyjnym

Solvency II

Art. 44, pkt. 2d:
System zarządzania ryzykiem obejmuje co najmniej następujące obszary:
e) zarządzanie ryzykiem operacyjnym

Ryzyko operacyjne to ryzyko straty wynikającej z niewłaściwych lub zawodnych procesów wewnętrznych, ludzi i systemów lub też ze zdarzeń zewnętrznych. Definicja ta obejmuje także ryzyko prawne, lecz nie obejmuje ryzyka strategicznego i ryzyka reputacji.



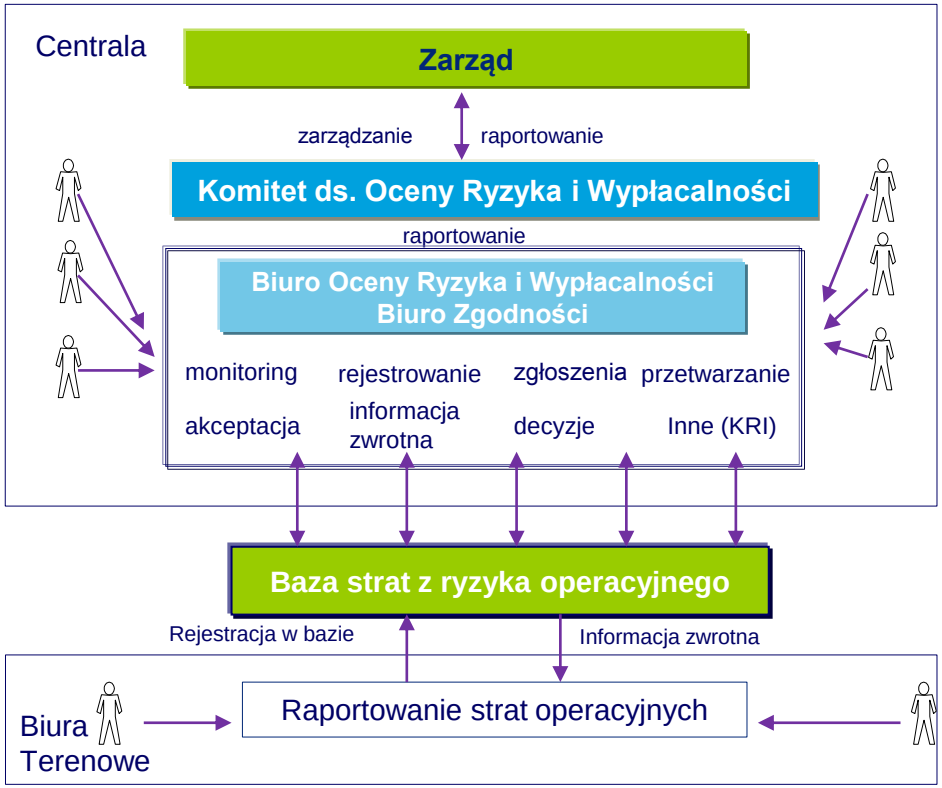
Ocena systemu zarządzania ryzykiem i kontroli wewnętrznej przez audyt wewnętrzny

Właściwy podział ról i odpowiedzialności

Umiejscowienie procesu zarządzania ryzykiem operacyjnym w strukturze organizacyjnej

Solvency II

Art. 44, pkt. 1 oraz 4:
„Zakłady ubezpieczeń i zakłady reasekuracji wprowadzają efektywny system zarządzania ryzykiem obejmujący strategie, procesy i procedury sprawozdawcze konieczne do określenia, pomiaru i monitorowania ryzyk (…)”
„Zakłady ubezpieczeń i zakłady reasekuracji ustanawiają funkcję zarządzania ryzykiem, która jest tak zorganizowana, aby ułatwić wdrożenie systemu zarządzania ryzykiem.”



Zadania jednostki odpowiedzialnej za zarządzanie ryzykiem w obszarze ryzyka operacyjnego:

- Gromadzenie informacji o zdarzenia i stratach operacyjnych
- Przeprowadzanie zintegrowanej oceny ryzyka operacyjnego (R&CSA)
- Monitoring KRI (Key Risk Indicators)
- Monitorowanie działań ograniczających ryzyko
- Opracowanie metodyki pomiaru ryzyka
- Kwantyfikacja ryzyka operacyjnego
- Rozwój metod i narzędzi zarządzania ryzykiem operacyjnym
- Opracowywania okresowych raportów i analiza dla Zarządu i Rady Nadzorczej

Rola Zarządu oraz Rady Nadzorczej

Zarząd lub odpowiedni organ administracyjny jest w pełni odpowiedzialny za zgodność działań zakładu ubezpieczeń i reasekuracji z zasadami wprowadzanymi przez Dyrektywę Solvency II.

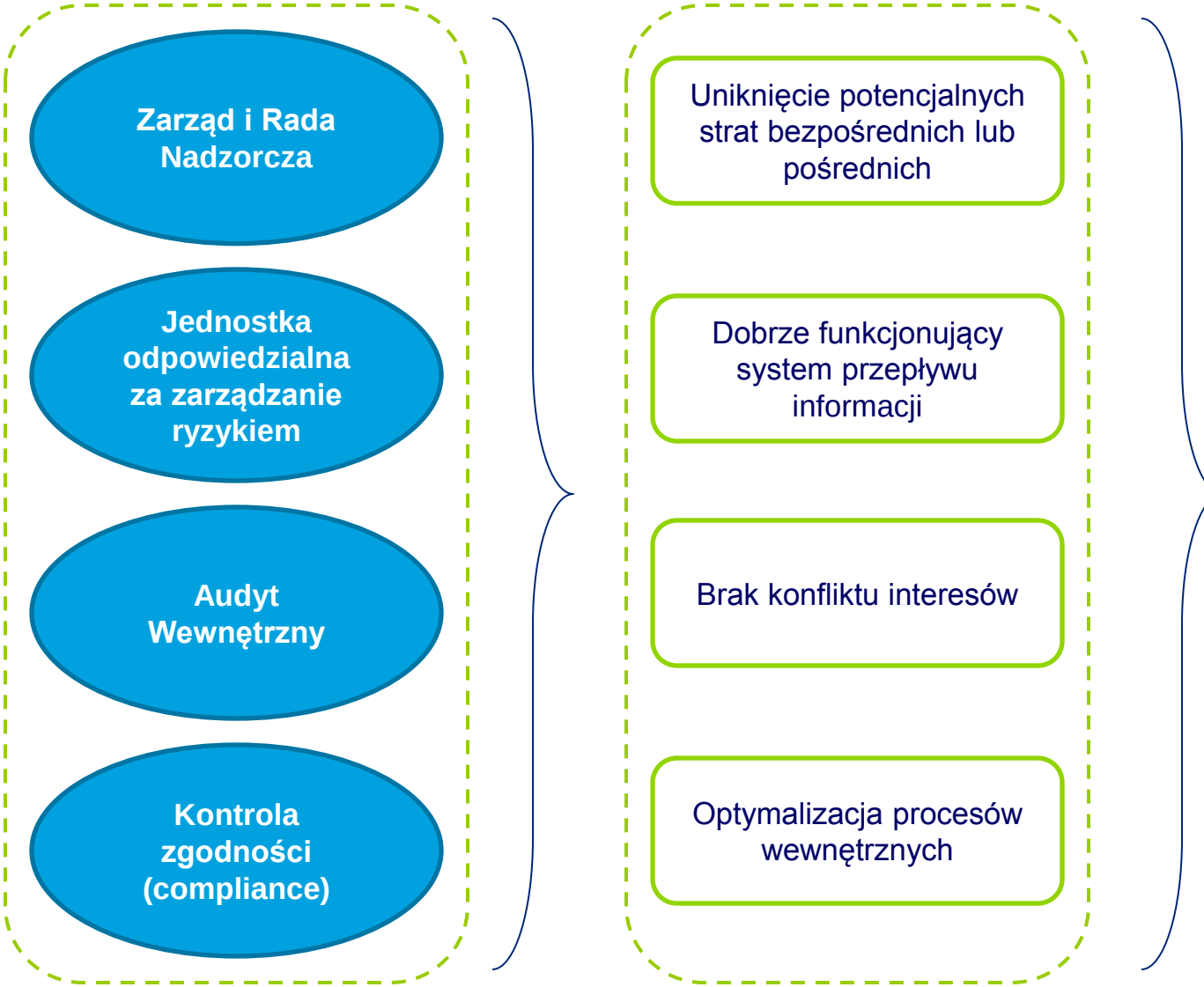
Odpowiedzialność Zarządu

1. Dokonywanie okresowych przeglądów skuteczności rozwiązań przyjętych w zakresie zarządzania ryzykiem.
2. Przekazywanie Radzie Nadzorczej informacji dot. najważniejszych rodzajów ryzyka, na jakie narażona jest Spółka oraz przyjętych mechanizmów kontrolnych.
3. Wprowadzenie polityki bezpieczeństwa i odpowiednich procedur wewnętrznych zapewniających skuteczne zarządzanie ryzykiem, w szczególności plany utrzymania ciągłości i plany awaryjne dla procesów krytycznych dla działalności Spółki.
4. Przygotowanie oraz wdrożenie strategii zarządzania ryzykiem.
5. Zapewnienie przeprowadzania efektywnego audytu wewnętrznego z ramienia niezależnego, wykwalifikowanego i kompetentnego personelu.

Odpowiedzialność Rady Nadzorczej

1. Nadzór nad spójnością procesu zarządzania ryzykiem ze strategią, działalnością i planem finansowym Spółki.
2. Analiza, czy struktura organizacyjna zapewnia efektywne zarządzanie ryzykiem.
3. Nadzór nad planowaniem i realizacją nowych projektów oraz wprowadzaniem zmian w procesach operacyjnych.
4. Akceptacja strategii zarządzania ryzykiem oraz jej regularny przegląd.
5. Nadzór nad zakresem i częstotliwością kontroli wewnętrznej oraz jej adekwatnością do poziomu narażenia Spółki na ryzyko.

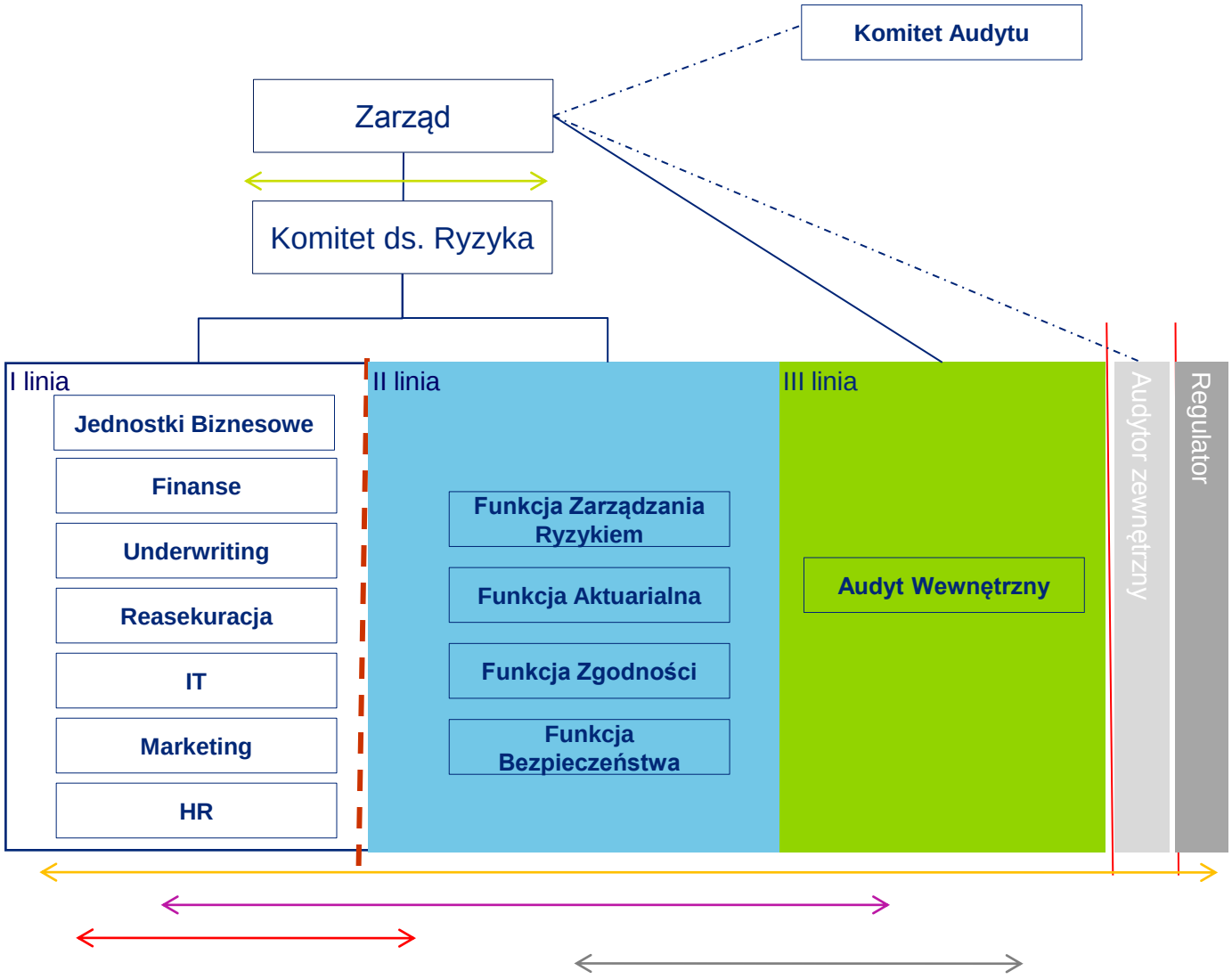
Efektywne zarządzanie ryzykiem to właściwy podział odpowiedzialności



Solvency II

Art. 44, pkt. 1:
„(…) system zarządzania ryzykiem jest skuteczny i dobrze zintegrowany ze strukturą organizacyjną i z procesami decyzyjnymi zakładu ubezpieczeń lub zakładu reasekuracji, z odpowiednim uwzględnieniem osób, które faktycznie zarządzają zakładem lub pełnią inne kluczowe funkcje."

Podział ról zgodnie z Solvency II



Etapy procesu zarządzania ryzykiem

1. Identyfikacja ryzyka

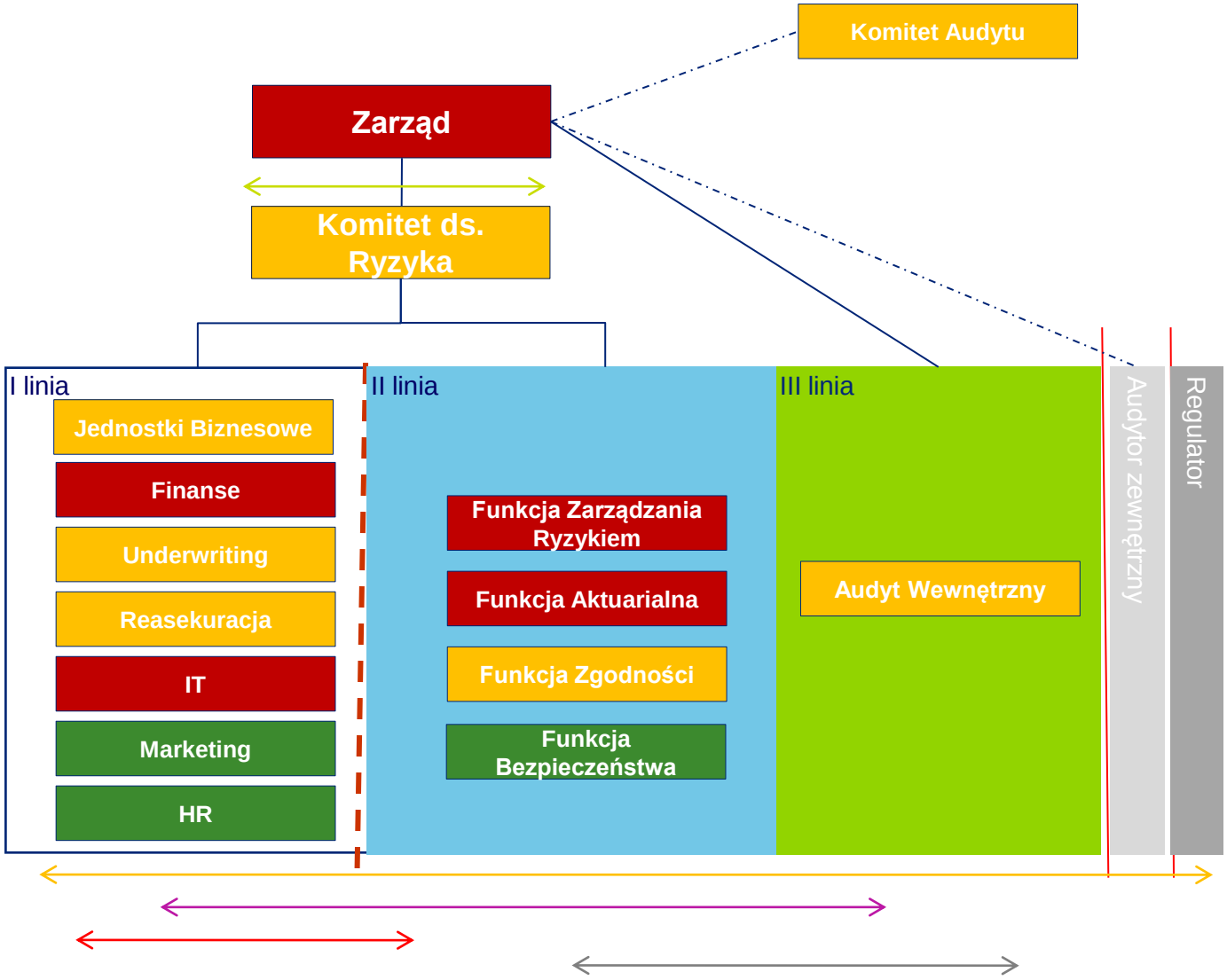
2. Analiza i ocena ryzyka

3. Ustalenie progu akceptowalności ryzyka

4. Postępowanie z ryzykiem

5. Monitorowanie procesu i dokonywanie zmian

Podział ról zgodnie z Solvency II



Etapy procesu zarządzania ryzykiem

1. Identyfikacja ryzyka

2. Analiza i ocena ryzyka

3. Ustalenie progu akceptowalności ryzyka

4. Postępowanie z ryzykiem

5. Monitorowanie procesu i dokonywanie zmian

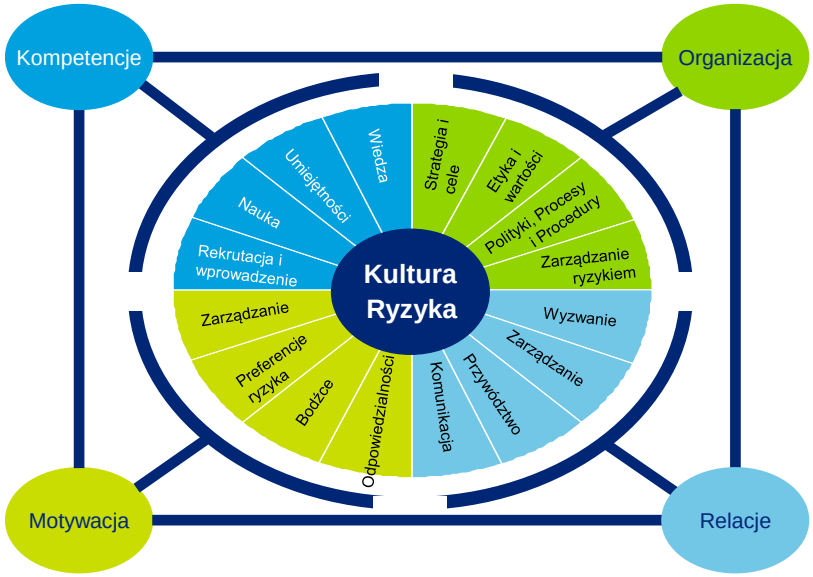
Znaczący wpływ | Średni wpływ | Niski wpływ

Podział odpowiedzialności zgodnie z Solvency II

Elementem sukcesu wdrożenia Solvency II jest również skuteczne propagowanie i zarządzanie nową kulturą ryzyka

Zespołowe zarządzanie kompetencjami odnośnie ryzyka w organizacji.

Jak zorganizowane jest zarządzanie ryzykiem i co jest uznawane za wartość?



Powody dlaczego ludzie zarządzają ryzykiem.

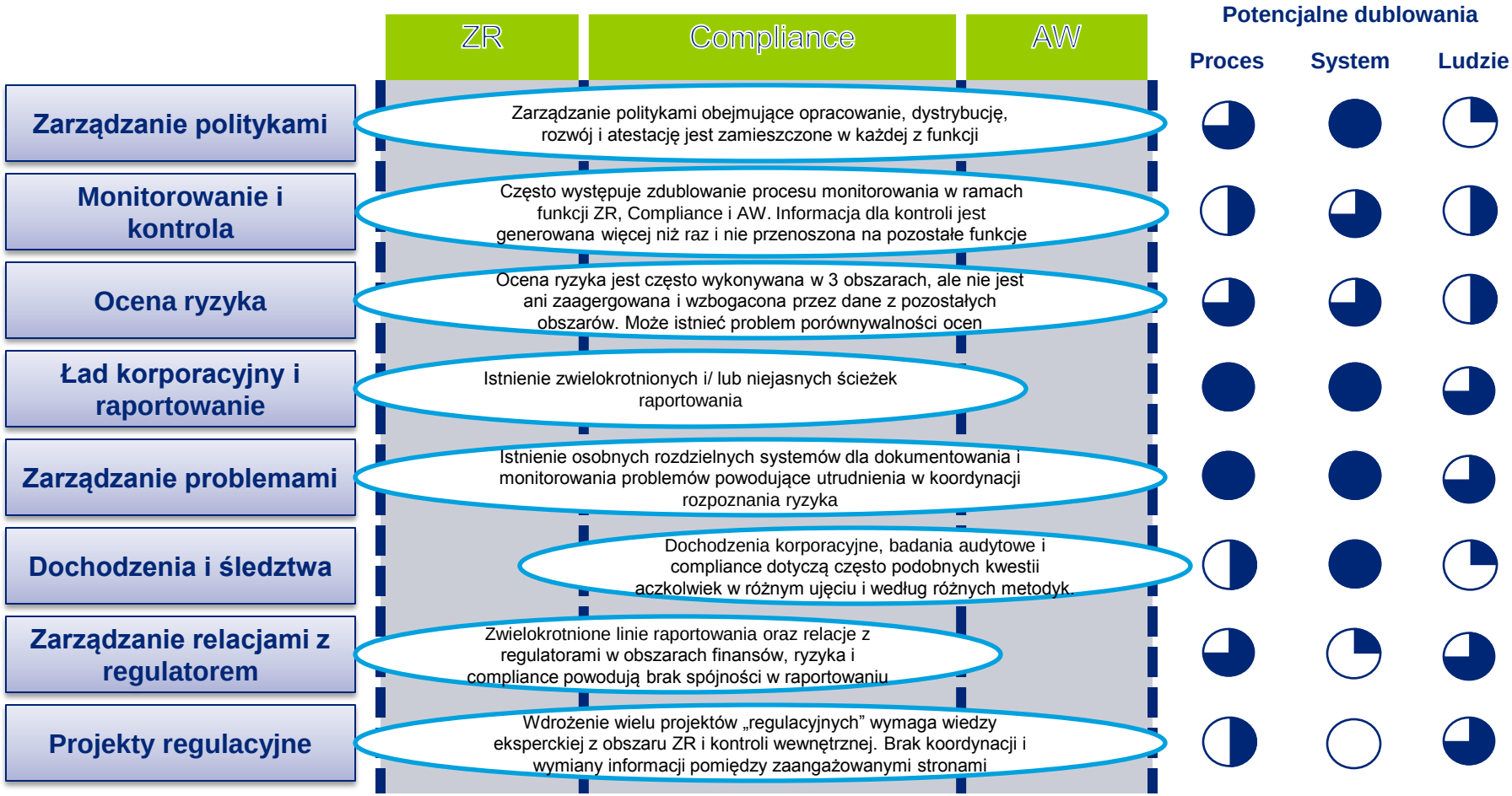
Jaki jest sposób interakcji pomiędzy ludźmi w organizacji?

- Włączenie w zintegrowany system zarządzania ryzykiem podejścia opartego na kulturze ryzyka pozwoli zrozumieć i właściwie zarządzać ludźmi bezpośrednio włączonymi w proces zarządzania ryzykiem.
- Wdrożenie Solvency II będzie się wiązało ze zmianami w ramach procesu zarządzania ryzykiem. Stąd ważne jest stworzenie właściwej wiedzy w organizacji co do wprowadzanych zmian, szczególnie w obszarach, gdzie wpływ Solvency II będzie największy.

CEIOPS
Committee of European Insurance and Occupational Pensions Supervisors

"Ważne jest, aby zakłady ubezpieczeń posiadały kulturę organizacyjną, która umożliwia i skutecznie wspiera funkcjonowanie systemu zarządzania. Wymaga to odpowiedniego „tonu " z (...) najwyższego szczebla kierownictwa zapewniającego odpowiednie wartości i priorytety organizacji". Dokument konsultacyjny CEIOPS

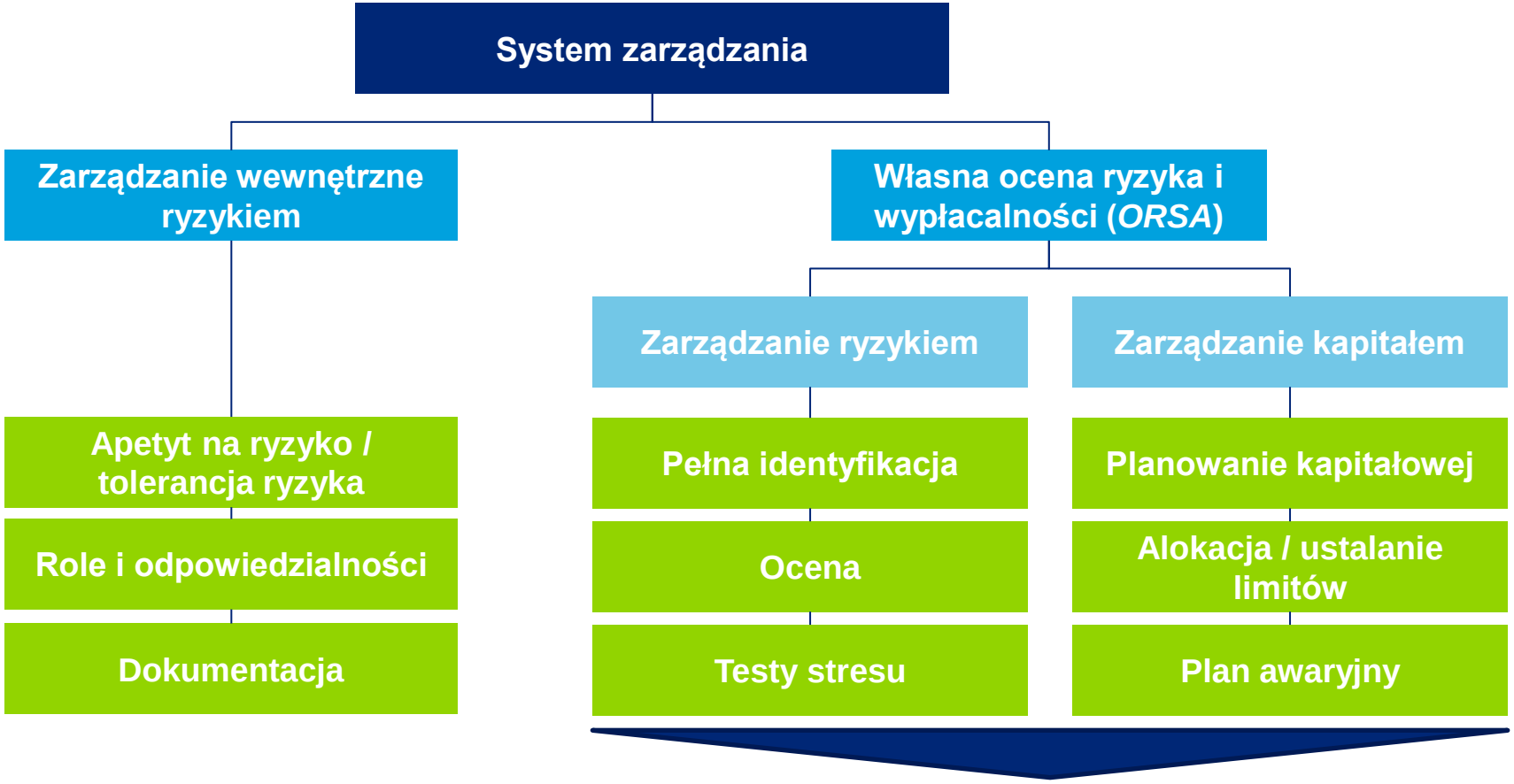
Potencjalne dysfunkcjonalności systemu governance podczas wdrożenia Solvency II



Ocena systemu zarządzania ryzykiem i kontroli wewnętrznej przez audyt wewnętrzny

Organizacja procesu zarządzania ryzykiem operacyjnym w kontekście wymogów ORSA

Definicja ORSA



Definicja ORSA

ORSA to całość procesów i procedur użytych do identyfikacji, oceny, monitoringu, zarządzania i raportowania krótko-i długoterminowych ryzyk zakładu ubezpieczeń (lub reasekuracji) oraz do określenia środków własnych potrzebnych do zapewnienia, że ogólne potrzeby z zakresu wypłacalności zakładu ubezpieczeń są spełnione w każdym momencie.

Filar II (ORSA) – główne wytyczne (1/2)

Główne wytyczne

1. **Wdrożenie ORSA jest obligatoryjne**, niezależnie od formuły rozwiązań wypracowanych w ramach wdrożenia Filaru I (formuła standardowa, model wewnętrzny).

2. **Uprawnienia organów nadzorczych**. W przypadku, kiedy organ nadzorujący wyrazi wątpliwości co do:

   a. poprawności opartych na ryzyku metod szacowania adekwatności kapitałowej,

   b. jakości wdrożonego systemu zarządzania ryzykiem (ORSA),

   będzie uprawniony do nałożenia wyższych wymogów kapitałowych w stosunku do zakładu ubezpieczeń.

3. **Ideą wymogów Filaru II (ORSA)**jest stworzenie zintegrowanego z procesami biznesowymi systemu zarządzania ryzykiem. W procesie ORSA istotna jest identyfikacja, pomiar, monitorowanie i kontrola ryzyk, które bezpośrednio dotyczą działalności danego zakładu ubezpieczeń.

4. **W skład katalogu ryzyk** wchodzą ryzyka, które zakład ubezpieczeń identyfikuje na potrzeby filaru I (ubezpieczeniowe, kredytowe, rynkowe, operacyjne), ale również ryzyka specyficzne dla jego działalności np. ryzyko płynności, utraty reputacji, ryzyko modelu, braku zgodności, jeśli zostały uznane przez zakład ubezpieczeń jako istotne.

Filar II (ORSA) – główne wytyczne (1/2)

Główne wytyczne

5. Główne wymogi **ilościowe**, jakie wprowadza ORSA to m.in.:
   - a. Opracowanie zasad ustalania apetytu i tolerancji na ryzyko w powiązaniu ze strategią biznesową zakładu ubezpieczeń,
   - b. Stworzenie metod pomiaru poszczególnych ryzyk zidentyfikowanych wSpółkach na potrzeby procesu ORSA
   - c. Opracowanie testów warunków skrajnych oraz sposobu uwzględnienia analizy scenariuszowej oraz testów warunków skrajnych w pomiarze ryzyka oraz przy ustalaniu i monitoringu limitów
   - d. Opracowanie procesu walidacji oraz weryfikacji adekwatności wykorzystywanych metod pomiaru na poziomie jakościowym i ilościowym
   - e. Opracowanie podejścia do agregacji wyników pomiaru poszczególnych ryzyk w celu określenia całkowitego poziomu ryzyka
6. Główne wymogi **jakościowe**, jakie wprowadza ORSA to m.in.:
   - a. Stworzenie strategii zarządzania ryzykiem powiązanej ze strategią biznesową oraz stworzenie właściwych pisemnych polityk i procedur zarządzania ryzykami związanymi z działalnością zakładu ubezpieczeń
   - b. Określenie właściwego podziału ról oraz zakresu odpowiedzialności Zarządu, Rady Nadzorczej, audytu wewnętrznego, kontroli wewnętrznej, zarządzającego ryzykiem, kontroli zgodności w procesie zarządzania ryzykiem
   - c. System kontroli wewnętrznej powinien być zintegrowany z systemem zarządzania ryzykiem
   - d. Wprowadzenie właściwego systemu raportowania wspierającego proces zarządzania ryzykiem

Elementy krytyczne wdrożenia wymogów ORSA w obszarze ryzyka operacyjnego

Zdefiniowanie procesu zarządzania ryzykiem operacyjnym

- Przegląd i aktualizacja wszystkich procesów i podprocesów biznesowych, w tym również zlecanych wykonawcom zewnętrznym (outsourcing). Przegląd powinien obejmować co najmniej:
  - Przebieg procesu
  - Procedury opisujące proces
  - Systemy IT
- Identyfikacja kluczowy procesów biznesowych z punktu widzenia działalności Spółki
- Przegląd mechanizmów kontrolnych dla poszczególnych procesów

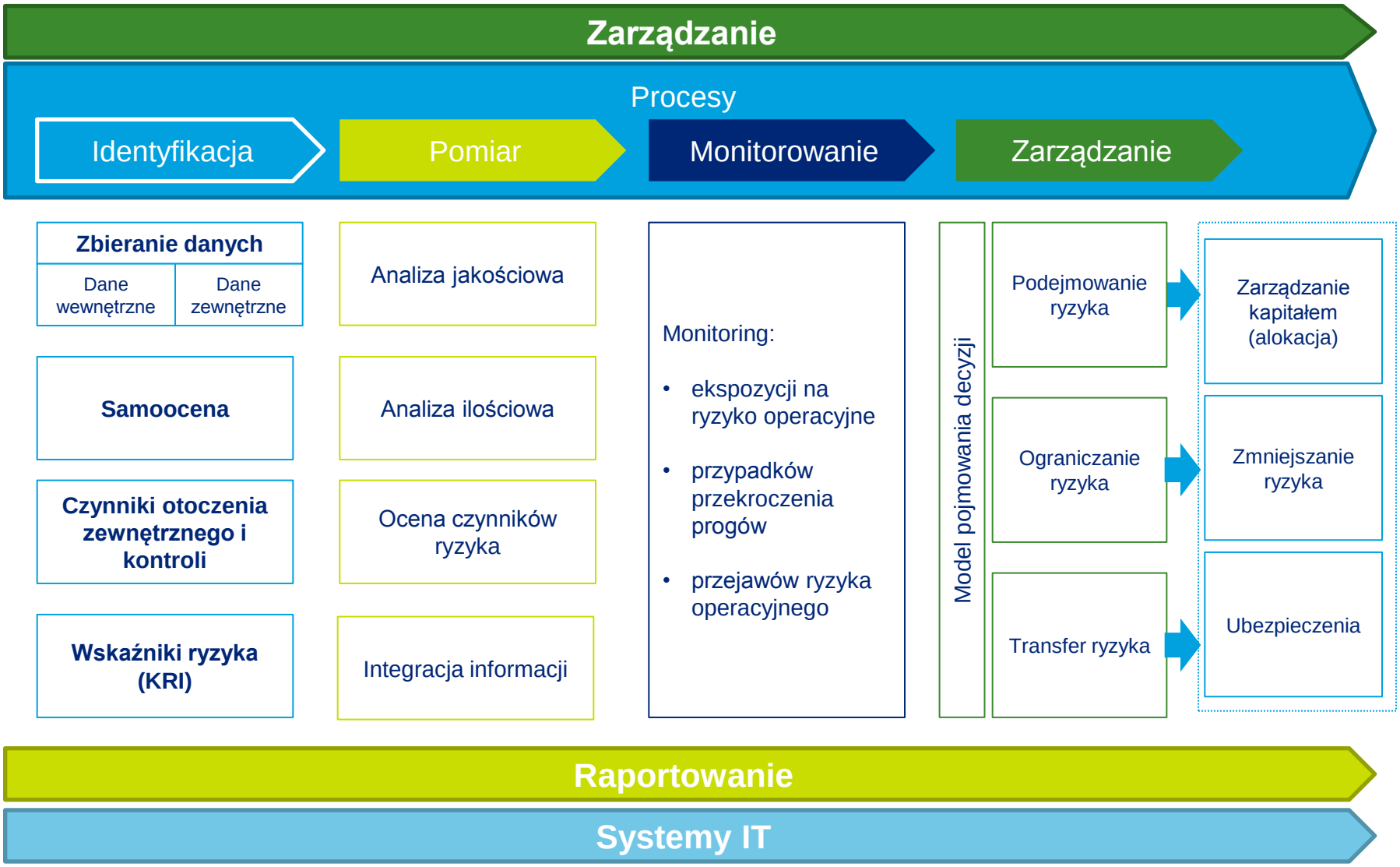
Opracowanie procedury zarządzania ryzykiem operacyjnym

- Zasady identyfikacji ryzyk operacyjnych w ramach procesów biznesowych (w wyniku samooceny przeprowadzanej przez wszystkie jednostki Spółki lub na wniosek jednostki kontrolującej ryzyko operacyjne)
- Kluczowe wskaźniki ryzyka operacyjnego (KRI) –określają w sposób ilościowy (częstotliwość wystąpienia, wielkość straty) poziom ryzyka i wrażliwość na dane ryzyko
- Limity dla wskaźników ryzyka –określają akceptowalny i ostrzegawczy poziom wskaźnika, stanowią system wczesnego ostrzegania
- Zasady procesu gromadzenia informacji o stratach operacyjnych (baza strat)
- Metody pomiaru ryzyka operacyjnego
- Raportowanie ryzyka operacyjnego
- Zasady oceny profilu ryzyka operacyjnego
- Metody zapobiegania zdarzeniom operacyjnym
- Testy warunków skrajnych dla ryzyka operacyjnego –zawierające scenariusze możliwych zdarzeń, o niskim prawdopodobieństwie zajścia, ale dużej potencjalnej stracie

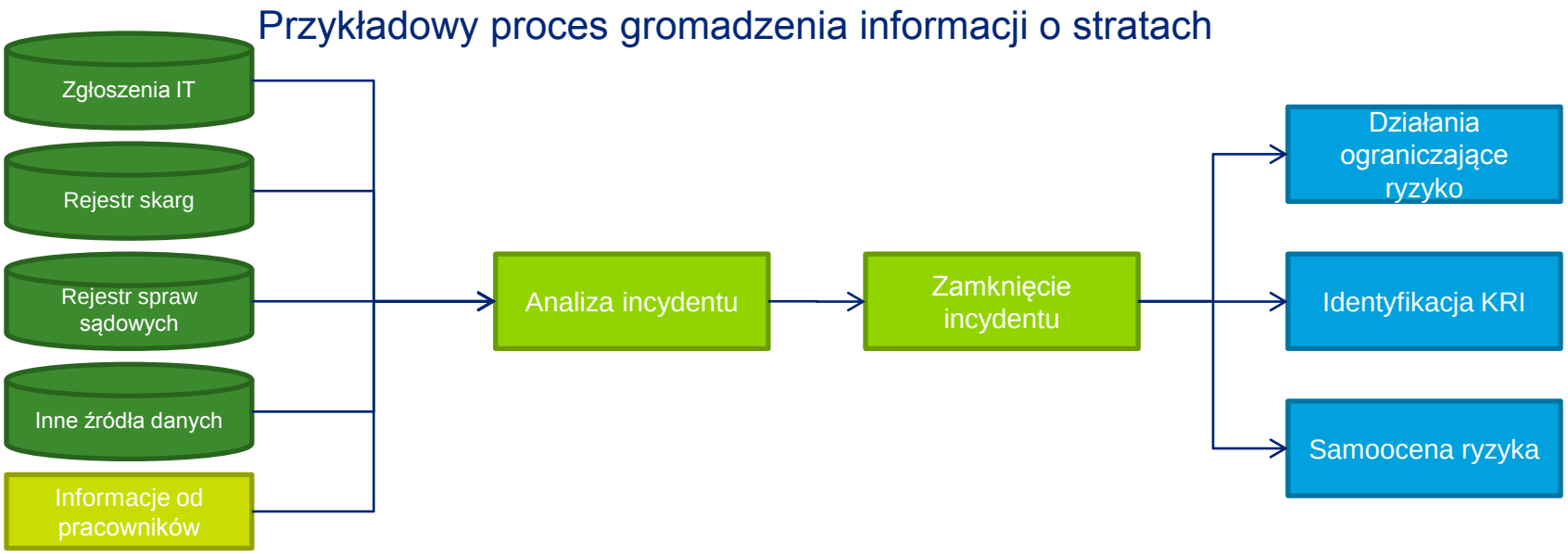
System zarządzania ryzykiem operacyjnym

System zarządzania ryzykiem operacyjnym stanowi kluczowy element systemu zarządzania ryzykiem. Efektywne zarządzanie ryzykiem operacyjnym wymaga uwzględnienia wszystkich punktów widocznych poniżej. Szczególnie istotny jest proces gromadzenia informacji o stratach oraz ich poprawna wycena zarówno w odniesieniu do strat rzeczywiście poniesionych jak i tzw. utraconych korzyści.

Jak zoptymalizować główne procesy na potrzeby sprawnego zarządzania ryzykiem operacyjnym?



Baza danych o zdarzeniach operacyjnych – propozycja wdrożenia



Kierunek przepływu informacji

Jednostka zgłaszająca zdarzenie ryzyka operacyjnego

- stwierdza powstanie nieprawidłowości
- ocenia przyczyny i skutki nieprawidłowości
- przekazuje informacje do jednostki zarządzania ryzykiem operacyjnym
- monitoruje zdarzenie
- ewidencja zdarzenia w aplikacji, rejestrującej straty operacyjne

Jednostka zarządzająca ryzykiem operacyjnym

- gromadzenie informacji w aplikacji
- weryfikacja danych w bazie zdarzeń
- raporty dla jednostek biznesowych, dla Rady Nadzorczej, Zarządu, Komitetów Ryzyka

Rada Nadzorcza, Zarząd, Komitet ryzyka

- system zarządzania ryzykiem
- działania w celu ograniczania ryzyka

Zakres gromadzonych informacji o stratach

Główne atrybuty zdarzenia, gromadzone w bazie strat

Kategoria zdarzenia operacyjnego

Rodzaj zdarzenia operacyjnego w ramach ww. kategorii ryzyka operacyjnego

Kwota brutto skutku finansowego i waluta
- niezbędna informacja dla pomiaru wielkości strat

Data zajścia zdarzenia

Rodzaj skutku finansowego (rzeczywisty, potencjalny, szacowany) - posiadanie informacji o potencjalnym rodzaju skutku finansowego jest dla instytucji finansowej krytyczny, gdyż straty potencjalne nie wpływają na wyliczenie wymogu kapitałowego

Wskazanie zdarzeń wykraczających swoim zasięgiem poza jedną linię biznesową (tak/nie), posiadanie tej informacji jest krytyczne ze względu na konieczność przyporządkowania konkretnych kwot strat finansowych do poszczególnych obszarów

Data odzysku oraz typ odzysku

Kwota odzysku i jej waluta – posiadanie tej informacji jest krytyczne, gdyż w przypadku strat szybko odwróconych (strat, których skutki finansowe zostały odzyskane w krótkim czasie od momentu zdarzenia) możliwe jest nieuwzględnianie przynajmniej części straty w pomiarze ryzyka

Zdarzenie powstałe na skutek zdarzeń rozciągniętych w czasie, lecz powiązanych ze sobą

Skutek finansowy dotyczy zaangażowania kredytowego (tak/nie) lub transakcji rynkowej (tak/nie) – informacja niezbędna dla pomiaru wielkości strat

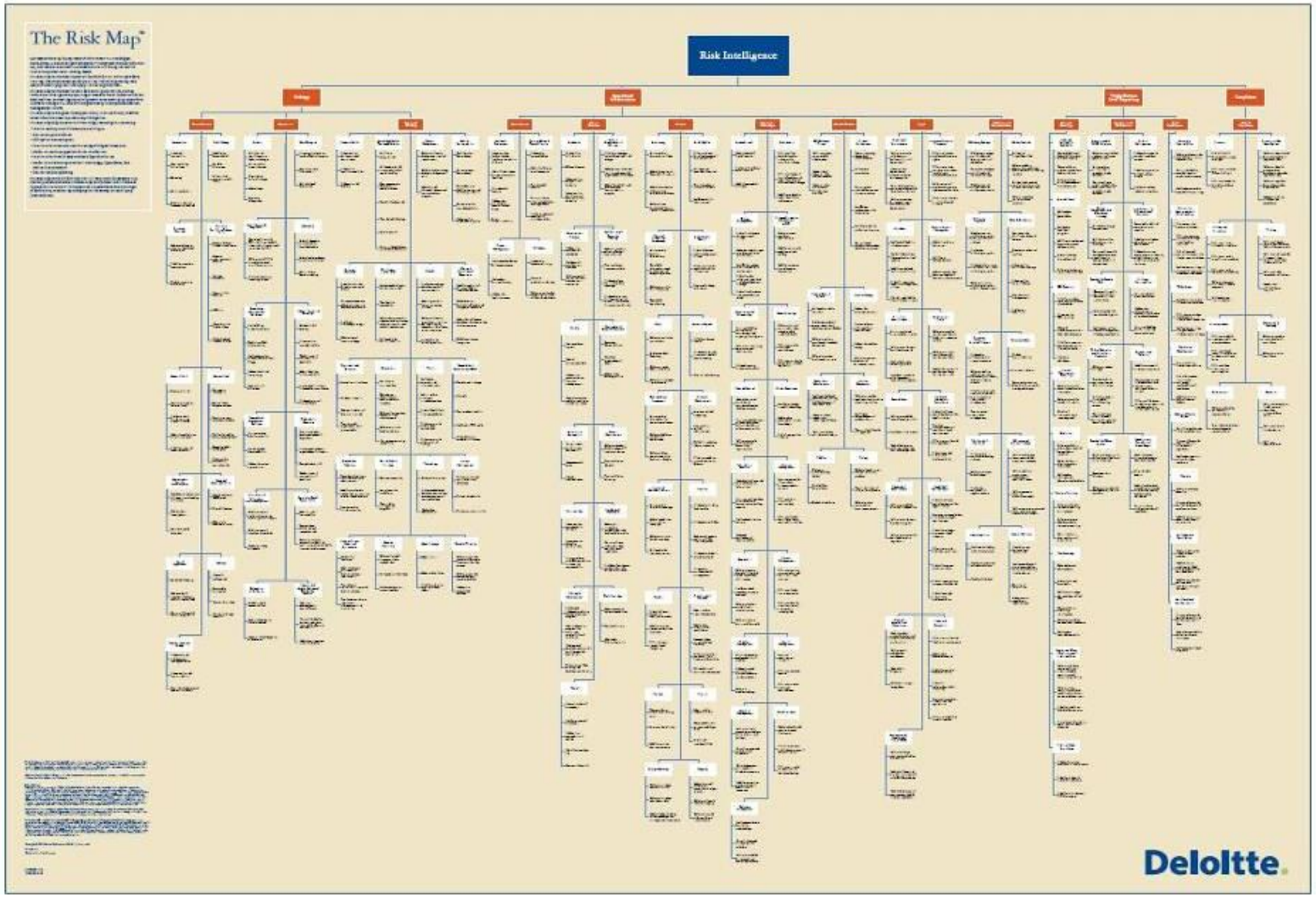
Identyfikator konta księgowego, na którym został zarejestrowany skutek finansowy zdarzenia

Powiązanie z innym zdarzeniem – informacja niezbędna do pomiaru wielkości strat

Inne (np. opis zdarzenia, przyczyna zdarzenia)

23

Risk Intelligence Map™ i zarządzanie ryzykiem operacyjnym



Proces samooceny ryzyka operacyjnego

Proces polega na:

- zidentyfikowaniu najbardziej istotnych ryzyk
- ocenie zidentyfikowanego ryzyka, najczęściej na podstawie oceny wartości i częstotliwości strat na jakie może być narażona Spółka w przypadku materializacji zidentyfikowanego ryzyka
- określaniu planów działań w celu poprawienia kontroli i zmniejszenia identyfikowanego ryzyka

Ryzyko oceniane podczas samooceny

- Ryzyko absolutne
- Ryzyko rezydualne
- Ryzyko oczekiwane

Własna ocena ryzyka i wypłacalności – Art. 45

1) W ramach systemu zarządzania ryzykiem każdy zakład ubezpieczeń i zakład reasekuracji przeprowadza własną ocenę ryzyka i wypłacalności. Ocena ta obejmuje co najmniej:
   a) ogólne potrzeby w zakresie wypłacalności przy uwzględnieniu specyficznego profilu ryzyka, zatwierdzonych limitów tolerancji ryzyka oraz strategii działalności zakładu;
   b) ciągłą zgodność z wymogami kapitałowymi określonymi w rozdziale VI sekcja 4 i 5 oraz wymogami odnoszącymi się do rezerw techniczno-ubezpieczeniowych określonymi w rozdziale VI sekcja 2;
   c) istotność, z którą profil ryzyka danego zakładu odbiega od założeń leżących u podstaw kapitałowego wymogu wypłacalności określonego w art. 101 ust. 3, obliczonego według standardowej formuły zgodnie z rozdziałem VI sekcja 4 podsekcja 2 lub według częściowego lub pełnego modelu wewnętrznego zakładu zgodnie z rozdziałem VI sekcja 4 podsekcja 3.
2) Do celów ust. 1 lit. a) zakład, którego to dotyczy, musi posiadać procesy, współmierne do charakteru, skali i złożoności ryzyk właściwych dla jego działalności, umożliwiające mu właściwe określenie i ocenę ryzyk napotykanych w perspektywie krótko i długoterminowej, na jakie jest lub może być narażony. Zakład przedstawia metody stosowane do dokonania tej oceny.
3) W przypadku, o którym mowa w ust. 1 lit. c), jeżeli stosowany jest model wewnętrzny, ocenę przeprowadza się wraz z przekalibrowaniem przekształcającym wewnętrzne dane dotyczące ryzyka na miarę ryzyka i kalibrację kapitałowego wymogu wypłacalności.
4) Własna ocena ryzyka i wypłacalności stanowi integralną część strategii działalności i jest stale uwzględniana przy podejmowaniu przez zakład strategicznych decyzji.
5) Zakłady ubezpieczeń i zakłady reasekuracji przeprowadzają ocenę, o ktorej mowa w ust. 1, regularnie i bezzwłocznie po wystąpieniu wszelkich znacznych zmian w ich profilu ryzyka.
6) Zakłady ubezpieczeń i zakłady reasekuracji informują organy nadzoru o wynikach każdej własnej oceny ryzyka i wypłacalności w ramach informacji przekazywanych na mocy art. 35.
7) Własna ocena ryzyka i wypłacalności nie służy do obliczania wymogu kapitałowego. Wymóg kapitałowy wypłacalności może być dostosowany tylko zgodnie z art. 37, 231-233 i 238.

Rola Organu Zarządzającego (podejście top down) i dokumentacja

Guideline 2 (Artykuł 45 Dyrektywy)

Zakład powinien zapewnić, że organ zarządzania zakładem bierze aktywny udział w procesie poprzez kierowanie przebiegiem oceny i kwestionowanie jej wyników.

Guideline 3 (Artykuł 45 (2) Dyrektywy)

Zakład powinien posiadać przynajmniej poniższą dokumentację na temat ORSA:

a) Politykę ORSA;

b) Rejestr każdego procesu ORSA;

c) Wewnętrzną dokumentację informacji ORSA;

d) Informacje ujawniane i przekazywane do organu nadzoru.

Guideline 4 (Artykuł 45 (2) Dyrektywy)

Polityka ORSA powinna być zgodna z ogólnymi zasadami zarządzania i dokumentacji procedur i powinna dodatkowo zawierać przynajmniej:

a) Opis procesów i procedur do przeprowadzenia ORSA;

b) Opis połączeń między profilem ryzyka, limitami tolerancji ryzyka i ogólnymi potrzebami wypłacalności;

c) Szczegóły na temat:

   i. Jak często przeprowadzać testy stresu / analizę wrażliwości oraz jakie testy i analizy mają być wykorzystane;

   ii. Założeń na podstawie których ma opierać się ocena i agregacja ryzyk;

   iii. Opis źródeł danych na których opiera się proces i kryteria i metodologię oceny jakości użytych danych;

   iv. Częstotliwość przeprowadzania (regularnego) ORSA i okoliczności, które by zainicjowały potrzebę przeprowadzenia ORSA poza regularnym cyklem.

Kluczowe wskaźniki ryzyka

Kluczowe czynniki ryzyka (Key Risk Indicators KRI) definiuje się jako zestaw parametrów procesu biznesowego, które z dużym prawdopodobieństwem odzwierciedlają zmiany profilu ryzyka operacyjnego tego procesu. Są to dane statystyczne, liczbowe, finansowe odnoszące się do określonych rodzajów ryzyka, są wyliczane oraz cyklicznie analizowane.

Przykład KRI

- Liczba skarg – wzrost liczby skarg wskazuje na duże prawdopodobieństwo wzrostu popełnianych błędów i w konsekwencji wzrostu ekspozycji na ryzyka operacyjne
- Rotacja kard
- Liczba prób włamań do systemów informatycznych Zakładu Ubezpieczeń

Główne zastosowania KRI

- **Raportowanie profilu ryzyka** dla kadry kierowniczej
- Wskazanie na konieczność działań, które pozwolą obniżyć ekspozycję na ryzyko: **„Sygnał wczesnego ostrzegania”**
- **Komunikowanie apetytu na ryzyko** poprzez ustalanie odpowiednich poziomów wartości progowych
- Pomoc w określaniu efektywności istniejących oraz dodatkowych procesów kontrolnych, które mają na celu minimalizowanie ryzyka
- Pomoc w **zwiększaniu świadomości ryzyka operacyjnego** – kreowanie kultury ryzyka operacyjnego

Rodzaje KRI

- Wyprzedzające (ex ante) – określają potencjalne straty oraz ekspozycję na ryzyko w przyszłości
- Bieżące – wymagają zwrócenia uwagi na zmniejszenie strat i ekspozycji na ryzyko
- Opóźnione (ex post) – odzwierciedlają historyczne przyczyny strat i ekspozycji na ryzyko

Jednym z elementów systemu wczesnego ostrzegania jest zaprojektowanie właściwego systemu raportowania…

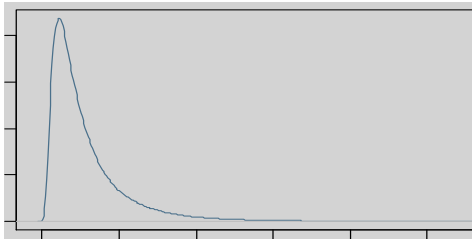
Główne ryzyka

Ryzyko	Strata (mln PLN)	Trend
Ryzyko_1		⬆
Ryzyko_2		➡
Ryzyko_3		⬇
Ryzyko_4		⬆
Ryzyko_5		⬆

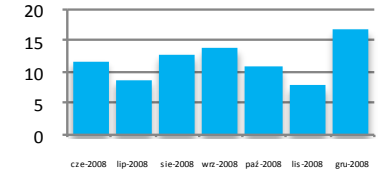
Wskaźniki Kluczowego Ryzyka

Poziom	Nazwa	Watość	Trend
🟡	KRI_1		⬆
🔴	KRI_2		➡
🟢	KRI_3		⬇
🟢	KRI_4		➡
🟡	KRI_5		⬇
🔴	KRI_6		⬆

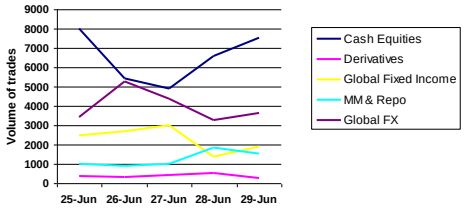
Strata nieoczekiwana



Straty finansowe

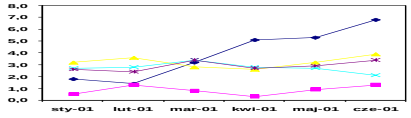


Transaction Volumes



Mapa ryzyka

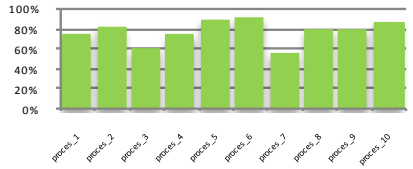
Rekomendacja



Komentarz

- wyjaśnienia do podwyższonego poziomu ryzyka.

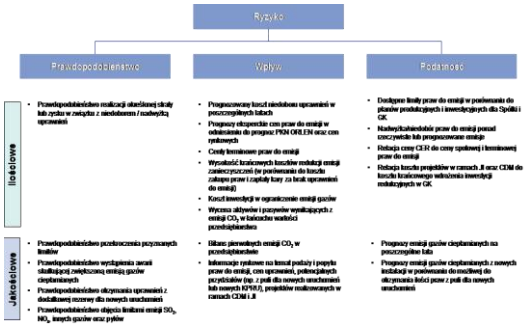
Efektywność kontroli



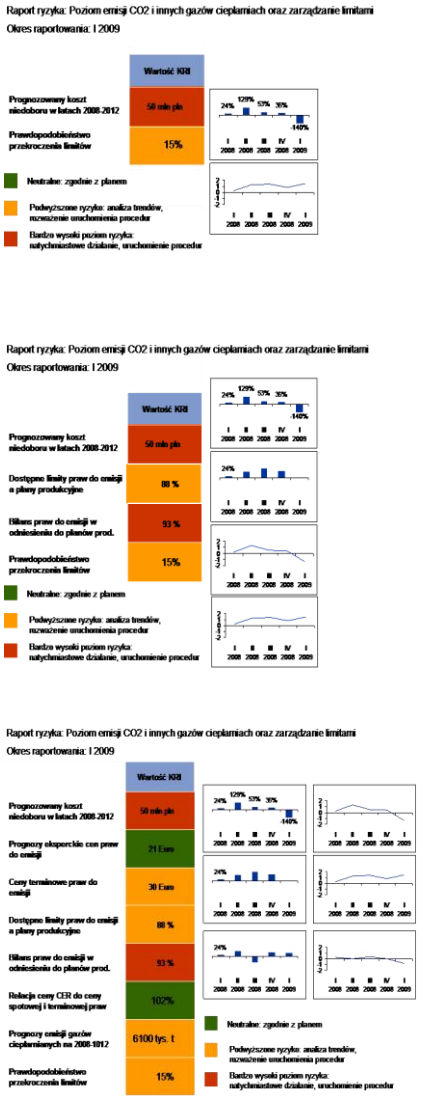
…z kolei różny poziom agregacji informacji ułatwia podejmowanie działań ograniczających ryzyko. Przykład raportowania KRI.

Pogłębiona analiza ryzyka (przyczynowo-skutkowa) pozwala na określenie wskaźników za pomocą których dokonywany będzie pomiar ekspozycji na dany rodzaj ryzyka. Wskaźniki te (KRI) mogą odnosić się do wpływu, podatności lub prawdopobieństwa. Mogą mieć charakter ilościowy lub jakościowy. Analizy ryzyka oraz kalibracja KRI dokonywana jest przez menedżerów – właścicieli ryzyka na podstawie apetytu Spółki na ryzyko przy metodologicznym wsparciu funkcji zarządzania ryzykiem.

Skala ryzyka określa przedziały neutralnego poziomu ryzyka, podwyższonego oraz krytycznego, przy którym wymagane jest natychmiastowe działanie.



Szczegółowość raportu jest dostosowana do potrzeb jego adresatów. Poziom agregacji informacji wzrasta ‘w górę’ hierarchii organizacyjnej.



Raport dla Zarządu zawiera kluczowe wskaźniki KRI oraz analizy trendu z danego obszaru ryzyka, ale uzupełniają go raporty z innych

Raport dla Dyrektora jednostki jest skróconą w zakresie tego ryzyka jest skróconą wersją, ale uzupełnia go skrócony raport z innego obszaru ryzyka / działalności operacyjnej

Raport dla Kierownika działu jest szczegółowy, zawiera wykaz wartości wielu wskaźników ryzyka oraz analizy trendów, ale ogranicza się do wąskiego zakresu działalności operacyjnej

Ocena systemu zarządzania ryzykiem i kontroli wewnętrznej przez audyt wewnętrzny

Wymagania oraz oczekiwania wobec audytu wewnętrznego w kontekście ORSA

Redefiniowanie roli Audytu Wewnętrznego wobec powstającej funkcji Zarządzania Ryzykiem oraz funkcji Zgodności

Solvency II

Art. 47, pkt 1:
„Funkcja audytu wewnętrznego obejmuje ocenę adekwatności i efektywności systemu kontroli wewnętrznej i innych elementów systemu zarządzania.”

Procesy zarządzania ryzykiem oraz systemy pomiaru tego ryzyka powinny być poddawane regularnym przeglądom przeprowadzanym przez audytorów wewnętrznych lub zewnętrznych.

Audyt wewnętrzny powinien być wykonywany przez niezależny, wykwalifikowany i kompetentny personel.

Osoby odpowiedzialne za kontrolę ryzyka operacyjnego powinny być uniezależnione od ocenianej jednostki operacyjnej, która generuje ryzyko.

1. Dokonywanie regularnej oceny zarówno zarządzania działalnością operacyjną poszczególnych jednostek, jak i weryfikowanie jakości samego procesu zarządzania ryzykiem i stosowanych mechanizmów kontroli.
2. Dostarczanie obiektywnej oceny: efektywności, adekwatności i skuteczności funkcjonującego systemu zarządzania oraz jakości przeprowadzanych operacji ubezpieczeniowych.
3. Dokonywanie okresowych przeglądów zasad ograniczania i kontroli ryzyka.
4. Analiza adekwatności systemów informatycznych wykorzystywanych w procesie zarządzania ryzykiem oraz przegląd procesów zbierania i utrzymywania danych.

Ocena systemu zarządzania ryzykiem i kontroli wewnętrznej przez audyt wewnętrzny

Koncepcja funkcji zgodności zintegrowanej z ryzykiem – metodyka Deloitte

Redefiniowanie roli funkcji Zgodności wobec powstającej funkcji Zarządzania Ryzykiem

Solvency II

Art. 46, pkt 2: „Funkcja zgodności z przepisami obejmuje doradzanie organowi administrującemu, zarządzającemu lub nadzorczemu w kwestiach zgodności z przepisami ustawowymi, wykonawczymi i administracyjnymi przyjętymi zgodnie z niniejszą dyrektywą. Obejmuje ona również ocenę możliwego wpływu wszelkich zmian otoczenia prawnego na operacje danego zakładu oraz wskazanie i ocenę ryzyka związanego z przestrzeganiem przepisów."

Obowiązki stanowiska ds. zgodności

- Monitorowanie zmian w przepisach prawa mających wpływ na działalność.
- Badanie i weryfikacja zgodności regulacji z przepisami prawa
- Opiniowanie i monitorowanie zgodności z projektem regulacji dotyczących Solvency II
- Raportowanie na poziom Zarządu i Rady Nadzorczej
- Wdrożenie procedury dot. funkcji zgodności
- Uczestnictwo we właściwych Komitetach – Audytu oraz ds. oceny ryzyka

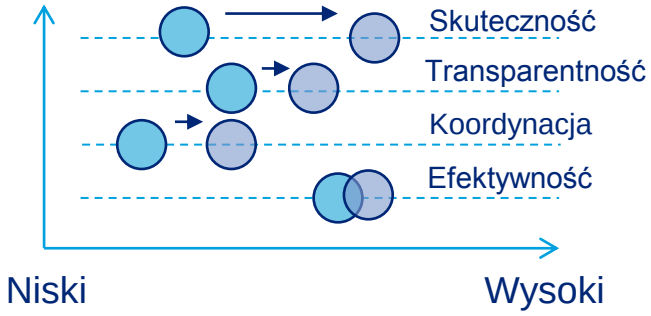
Miejsce funkcji zgodności wśród jednostek uczestniczących w procesie zarządzania ryzykiem – obszary nakładania się zadań

	Ryzyko Operacyjne	Funkcja zgodności	Audyt Wewnętrzny
Polityki i Procedury	Często przygotowanie, dystrybucja czy weryfikowanie polityk/procedur jest „zasilosowane" w poszczególnych funkcjach.		
Polityki i Procedury	Duplikacja czy nawet „tryplikacja" monitoringu/audytu/przeglądów wykonywanych przez każdą z funkcji jest na porządku dziennym. Weryfikacja i końcowe zapewnienie jest osiągane w ten sposób kilkukrotnie bez wzajemnego wykorzystania produktów prac.		
	Brak właścicielstwa powoduje, że przeglądy zgodności są wykonywane kilkukrotnie przez różne jednostki organizacyjne bez koordynacji.		
Ocena Ryzyka	Ocena ryzyka jest wykonywana przez każdy zespół bez uzgodnienia i koordynacji prac. Wyniki są trudno porównywalne, brak połączenia z procesem samooceny.		
Raportowanie	Zwielokrotnione, bez wspólnych uzgodnionych linii raportowania. Raporty prezentują różne spostrzeżenia, różne punkty widzenia, różne terminologie i konteksty.		
Zarządzanie Usprawnieniami	Każda z funkcji ma własne rozwiązania i metodyki do śledzenia postępów prac nad wdrażaniem usprawnień. Bark współpracy w zakresie weryfikacji powdrożeniowej.		
Definicje i Kategorie Ryzyk	Różna nomenklatura, modele. Odmienna kategoryzacja i sposoby oceny.		

Nasza odpowiedź to Integrated Compliance & Risk Management

Integrated Compliance & Risk Management (ICRM) jest praktycznym podejściem do realizacji zadań związanych z zarządzaniem ryzykiem i zgodnością. Rozpoczynając wdrożenie ICRM należy położyć duży nacisk na uświadomienie oczekiwanego ostatecznego obrazu funkcji zgodności, aby przyjęty proces wdrożeniowy zapewnił jego osiągnięcie…

Interesariusze / Drivery Zmian



Wymiar operacyjny	Oczekiwane rezultaty
Poprawa Efektywności Obniżenie Kosztów	• Ujednolicony, wspólnie koordynowany proces zarządzania ryzykiem. • Brak luk oraz zduplikowanych zadań. • Zracjonalizowany proces obniżający koszty i podnoszący jakość zarządzania ryzykiem.
Poprawa Skuteczności	• Oparcie planowania zaangażowania na ocenie ryzyka niezgodności. • Efektywne planowanie środków w oparciu o analizę ryzyka, korzyści i kosztów.
Jasna Odpowiedzialność Zdefiniowane Relacje	• Jasno sprecyzowane role, zadania i odpowiedzialność. • Zdefiniowany przepływ informacji pomiędzy jednostkami i regulatorem.
Jednolita Ocena Ryzyka	• Koordynacja pomiędzy biznesem i poszczególnymi jednostkami zarządzającymi ryzykiem w celu podniesienia gotowości i czasu odpowiedzi na zagrożenie. • Spójne zarządzanie obłożeniem pracą.
Technologia wspierająca	• Zautomatyzowane narzędzia do identyfikacji ryzyk i luk. • Automatyczna dokumentacja kontroli oraz wymogów regulacyjnych. • System śledzenia wdrożeń i skuteczności kontroli.
Skonsolidowane Raportowanie	• Centralny zagregowany system raportowania ryzyka i zgodności. • Wspólne miary i kategorie ryzyk, wielowymiarowe raportowanie w przekroju na linie biznesowe, procesy, wymogi, …

Integrated Compliance & Risk Management(ICRM)
Proces wdrożeniowy

Dane wejściowe

- Zmieniające się otoczenie regulacyjne
- Procedury wewnętrzne
- Presja Rynkowa / Konkurencja
- Istniejąca infrastruktura „silosowa" Skomplikowane i fragmentaryczne rozwiązania

TRANSFORMACJA ICRM

Dane wyjściowe

Zintegrowany proces zarządzania zgodnością i ryzykiem wsparty odpowiednią infrastrukturą:
- **Ludzie,**
- **Procesy,**
- **Ład,**
- **IT**

Podniesiona skuteczność i obniżone koszty

Uporządkowany Ład Korporacyjny i harmonijne przepływy informacji

Transparentność

Całkowite wdrożenie ICRM to 12-18 miesięcy jednak już po kilku miesiącach widoczne są pierwsze efekty i oszczędności ….

Start projektu — 180 dni — 360 dni

Początkowe Oszczędności :
- Dodatkowe korzyści organizacyjne dzięki zwiększonej wydajności
- Eliminacja nakładających się funkcji
- Eliminacja zbędnych działań
- Podejście do testowania bazujące na ryzyku
- Ulepszona struktura komitetu ds. ryzyka skupiona na kluczowych ryzykach

Oszczędności krótkoterminowe:
- Alokacja zasobów względem ryzyk
- Usprawnione raportowanie
- Racjonalizacja kontroli
- Transparentne i skoordynowane zarządzanie ryzykiem

Oszczędności długoterminowe:
- Standaryzacja procesów i kontroli
- Zautomatyzowany workflow
- Zautomatyzowane kontrole prewencyjne oraz KPIs/KRIs dla lepszej alokacji zasobów

Nowoczesna funkcja zgodności zgodnie z modelem ICRM

Value-added i zorientowana biznesowo

- Odejście od jednostki reaktywnej w kierunku „patrzącej-w-przód" funkcji starającej się przewidywać ryzyka regulacyjne krystalizujące się na arenie lokalnej i międzynarodowej
- Wbudowywanie elementów zarządzania ryzykiem zgodności w procesy biznesowe na najniższym poziomie i odchodzenie od pisania „opasłych" polityk i podręczników
- Wzięcie odpowiedzialności za aktywne i ciągłe szkolenie ścisłego kierownictwa w zakresie wymogów regulacyjnych – wskazywanie strategicznych implikacji zamiast cytowania przepisów i przytaczania konsekwencji

Efektywna kosztowo

- Systematyczne usuwanie nieefektywności wynikających z kompleksowości/wielości regulacji wewnętrznych i systemów
- Ciągłe poszukiwanie i usuwanie duplikacji oraz luk
- Wypracowanie „radaru" (narzędzi) zapewniającego szybkie osiąganie i utrzymywanie zgodności ze zmieniającym się środowiskiem regulacyjnym
- Eliminacja niepotrzebnych elementów kontrolnych i warstw raportowania, które są spadkiem ewolucyjnego osiągania zgodności

Zarządzająca ryzykiem braku zgodności

- Transformacja w dyscyplinę zarządzania ryzykiem, nakierowaną na wspieranie osiągania celów biznesowych organizacji
- Rozwój zawodowy pracowników, przekształcenie w pragmatyczny zespół rozumiejący biznes, regulacje i zarządzanie ryzykiem
- Przygotowanie spójnego systemu raportowania zarządczego wspierającego podejmowanie decyzji

Ocena systemu zarządzania ryzykiem i kontroli wewnętrznej przez audyt wewnętrzny

Przełożenie wyników zadań audytowych na całościową ocenę systemu zarządzania ryzykiem i kontroli wewnętrznej

Opracowanie modelu współpracy Audytu Wewnętrznego oraz funkcji Zarządzania Ryzykiem

Zarządzanie Ryzykiem

Ustanowienie profilu ryzyk, polityk i kontroli

Wdrożenie miar ryzyka i systemu raportowania

Odpowiedzialność

Audyt Wewnętrzny

Testowanie skuteczności profilu ryzyka, polityk i kontroli

Walidacja narzędzi do identyfikowania ryzyka

Weryfikacja

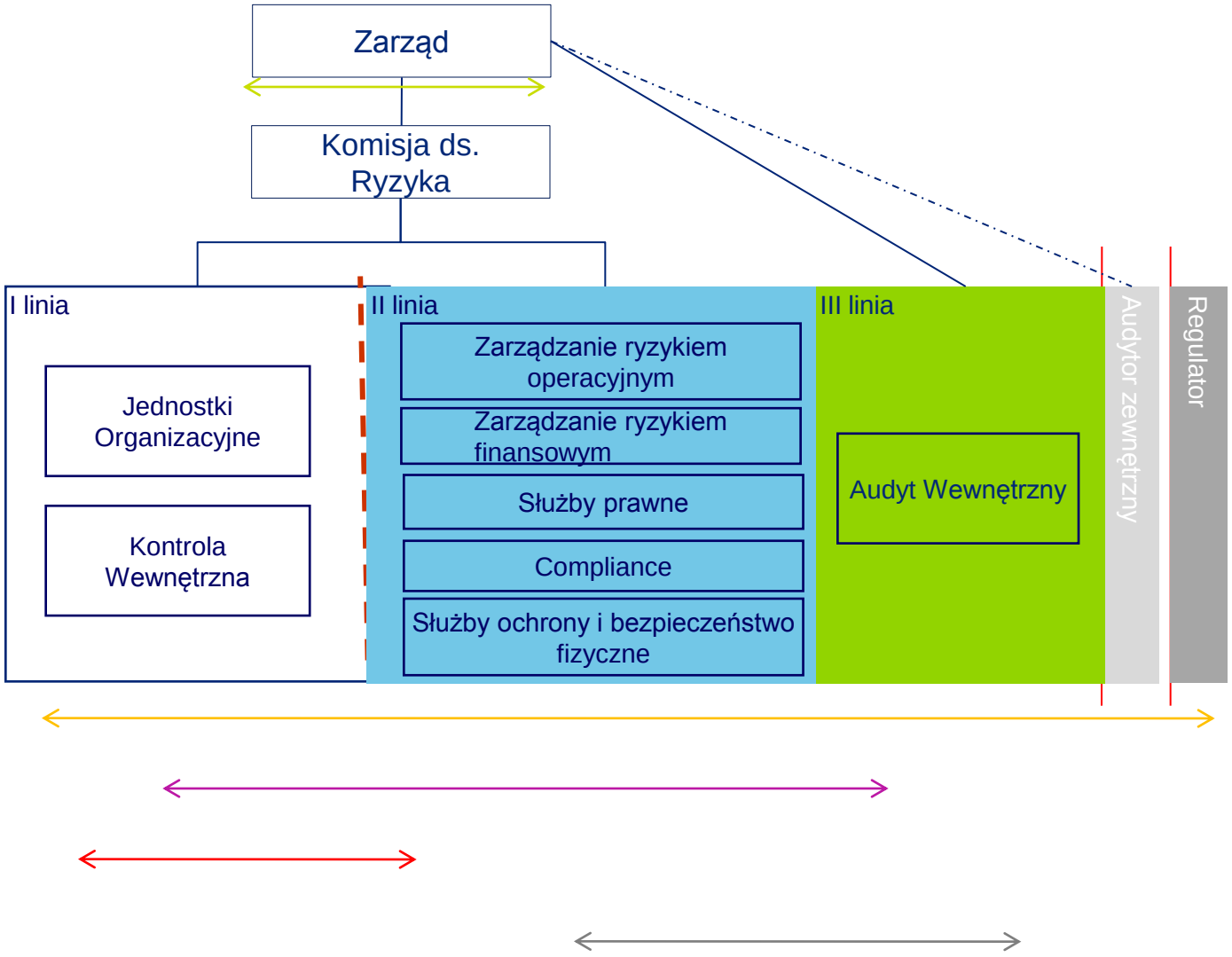
Rola Audytu Wewnętrznego w procesie zarządzania ryzykiem
Zintegrowane podejście

Rola audytu w kontekście Zarządzania Ryzykiem	Role, których audyt wewnętrzny nie powinien spełniać
• Kontrola procesu zarządzania ryzykiem • Kontrola poprawności szacowania ryzyka • Przegląd procesu zarządzania istotnym ryzykiem • Ocena raportów z istotnych ryzyk	• Ustanawianie apetytu na ryzyko • Wpływanie na proces Zarządzania Ryzykiem • Podejmowanie decyzji o reakcji na ryzyko • Wdrażanie odpowiedzi na ryzyko • Odpowiedzialność za Zarządzanie Ryzykiem

Solvency II i rola audytu wewnętrznego

Umiejscowienie i rola audytu wewnętrznego w ramach systemu zarządzania zakładem ubezpieczeniowym

Koncepcja trzech linii obrony



Etapy procesu zarządzania ryzykiem - model oparty na COSO II

1. Identyfikacja ryzyka

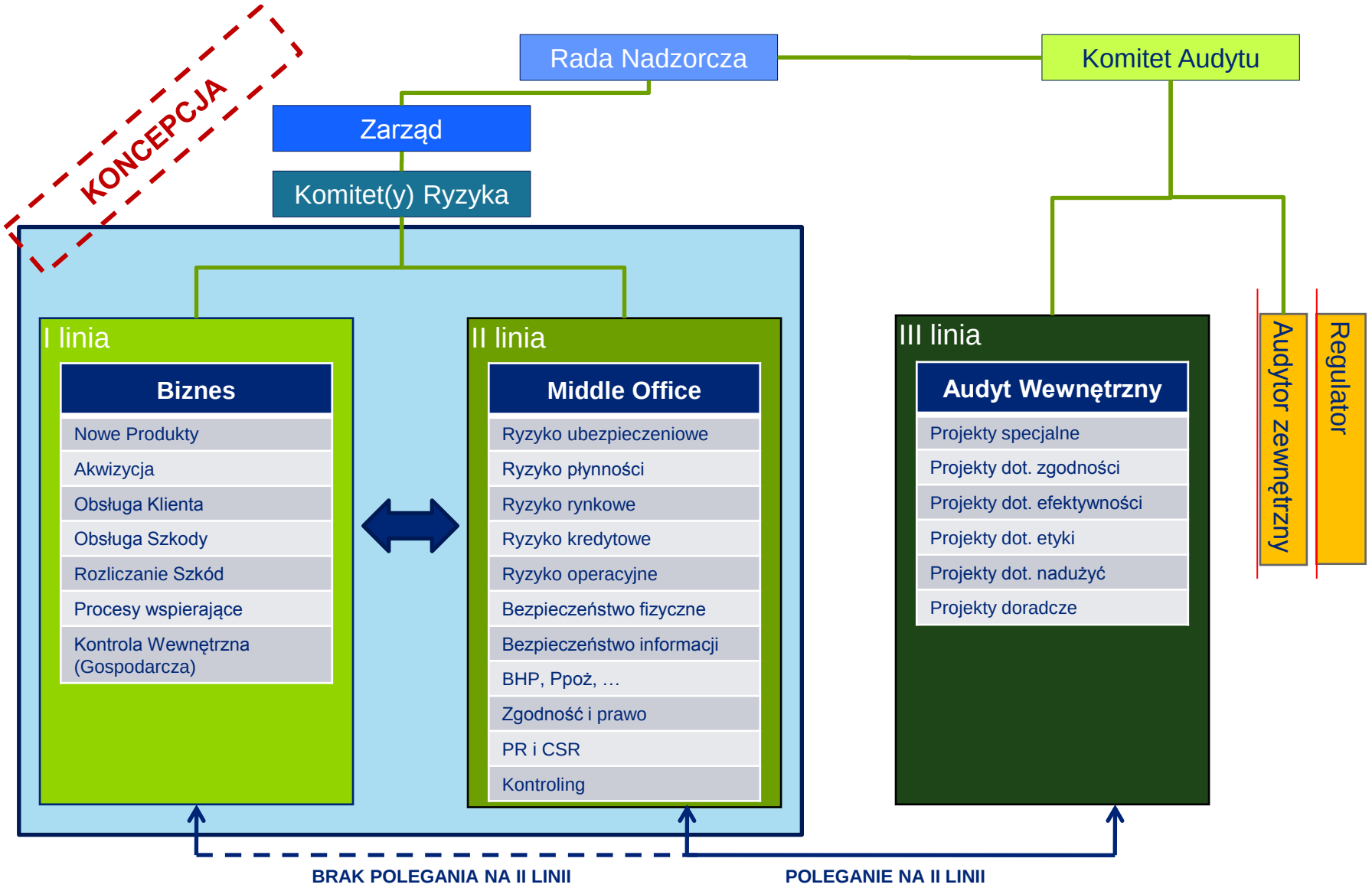
2. Analiza i ocena ryzyka

3. Ustalenie progu akceptowalności ryzyka

4. Postępowanie z ryzykiem

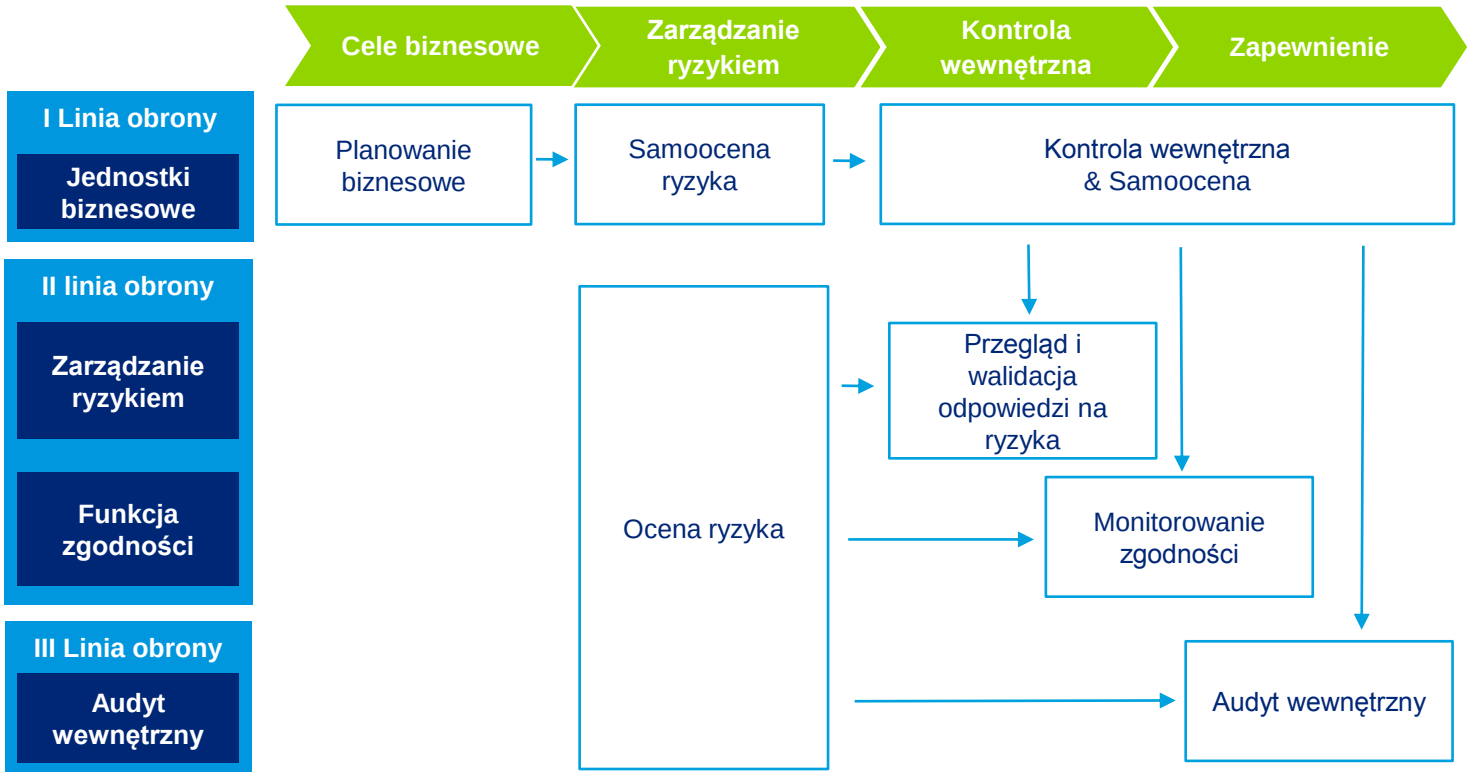
5. Monitorowanie procesu i dokonywanie zmian

Organizacja systemu zarządzania ryzykiem i audytu wewnętrznego



Kluczowe jest, żeby struktura organizacyjna była dobrze zintegrowana z systemem zarządzania ryzykiem

Struktura organizacyjna powinna zapewniać wsparcie procesu ORSA i systemu zarządzania ryzykiem oraz podział odpowiedzialności zgodnie z koncepcją „trzech linii obrony”.



Korzyści wynikające prawidłowego wdrożenia struktury organizacyjnej:

- uspójnienie definicji, procedur i metodyk
- uzgodnienia i koordynacja prac w celu końcowego zapewnienia
- jednolita ocena ryzyka, umożliwiająca porównywalność wyników i połączenie z procesem samooceny
- uzgodnienie linii raportowania, spostrzeżeń, punktów widzenia, terminologii
- odejście od jednostki reaktywnej w kierunku „patrzącej w przyszłość”

Solvency II i rola audytu wewnętrznego

Wymogi regulacyjne wobec audytu wewnętrznego

Wymogi regulacyjne wobec Kontroli Wewnętrznej i Audytu Wewnętrznego – Solvency II

Podstawa prawna

Dyrektywa Parlamentu Europejskiego i Rady w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (SOLVENCY II) (2009/138/WE).

Kwestie związane z kontrolą wewnętrzną i audytem wewnętrznym zostały ujęte w artykułach 41 – 50.

Kontrola wewnętrzna, Art. 46
„Zakłady ubezpieczeń i zakłady reasekuracji wprowadzają efektywny system kontroli wewnętrznej. System ten obejmuje co najmniej procedury administracyjne i księgowe, organizację kontroli wewnętrznej, odpowiednie ustalenia w zakresie raportowania na wszystkich szczeblach zakładu oraz funkcję zgodności z przepisami"

Główne zadania kontroli wewnętrznej

- Organizacja systemu kontroli wewnętrznej
- Identyfikacja wszystkich występujących procesów wraz z identyfikacją ryzyk z nimi związanych oraz określeniem ich istotności – stworzenie mapy ryzyka
- Przeprowadzania przez audyt wewnętrzny obiektywnego przeglądu i oceny wewnętrznego systemu kontroli
- Cykliczne raporty z audytu dla Zarządu i Rady Nadzorczej zawierające wnioski z przeprowadzonych przeglądów

Wymogi regulacyjne wobec Kontroli Wewnętrznej i Audytu Wewnętrznego – Solvency II

System kontroli wewnętrznej to zbiór operacyjnych procesów obejmujących pracowników merytorycznych i administracyjnych na każdym szczeblu.

Elementy prawidłowego systemu kontroli wewnętrznej:

Prawidłowe środowisko kontroli oraz nadzór ze strony kierownictwa	• Poziom zintegrowania, wartości etyczne oraz kompetencje personelu • Struktura organizacyjna • Filozofia oraz styl zarządzania • Czynniki zewnętrzne mające wpływ na sposoby funkcjonowania (np. niezależne audyty, środowisko regulacyjne, konkurencyjność rynku) • Metody przypisywania uprawnień i odpowiedzialności oraz sposobu organizacji i rozwoju zasobów ludzkich • Zaangażowanie i sposoby działania prezentowane przez Zarząd oraz jego komitety, w szczególności Komitet Audytu i Zarządzania Ryzykiem
Mechanizmy kontrolne	• Skuteczne i sprawne procesy realizujące cele oraz minimalizujące ryzyka • Polityki i procedury ustanowione w celu zapewnienia efektywnego funkcjonowania procesów kontrolnych • Przegląd czynności operacyjnych • Zatwierdzenia i autoryzacje transakcji i czynności • Podział obowiązków • Planowanie urlopów oraz okresowe przesunięcia obowiązków osób na kluczowych stanowiskach • Kontrola dostępu oraz zasady użycia wrażliwych aktywów, danych i systemów • Niezależne kontrole i weryfikacje efektywności operacyjnej oraz uzgodnień sald
Komunikacja	• Systemy zarządzania informacjami identyfikują i pobierają odpowiednie dane na czas • Systemy księgowe zapewniają właściwie powiązane dane w stosunku do aktywów i pasywów • Systemy informatyczne zapewniają skuteczną komunikację w zakresie pozycji i czynności • Plan działania na wypadek awarii systemów informatycznych
Monitoring	• Okresowa ocena kontroli wewnętrznej w drodze samooceny i niezależnego audytu • Systemy zapewniają regularne oraz właściwe raportowanie wad kontroli • Funkcjonowanie mechanizmów zapewniających regularne modyfikacje polityk i procedur

Redefiniowanie roli Audytu Wewnętrznego wobec powstającej funkcji Zarządzania Ryzykiem oraz funkcji Zgodności

Dostosowanie funkcji audytu wewnętrznego do wymogów Solvency II

Zadania dotyczące analizy oraz oceny ryzyka

- Uwzględnienie w rocznych planach audytu zadań mających na celu analizę i ocenę ryzyk poszczególnych obszarów
- Weryfikacja, czy mechanizmy kontrolne zidentyfikowanych ryzyk funkcjonują skutecznie a poziom ryzyk pozostaje na akceptowalnym poziomie
- Wdrożenie wytycznych postępowania w przypadku ryzyk na nieakceptowanym poziomie
- Stworzenie wytycznych dotyczących analizy i oceny ryzyk

Stworzenie zasad przygotowywania rocznych planów audytu oraz programów audytów

- Plan audytu powinien być tworzony w oparciu o listę zidentyfikowanych kluczowych ryzyk występujących w Spółce
- Plan audytu powinien być akceptowany przez Komitet Audytu
- Programy audytów powinny zawierać co najmniej następujące elementy:
  - Ryzyka, procesy, jednostki i okres organizacyjne podlegające audytowi
  - Listę poszczególnych kroków realizacji zadania wraz ze wskazaniem oczekiwanych odpowiedzi na ryzyko w tym kontroli wewnętrznych, metod badania, wielkość badanej próby, harmonogramu prac i ich zakończeni
  - Testy uzgodnione z funkcją Zgodności

Raportowanie

- Przygotowywanie okresowych raportów z wyników audytów sporządzanych przez Audytora Wewnętrznego i przekazywanych Komitetowi Audytu i Prezesowi Zarządu Spółki

Kierunek transformacji Departamentu Audytu Wewnętrznego
Kluczowe założenia

1. **Audyt Wewnętrzny powinien:**
   - Być niezależny – podległy bezpośrednio Prezesowi Zarządu, raportować do Komitetu Audytu przy RN
   - Być obiektywny – nie zaangażowany w bieżącą działalność operacyjną
   - Przysparzać wartości – jego działania powinny być ukierunkowane i przyczyniać się do wzrostu efektywności działania Spółki

2. **Audyt Wewnętrzny** powinien:
   - Wspierać organizację poprzez rozpoznanie i ocenę znaczących zagrożeń ryzykiem (jednakże, nie jest on odpowiedzialny za wdrożenie i zarządzanie tym procesem)
   - Przyczyniać się do usprawnienia systemów zarządzania ryzykiem i kontroli
   - Rezultaty prowadzonych przez Audyt Wewnętrzny prac powinny zasilać proces zarządzania ryzykiem

3. Audyt Wewnętrzny powinien **funkcjonować w sposób maksymalnie skoordynowany z innymi** (wewnętrznymi i zewnętrznymi) **funkcjami kontrolnymi i nadzorczym**

4. Audyt Wewnętrzny powinien funkcjonować w sposób **zapewniający efektywność procesu raportowania**

5. Możliwość zatrudnienia/wynajęcia dobrze opłacanych **specjalistów z różnych dziedzin audytu wewnętrznego** oraz wykorzystywania ich wiedzy i doświadczenia

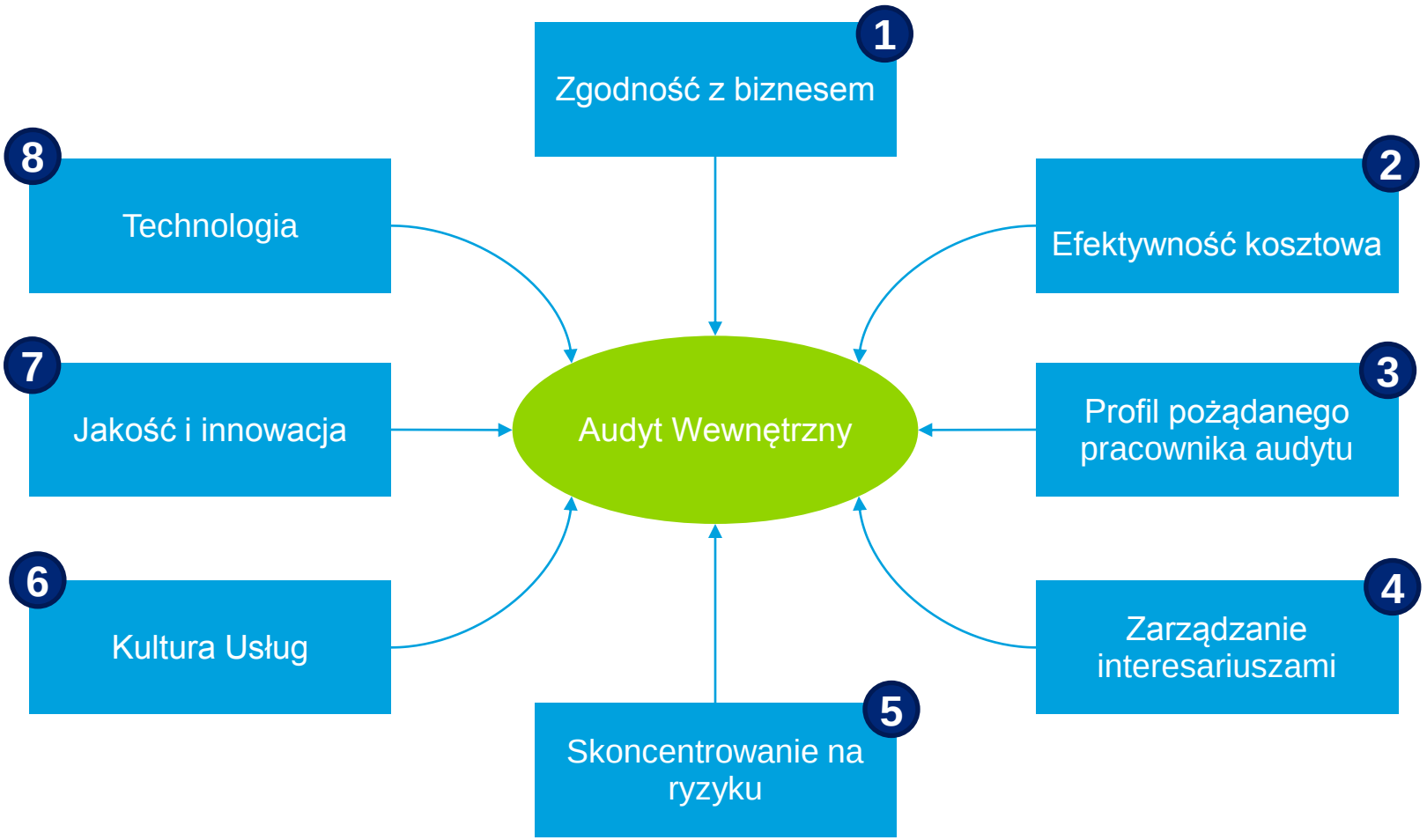
6. Uniwersum audytu wewnętrznego spółki holdingowej powinno obejmować wszystkie obszary ryzyka również te, które funkcjonalnie znajdują się w spółkach zależnych

7. Audyt Wewnętrzny realizujący zadania audytowe w sposób zaplanowany powinien być traktowany odrębnie od inspekcyjnej kontroli wewnętrznej rozumianej jako realizacja zleconych zadań doraźnych

Solvency II i rola audytu wewnętrznego

Dobre praktyki – oczekiwania wobec audytu wewnętrznego

Dobre praktyki – oczekiwania interesariuszy (1/3)



Dobre praktyki – oczekiwania interesariuszy (2/3)

1. Wartość zgodna z oczekiwaniami interesariuszy

- Misja i wizja są wyraźnie sformułowane i zakomunikowane
- Zakres usług jest dobrze określony i zakomunikowany
- Strategia obejmuje wizję i kluczowe cele

2. Dostarczanie usług efektywnych kosztowo

- Inwestycja w strukturę audytu bazuje na konserwatywnym podejściu ROI (Return on Investment)
- Zarządzanie docelową wydajnością audytu jest podstawą efektywności kosztowej

3. Dostosowanie pożądanego profilu audytorów wewnętrznych

- Właściwe dopasowanie odpowiednich specjalistów do zadań audytowych
- Formalna ścieżka kariery dla pracowników audytu wewnętrznego
- Ciągłe rozwijanie umiejętności, wiedzy, doświadczenia i kwalifikacji audytorów wewnętrznych

4. Zarządzanie relacjami z interesariuszami

- Interesariusze postrzegają audyt wewnętrzny jako wysoko wykwalifikowanych specjalistów
- „FeedBack" jest cenionym źródłem informacji, na równi z przeprowadzanymi ankietami opisującymi jakość usług audytu
- Regularne raportowanie tzw. „wartości dodanej" jaką przyniósł audyt wewnętrzny

Dobre praktyki – oczekiwania interesariuszy (3/3)

5. Skoncentrowanie działalności na krytycznych obszarach usług

- Ocena ryzyka powinna zawierać ryzyka biznesowe, nowe ryzyka , jak i ryzyko nadużyć
- Plany audytu powinny być wystarczająco elastyczne, aby zareagować na ryzyka nowopowstałe i ryzyka biznesowe
- Planowanie audytu i zasobów bazuje na podejściu „Top-down" i strategii

6. Rozpowszechnianie kultury usług

- Metryki mierzą satysfakcję klienta bazując na oczekiwaniach interesariuszy
- Szkolenia zawierają w sobie elementy poprawiające znajomość biznesu, ocenę i niezależność
- Wszystkie usługi audytowe zapewniają równość, niezależność, obiektywność i wartość dla interesariuszy

7. Promocja poprawy jakości i zwiększenia innowacji

- Określenie i przekazanie obowiązujących norm
- Przeprowadzanie regularnych przeglądów w celu zlokalizowania możliwości poprawy jakości
- Innowacja powinna być osadzona w kulturze audytu wewnętrznego, konsekwentnie wspierana i nagradzana

8. Skuteczne zastosowanie technologii

- Systemy kontroli są stosowane w celu poprawy skuteczności i efektywności kontroli
- Technologia jest wykorzystywana w celu poprawy efektywności procesu audytu przez
- Ciągłość technik audytu jest dźwignią do zwiększenia zakresu kontroli i zapewnieniu wskaźników ryzyka, które mogą być sygnałami wczesnego ostrzegania przed zagrożeniem

Solvency II i rola audytu wewnętrznego

Nowe zadania audytu wewnętrznego

Zmiany zachodzące w misji Audytu Wewnętrznego

Oczekiwania wobec Audytu Wewnętrznego

- Rola zaufanego doradcy dla Kierownictwa
- Dynamiczna funkcja skupiająca się na identyfikacji ryzyk biznesowych
- Przekazywanie użytecznych informacji o szansach i słabościach wraz z rekomendacjami działań zaradczych

Wymagania wobec Departamentu Audytu Wewnętrznego

- Raportowanie do:
  - Komitetu Audytu odpowiedzialnego za monitorowanie skuteczności systemów kontroli wewnętrznej, audytu wewnętrznego oraz zarządzania ryzykiem (Ustawa z dnia 22 maja 2009 r. o biegłych rewidentach i ich samorządzie, podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym)
  - Zarządu, który podejmuje decyzje dotyczące zarządzania Spółką na podstawie rezultatów badań audytowych
- Zdefiniowanie misji, wizji, roli, odpowiedzialności i ścieżki przepływu informacji, tak aby zapewniały poziom wsparcia dla bieżącej działalności
- Nowe regulacje Solvency II nakładają na audytorów wewnętrznych konieczność posiadania specjalistycznej wiedzy w różnorodnych obszarach – metody pomiaru ryzyka, weryfikacja i walidacja modeli statystycznych, weryfikacja adekwatności całościowego systemu zarządzania ryzykiem w ramach procesu ORSA

Czynniki zmiany roli Audytu Wewnętrznego

- Technologia wymiany informacji pomiędzy organizacjami i departamentami
- Nacisk interesariuszy na zarządzanie ryzykiem i zapewnienie zgodności
- Wzrost znaczenia Komitetu Audytu

Nowe zadania audytu wewnętrznego w kontekście zapisów Solvency II dla funkcji aktuarialnej

Solvency II

Art. 44, pkt 2: „System zarządzania ryzykiem obejmuje co najmniej następujące obszary:
a) ocena ryzyka przyjmowanego do ubezpieczenia i tworzenie rezerw…”

Art. 48, pkt 1: „Zakłady ubezpieczeń i zakłady reasekuracji zapewniają skuteczną funkcję aktuarialną w celu:
a) koordynacji ustalania wartości rezerw techniczno-ubezpieczeniowych;
b) zapewnienia adekwatności metodologii i stosowanych modeli, jak również założeń przyjętych do ustalania rezerw techniczno-ubezpieczeniowych;
c) oceny, czy dane wykorzystane do obliczenia rezerw techniczno-ubezpieczeniowych są wystarczające i czy są odpowiedniej jakości;
d) porównania najlepszych oszacowań z danymi wynikającymi ze zgromadzonych doświadczeń;
e) informowania organu administrującego, zarządzającego lub nadzorczego o wiarygodności i adekwatności ustalania wartości rezerw techniczno-ubezpieczeniowych;
f) nadzorowania obliczeń rezerw techniczno-ubezpieczeniowych w przypadkach określonych w art. 82;
g) wyrażania opinii na temat ogólnej polityki przyjmowania ryzyka do ubezpieczenia;
h) wyrażania opinii na temat adekwatności rozwiązań w zakresie reasekuracji; oraz
i) wnoszenia wkładu w efektywne wdrażanie systemu zarządzania ryzykiem, o którym mowa w art. 44, w szczególności w odniesieniu do modelowania ryzyka leżącego u podstaw obliczeń wymagań kapitałowych określonych w rozdziale VI sekcja 4 i 5, oraz w odniesieniu do oceny, o której mowa w art. 45.”

Zgodnie z zadaniami nałożonymi na audyt wewnętrzny przez Solvency II jest on zobowiązany do oceny adekwatności i efektywności systemu zarządzania ryzykiem, którego część stanowi **ocena ryzyka przyjmowanego do ubezpieczenia i tworzenie rezerw (funkcja aktuarialna)**.

Nowe zadania audytu wewnętrznego w kontekście zapisów Solvency II dla funkcji aktuarialnej

Zgodnie z wytycznymi do regulacji Solvency II opublikowanymi przez Europejski Organ Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (EIOPA) do szczególnych obszarów podlegających badaniu w ramach zadań audytowych powinny należeć mechanizmy kontrolne zapewniające:

1. **Kompletność danych** – Funkcja aktuarialna powinna zapewniać, że dane wykorzystywane w kalkulacji rezerw techniczno-ubezpieczeniowych pokrywają wystarczająco duży okres obserwacji, który charakteryzuje badaną rzeczywistość. Wybór danych powinien być oparty na maksymalnej liczbie adekwatnych obserwacji, z zastrzeżeniem ograniczeń wynikających ze zgodności z wszystkimi pozostałymi wytycznymi.
2. **Adekwatność danych** – Funkcja aktuarialna powinna zapewniać, że dane odnoszące się do różnych okresów czasu są spójne.

Audyt wewnętrzny w ramach prowadzonych zadań audytowych powinien weryfikować, czy mechanizmy kontrolne wskazane w wytycznych dla funkcji aktuarialnej służące **analizie i walidacji jakości danych** realizowane są w prawidłowy i efektywny sposób.

- Dokładność i kompletność danych powinna być oceniana przez **szereg kontroli**. Zakres kontroli powinien być na tyle wyczerpujący, aby pokryć analizę wszystkich elementów objętych kryteriami kompletności i adekwatności, umożliwiając wykrycie ewentualnych nieprawidłowości. Ocena powinna być przeprowadzona na odpowiednio niskim poziomie szczegółowości.
- W trakcie przeglądu jakości danych w kontekście obliczania rezerw techniczno-ubezpieczeniowych, funkcja aktuarialna powinna **uwzględniać wnioski z analiz przeprowadzonych przez audyt zewnętrzny lub inne podmioty**. W razie zidentyfikowania istotnych problemów w odniesieniu do jakichkolwiek wymagań dotyczących dokładności, kompletności lub adekwatności wybranych danych, problemy te powinny być dokładnie przeanalizowane, a dane te nie powinny być wykorzystywane bez ustalenia odpowiednich rozwiązań w celu przezwyciężenia zidentyfikowanych problemów.
- W trakcie procesu sprawdzania poprawności danych, należy również wziąć pod uwagę **źródło danych i ich przeznaczenie**.

Nowe zadania audytu wewnętrznego w kontekście zapisów Solvency II dla funkcji aktuarialnej

W celu prawidłowej koordynacji kalkulacji rezerw techniczno-ubezpieczeniowych, funkcja aktuarialna powinna w szczególności koordynować ocenę i weryfikację stosownych danych przed ich wykorzystaniem zgodnie z przeznaczeniem. Zadanie to obejmuje:

- **Wybór danych do wykorzystania w wycenie**, uwzględniając kryteria dokładności, adekwatności i kompletności danych, biorąc pod uwagę metodologie, które byłyby najbardziej odpowiednie do zastosowania podczas kalkulacji. W tym procesie powinny zostać wykorzystane wszystkie adekwatne narzędzia, w celu weryfikacji jakichkolwiek istotnych różnic, które można wskazać poprzez porównanie danych z różnych okresów lub różnych analiz;
- **Raportowanie rekomendacji w zakresie wdrożenia usprawnień procedur wewnętrznych**, które zostały uznane za istotne dla poprawy zgodności. Określenie przypadków, w których dodatkowe dane zewnętrzne są wymagane, oraz ocena jakości tych danych, podobnie jak dla danych wewnętrznych, z uwzględnieniem ich specyfiki (określenie, czy dane rynkowe są wymagane lub kiedy powinno być oparte na dążeniu do usunięcia braków w zakresie jakości danych wewnętrznych) i możliwości usprawnienia dostępnych danych.
- **Ocena, czy wymagane są jakieś usprawnienia w odniesieniu do dostępnych danych** zgodnie z najlepszymi praktykami aktuarialnymi, w celu poprawy jakości dopasowania i wiarygodności szacunków pochodzących z aktuarialnych i statystycznych metodyk ustalania rezerw w oparciu o te dane.
- **Rejestrowanie wszelkich istotnych informacji zebranych w tym procesie**, które mogą okazać się istotne dla innych etapów kalkulacji rezerw techniczno-ubezpieczeniowych, odnoszących się do rozumienia podstawowych ryzyk poprzez analizę danych, jak również do wiedzy na temat mocnych stron i ograniczeń dostępnych danych.

Nowe zadania audytu wewnętrznego w kontekście zapisów Solvency II dla funkcji aktuarialnej

Pozostałe zadania funkcji aktuarialnej wspierane i weryfikowane przez zadania realizowane przez audyt wewnętrzny, szczegółowo opisane w wytycznych EIOPA, obejmują:

- **Analizę nieprawidłowości danych**, w szczególności: identyfikację ich źródeł, ocenę wpływu nieprawidłowości na poziom zgodności z wymaganiami w zakresie jakości danych, modyfikację danych, wydawanie rekomendacji przez funkcję aktuarialną, zastosowanie oceny eksperckiej (w tym w odniesieniu do wiarygodności danych) oraz dokumentowanie ograniczeń danych;
- **Wykorzystanie danych pochodzących z zewnętrznego źródła**, w szczególności: wykorzystanie danych rynkowych oraz ustalenie warunków koniecznych do spełnienia przez dane rynkowe;
- **Zadania w zakresie segmentacji i ustalania zobowiązań ubezpieczeniowych**, których celem jest osiągnięcie dokładnej wyceny rezerw techniczno-ubezpieczeniowych.
- **Budowanie założeń na potrzeby kalkulacji rezerw** w zakresie m.in.: biometrycznych czynników ryzyka, identyfikacji i określenia wydatków, alokacji wydatków, projekcji wydatków, wyceny opcji i gwarancji przy uwzględnieniu sposobów zachowania właścicieli polis, przyszłych działań kierownictwa, przyszłych świadczeń uznaniowych.

Wytyczne dotyczą również **metodologii wykorzystywanych na potrzeby wycen rezerw techniczno-ubezpieczeniowych**, z którymi zgodność również powinna stanowić przedmiot okresowych zadań audytowych.

Cele i zadania funkcji aktuarialnej w zakresie systemu kontroli wewnętrznej

Przedsiębiorstwa powinny zapewnić wystarczające, jasne i adekwatne mechanizmy kontrolne w procesie kalkulacji i określania rezerw techniczno-ubezpieczeniowych.

W przypadku istotnych różnic w szacunkach rezerw techniczno-ubezpieczeniowych odnoszących się do różnych lat, funkcja aktuarialna powinna przedstawić wyjaśnienie, włączając identyfikację i wyjaśnienie źródeł odchyleń oraz ustalenie pochodzenia czynników je powodujących – wewnętrzne czy zewnętrzne.

Funkcja aktuarialna powinna uwzględniać wzajemne powiązania pomiędzy umowami reasekuracji przedsiębiorstwa, polityką ubezpieczeniową i rezerwami techniczno-ubezpieczeniowymi.

Funkcja aktuarialna powinna corocznie zgłaszać problemy i wnioski odnoszące się do zadań leżących w zakresie jej odpowiedzialności do organów administracyjnych, kierowniczych lub nadzorczych. Wszelkie istotne nieprawidłowości powinny być przedstawione do organów administracyjnych, kierowniczych lub nadzorczych wraz z rekomendacjami, w jaki sposób mogą być one usunięte, włączając terminy wykonania działań z tym związanych. Minimalne wymagania w zakresie raportowania przez funkcję aktuarialną zostały przedstawione w wytycznych.

Funkcja aktuarialna powinna zapewnić, że główne czynniki ryzyka są odzwierciedlone i odpowiednio zaadresowane w modelu wyceny stanowiącym podstawę do kalkulacji rezerw techniczno-ubezpieczeniowych, poczynionych założeniach i wykorzystanych metodykach. Należy również zapewnić stabilność modelu w odniesieniu do drobnych zmian w nim uwzględnianych.

Funkcja aktuarialna powinna wyjaśniać wszelkie istotne odchylenia pomiędzy najlepszymi szacunkami a doświadczeniami, poprzez identyfikację ich przyczyn oraz proponowanie, w stosownych przypadkach, odpowiednich zmian założeń będących podstawą modelu w celu złagodzenia wynikłych różnic.

Funkcja aktuarialna powinna wyrazić opinię, które ryzyka powinny zostać pokryte przez model wewnętrzny, w szczególności w stosunku do ryzyk odnoszących się do warunków prowadzenia działalności oraz sposobu ustalania współzależności pomiędzy ryzykami. Opinia ta powinna opierać się na analizie technicznej i powinna odzwierciedlać doświadczenie i ocenę ekspercką funkcji.

Działania funkcji aktuarialnej powinny być uzupełnione przez odpowiednią procedurę obserwacji ich rezultatów, w celu śledzenia czynności naprawczych podejmowanych w obszarach, w których zidentyfikowano nieprawidłowości.

Solvency II i rola audytu wewnętrznego

Koncepcja audytu wewnętrznego zintegrowanego z ryzykiem – Metodyka Deloitte

Pożądany podział odpowiedzialności powinien być efektywny kosztowo i współgrać z biznesem

Deloitte stosuje dziewięć zasad dla rozwinięcia zdolności zarządzania ryzykiem w ramach określonej struktury organizacyjnej. Jest to holistyczne i jednorodne podejście do wypracowania skutecznego i wydajnego programu zarządzania ryzykiem. Jednocześnie metodyka jest elastyczna i pozwala na skupienie się na kluczowych obszarach usprawnień zgodnie z Solvency II, które pozwolą na uzyskanie największych efektów.

Risk Intelligent Enterprise™ Program Methodology

Metodyka Risk Intelligence Program stosuje dziewięć zasad Risk Intelligent Enterprise dla rozwinięcia zdolności zarządzania ryzykiem w przedsiębiorstwie. Jest to holistyczne i jednorodne podejście do wypracowania skutecznego i wydajnego programu zarządzania ryzykiem. Jednocześnie metodyka jest elastyczna i pozwala na skupienie się na kluczowych obszarach usprawnień, które pozwolą na uzyskanie największych efektów.

(Nie)komfortowa dyskusja o ryzyku …

Zasada #1: W przedsiębiorstwie, które można określić jako Risk Intelligent jest używana ***wspólna*** *oraz* ***jednolita*** *dla całej organizacji* ***definicja ryzyka****, która odnosi się zarówno do* ***ochrony wartości*** *jaki i jej* ***tworzenia***

- Ryzyko to niewygodny temat do dyskusji
- Uczestnicy dyskusji postrzegają ryzyko w kategoriach zagrożenia (ryzyko jako zjawisko negatywne)
- Każdy element strategii niesie ze sobą potencjalną nagrodę i zagrożenie porażką
- Dyskusja o ryzyku jako nieodłącznym elemencie zwrotu z kapitału, nagrodzie za ryzyko, zmienia optykę dyskusji

W związku z tym istnieje potrzeba zaadoptowania nowej, bardziej zrównoważonej definicji ryzyka:

Ryzyko to możliwość powstania straty, szkody lub **ograniczenie szansy osiągnięcia korzyści**, która może negatywnie wpłynąć na osiągnięcie celów przedsiębiorstwa.

Standardy niczym solidne fundamenty domu …

- Aby zapewnić porządek i efektywne działanie potrzebna jest przejrzysta struktura, która zależy od potrzeb
- Niezależnie od potrzeb ramy działania są narzucane przez rozwiązania modelowe, np. COSO ERM, Turnbull czy normę ISO, które spełnią rolę solidnych fundamentów
- Tak skonstruowane rozwiązanie w zakresie zarządzania ryzykiem umożliwia skuteczną ocenę, które szanse można wykorzystać a których zagrożeń unikać
- Odporne procesy i procedury zarządzania ryzykiem muszą spełniać stawiane im cele a jednocześnie powinny:
    - Być spójne z przyjętą strategią biznesową
    - Być adaptowalne do:
        - Dynamicznego otoczenia biznesowego
        - Zmian w wymogach regulacyjnych

System jednak nie może być zbyt skomplikowany aby był praktyczny

*Zasada #2: **Jednolite** oraz **zgodne** ze Standarami metodyka i procedury zarządzania ryzykiem są stosowane w **całej** organizacji*

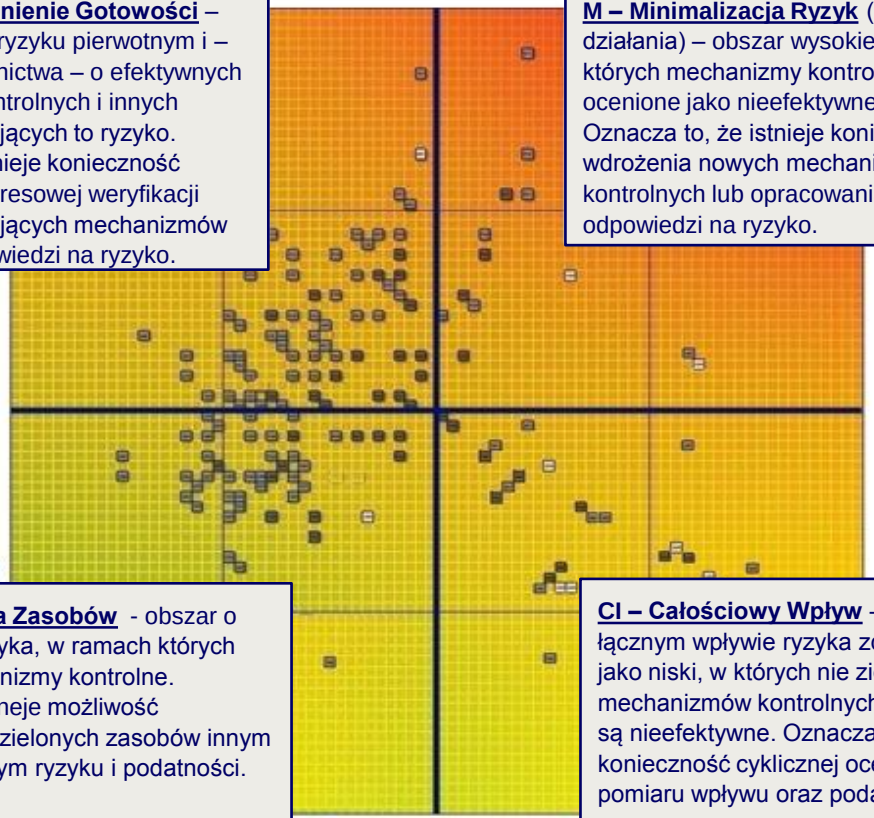
Model MARCI – koncepcja audytu zintegrowana z ryzykiem

A – Audyt, Zapewnienie Gotowości – obszar o wysokim ryzyku pierwotnym i – w percepcji kierownictwa – o efektywnych mechanizmach kontrolnych i innych działaniach adresujących to ryzyko. Oznacza to, że istnieje konieczność monitorowania i okresowej weryfikacji efektywności istniejących mechanizmów kontrolnych i odpowiedzi na ryzyko.

M – Minimalizacja Ryzyk (konieczność działania) – obszar wysokiego ryzyka w których mechanizmy kontrolne zostały ocenione jako nieefektywne lub ich brak. Oznacza to, że istnieje konieczność wdrożenia nowych mechanizmów kontrolnych lub opracowania nowych odpowiedzi na ryzyko.

- Skutki finansowe
- Reputacja
- Środowisko
- Zdrowie
- Bezpieczeństwo
- Prawne
- Tempo materializacji

WPŁYW



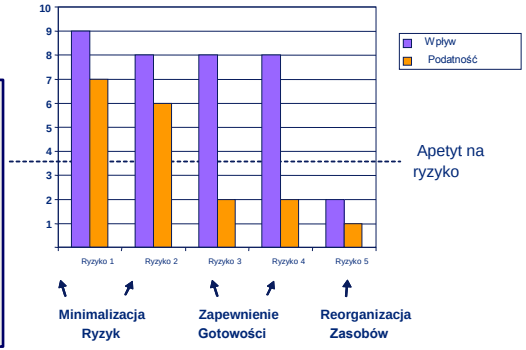
R – Reorganizacja Zasobów - obszar o niskim wpływie ryzyka, w ramach których funkcjonują mechanizmy kontrolne. Oznacza to, że istineje możliwość przesunięcia przydzielonych zasobów innym obszarom o wyższym ryzyku i podatności.

CI – Całościowy Wpływ – obszar o łącznym wpływie ryzyka zdefiniowanym jako niski, w których nie zidentyfikowano mechanizmów kontrolnych lub istniejące są nieefektywne. Oznacza to, że istnieje konieczność cyklicznej oceny tych ryzyk i pomiaru wpływu oraz podatności.

PODATNOŚĆ

- Skuteczność działań adresujących ryzyko
- Szybkość reakcji
- Stopień skomplikowania
- Skala i tempo zmian

Metoda MARCI – służy do prezentacji oceny ryzyk według wcześniej określonych parametrów (tj. podatności i wpływu ryzyka). Umiejscowienie na wykresie będzie stanowić podstawę do określenia reakcji na ryzyko w kontekście istniejących już mechanizmów kontroli. W zależności od wagi ryzyka należy przypisać do jednej z czterech kategorii.



Niczym orkiestra symfoniczna …

*Zasada #3: **Główne zadania, kompetencje, odpowiedzialność** i **uprawnienia** związane z zarządzaniem ryzykiem w organizacji są **jasno określone***

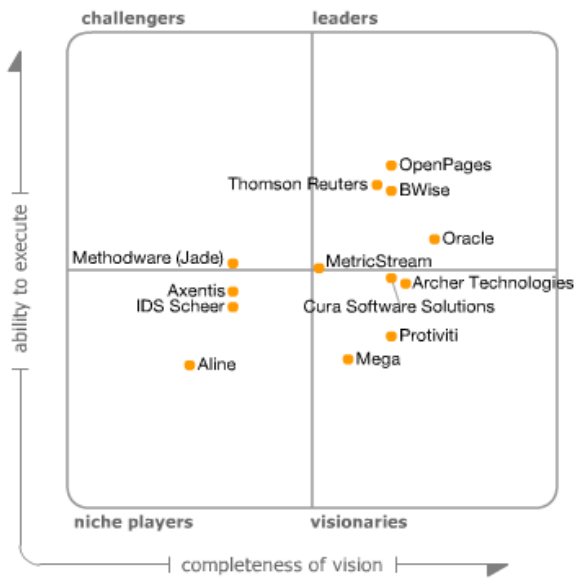
- Poprawne zarządzanie ryzykiem jest wysiłkiem grupowym - pomimo podziału ról, skomplikowane procesy odbywają się równolegle
- Część zadań odbywa się w tle, tj. bez uświadomienia tego faktu uczestnikom procesu, pomimo tego należy zapewnić ich codzienną realizację
- Dlatego niezbędny jest proces informowania, szkolenia i komunikowania, aby wszyscy uczestnicy mieli świadomość wagi i konsekwencji indywidualnych działań dla wspólnego wyniku - jak w orkiestrze

Kierujemy się wspólną mapą …

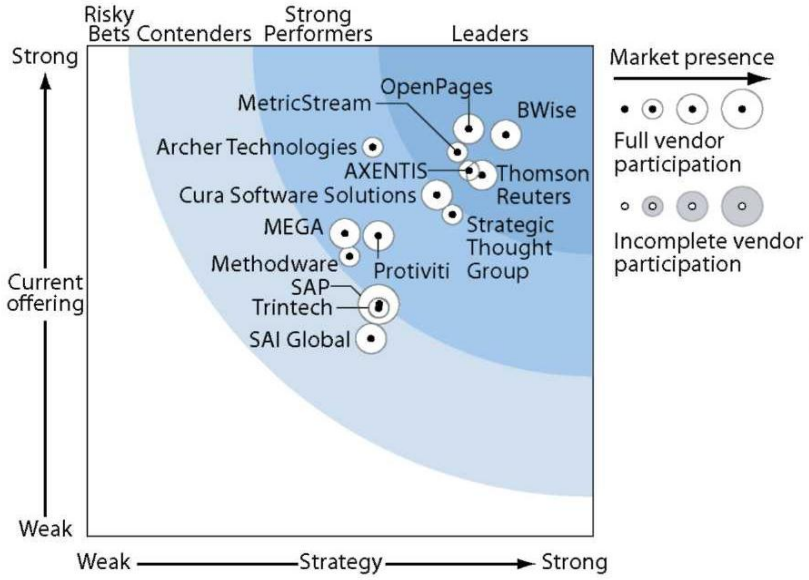
*Zasada #4: Organizacja wykorzystuje **wspólną infrastrukturę** wspierającą jednostki organizacyjne w wypełnianiu przez nie ich zadań związanych zarządzaniem ryzykiem*

- Skuteczne zarządzanie ryzykiem wymaga specjalizacji, ale Specjaliści w zarządzaniu ryzykiem są postrzegani jak zamknięta subkultura, która posiada własny dialekt, zwyczaje, rytuały a nawet przekonania
- **Ponieważ ryzyko nie istnieje w izolacji, specjaliści nie mogą pozostawać zamknięci w silosach organizacyjnych czy odcięci od biznesu własnym językiem i terminologią**
- Aby zarządzanie ryzykiem było skuteczne i wspierało osiąganie zysków muszą powstać mosty łączące silosy merytoryczne i organizacyjne w postaci wspólnej infrastruktury:
    - Koordynacja i synchronizacja działań
    - Harmonizacja słowników i pojęć
    - Wspólne narzędzia
    - Wspólne procesy, i systemy tam gdzie jest to tylko możliwe
    - Eliminacja duplikacji wysiłków
    - Okresowe dyskusje dot. ryzyka, strategii
    - Włączenie ryzyka w proces podejmowania decyzji
    - Przygotowanie miar do pomiaru skuteczności zarządzania ryzykiem

Rankingi platform do zarządzania ładem korporacyjnym, ryzykiem i zgodnością



Gartner (lipiec 2009)



The Forrester Wave (lipiec 2009)

- Na bazie naszych doświadczeń proponujemy rozważyć następujące kwestie przygotowując wybór systemu:
  - Funkcjonalność oraz perspektywy rozwoju systemu - pozycję w rankingach światowych
  - Dostępność prekonfigurowanych wersji branżowych
  - Obecność na lokalnym polskim rynku firmy wspierającej i posiadająca zaplecze (zarówno dot. systemu jak i ERM)
  - Dostępność polskiej wersji językowej
  - Funkcjonalność wspierania Audytu Wewnętrznego oraz integrację z modułami ERM (niedoceniane)
  - Współpracę dostawcy systemu IT z firmami doradczymi (synergia metodyk i systemu IT)

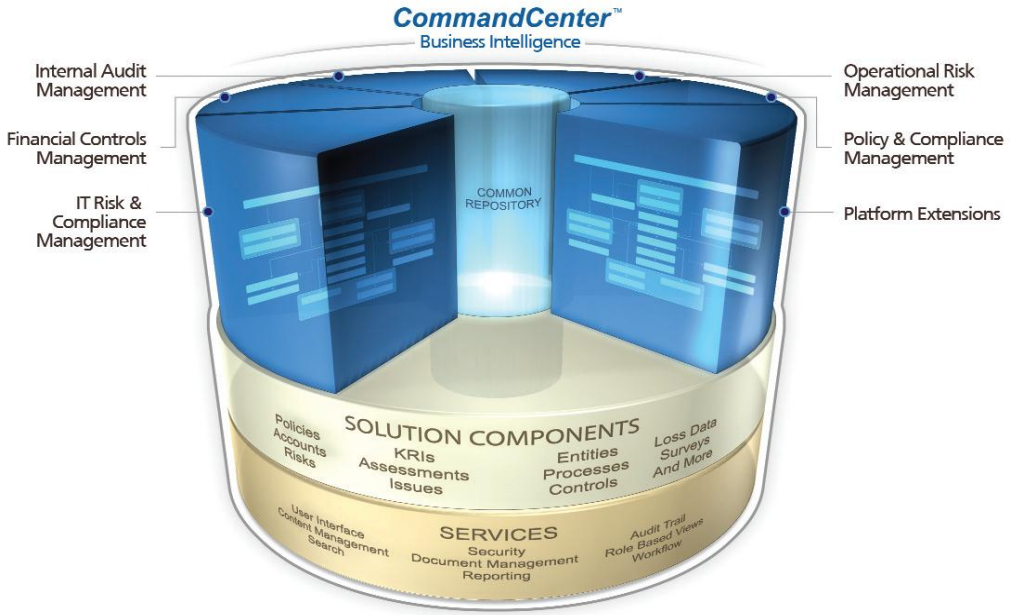
Platforma OpenPages

Platforma OpenPages służy jako podstawa do działań ERM w organizacji poprzez możliwość połączenia inicjatyw w zakresie ryzyka i zgodności w pojedynczy system. Rozwiązania w zakresie Zarządzania Kontrolami Finansowymi, Zarządzania Ryzykiem Operacyjnym, Ryzykiem IT i Zgodności, Zarządzania Polityką i Zgodnością oraz Zarządzania Audytem Wewnętrznym zapewniają modułowe i zintegrowane podejście do ładu korporacyjnego, ryzyka i zgodności, umożliwiając organizacji:

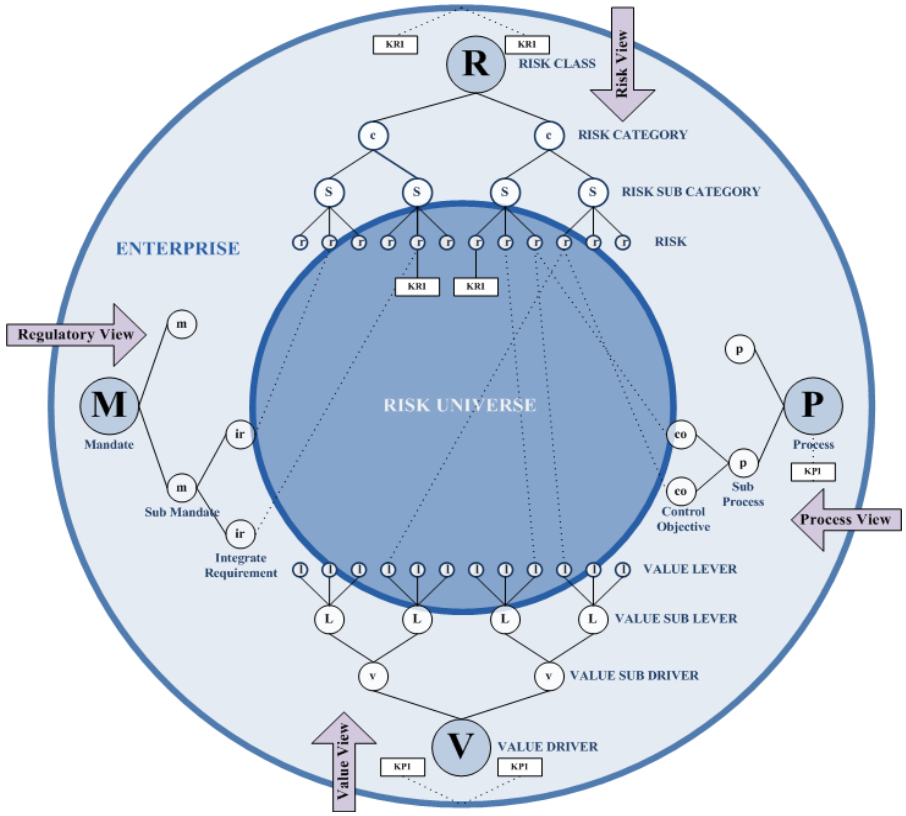
- Zarządzanie ryzykiem i zgodnością w odniesieniu do różnych regulacji
- Zrozumienie współzależności pomiędzy procesami, ryzykami i kontrolami, które są dzielone między departamentami, jednostkami biznesowymi oraz geograficznie
- Wdrożenie jednolitego i uproszczonego podejścia do ERM

Platforma OpenPages obejmuje zestaw usług, które wspierają wszystkie w niej zawarte rozwiązania. Usługi te pokrywają podstawowe moduły rozwiązania OpenPages. Należą do nich:

- Elastyczna konfiguracja
- Workflow na poziomie organizacji
- Zarządzanie zawartością
- Ankiety i oceny
- Import / eksport
- Zintegrowane interfejsy i raportowanie
- Zarządzanie dokumentami
- Umiędzynarodowienie
- Bezpieczeństwo oparte na rolach
- Wielopoziomowa hierarchia biznesowa



Platforma OpenPages



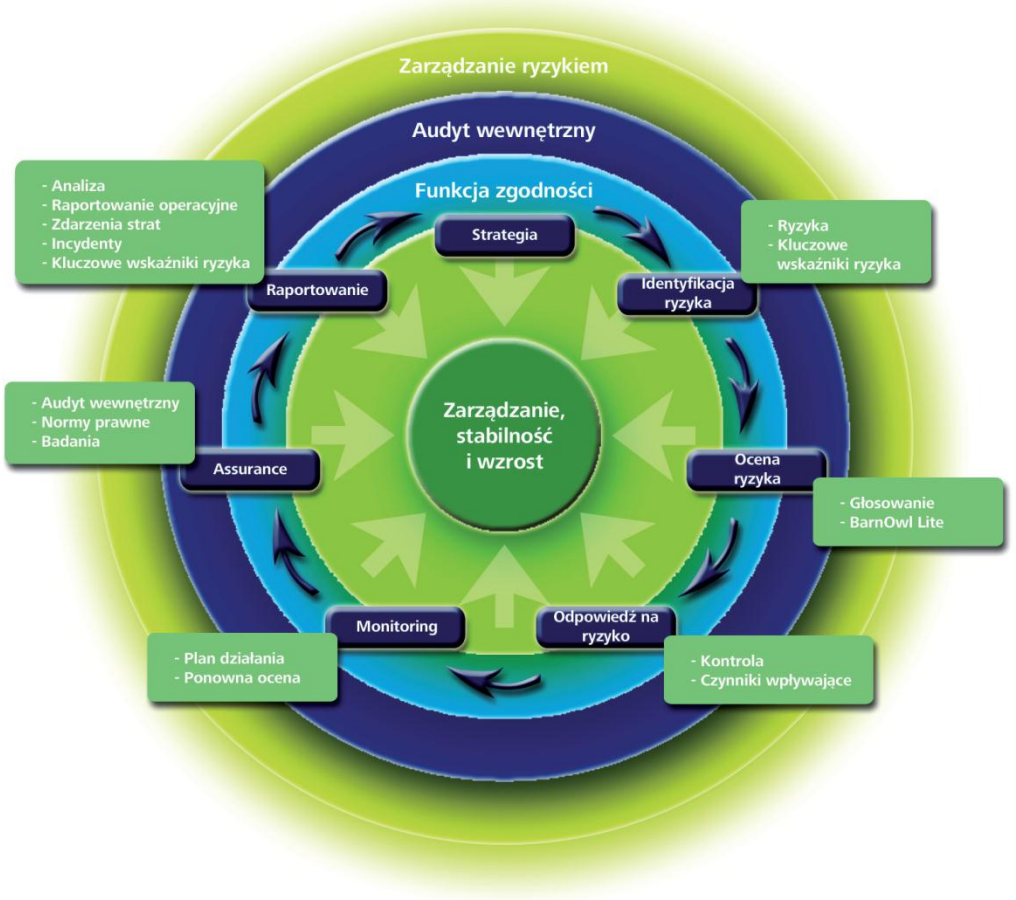
Istnieje gotowa prekonfigurowana platforma Open Pages Risk Intelligence Platform przygotowana we współpracy z Deloitte.

- System prekonfigurowany, umożliwia szybki start -‘ERM w pudełku’
- Zawiera wiele wbudowanych dobrych praktyk, standardów i semi-standardów (np. ITIL, Cobit, ISO, …)
- Pozwala na błyskawiczne wdrożenie i rozpoczęcie wykorzystywania wiedz i danych zgromadzonych w systemie
- Oparta na sprawdzonej i uznanej metodyce ERM – Risk Intelligence

Platforma BarnOwl

Czym jest BarnOwl?

- Jest w pełni zintegrowanym rozwiązaniem do zarządzania ryzykiem, audytu wewnętrznego ora zapewnienia zgodności
- Wspiera i umacnia najlepsze praktyki dotyczące struktur ERM i Audytu Wewnętrznego, włącznie : regulacjami, aktami prawnymi czy strukturami ryzyk takimi jak Standardy Audytu Wewnętrzneg Basel II, King III, Turnbull, AS/NZS 4360, ISO31000, COSO, CoCo, Cobit
- Został opracowany przez specjalistów w dziedzinie zarządzania ryzykiem, kontroli wewnętrznej i audytu wewnętrznego, którzy zapewniają, że metodologie najlepszych praktyk ich struktury są i będą wspierane przez oprogramowanie



- Wdrożony w ponad 50 dużych firmach lokalnych i międzynarodowych, wykorzystywane przez ponad 60 departamentów z sektora publicznego

Nie uprawiamy grzybów …

Zasada #5: Organy zarządcze oraz nadzorcze (np. Zarząd, Komitet Audytu, itp.) posiadają ***odpowiedni wgląd*** *w* ***przejrzyste*** *praktyki związane z zarządzaniem ryzykiem w organizacji i wywiązują się z własnych zadań w tym zakresie*

- Zarządy a nierzadko RN lub Komitety Audytowe, traktują ryzyko jak uprawę grzybów – „… dobrze zrobi im jakieś ciemne miejsce, najlepiej gdzieś głęboko w piwnicy„
- Wobec międzynarodowych i krajowych regulacji oraz standardów, organy nadzorcze i kierownicze przedsiębiorstwa mają jednoznacznie zdefiniowaną rolę w procesie zarządzania jak i ujawniania ryzyka:
    - Zapewnić wdrożenie odpowiednich miar zarządzania ryzykiem zanim ryzyko się zmaterializuje
    - Inwentaryzować i oceniać zarówno ryzyko jak i wdrożone strategie zarządzania
    - Zmotywować i zaangażować kierownictwo niższego szczebla do dyskusji o ryzyku, scenariuszach, szansach a także zagrożeniach i możliwych środkach zaradczych
    - Ustanawiać i weryfikować apetyt na ryzyko
    - Zorganizować proces niezależnego zapewnienia
    - Raportować zarządzanie ryzykiem

A ryzykiem to zajmujemy się w piątki …

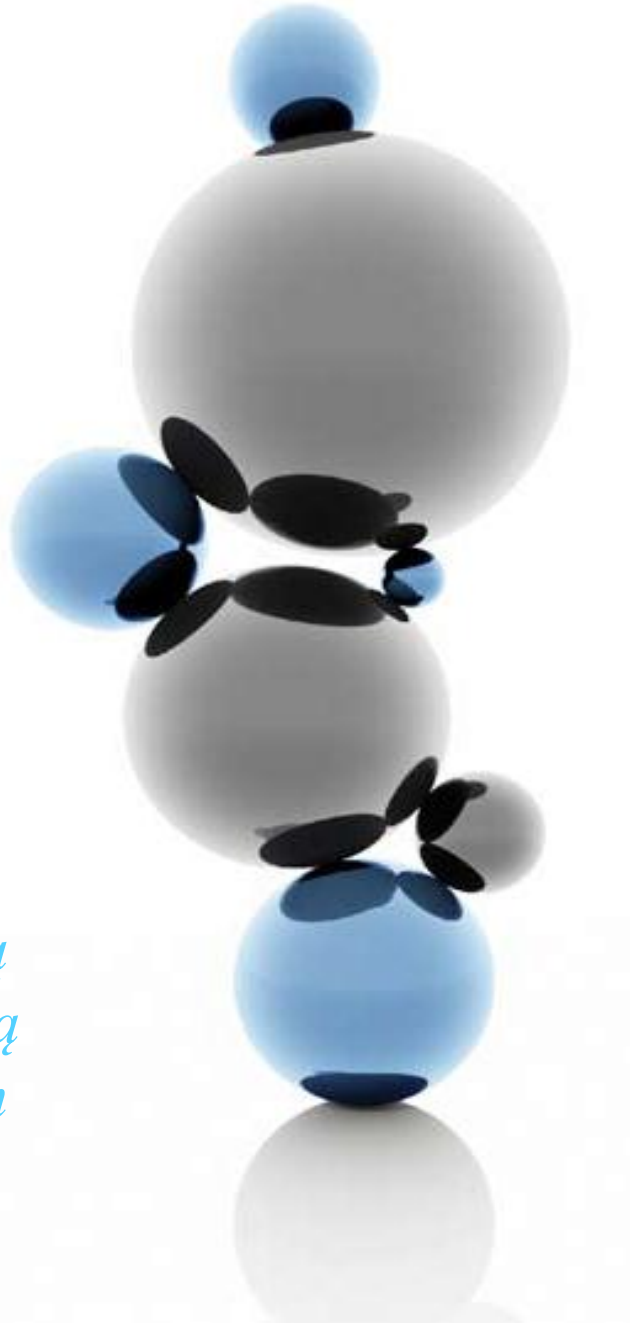
- Ścisłe kierownictwo ma jasno zdefiniowaną rolę i odpowiedzialność: zadaniem jest zainspirować i motywować pracowników na wszystkich szczeblach do myślenia o ryzyku - **zadaniem Kierownictwa jest ustanowić kulturę zarządzania ryzykiem**
- Odpowiednim centrum dowodzenia może być komitet ryzyka na poziomie Zarządu – platforma integracji zarządzania ryzykiem i strategii, ustanawiania polityki i apetytu na ryzyko

*Zasada #6: **Ścisłe kierownictwo** organizacji jest **odpowiedzialne** za opracowanie, wdrożenie i utrzymanie efektywnego programu zarządzania ryzykiem*

Wspieramy zarządzanie ryzykiem …

Zasada #7: Jednostki organizacyjne (departamenty, działy, itd.) są ***odpowiedzialne*** *za wykonywanie swoich zadań oraz zarządzanie ryzykami, które ponoszą – zgodnie z zasadami zarządzania ryzykiem* ***określonymi*** *przez* ***kierownictwo*** *organizacji*

Zasada #8: Określone funkcje w organizacji (np. finanse, komórka obsługi prawnej, HR, itd.) mają ***istotny*** *wpływ na jej funkcjonowanie i dostarczają* ***wsparcia*** *pozostałym jednostkom organizacyjnym w zakresie zarządzania ryzykiem*



Niezależne zapewnienie daje komfort …

Zasada #9: Określone funkcje dostarczają obiektywnego ***zapewnienia*** *oraz monitorują program* ***zarządzania ryzykiem*** *w organizacji, raportują jego* ***efektywności*** *do organów* ***nadzorczych, zarządczych*** *oraz* ***kierownictwa***

- Zadaniem audytu, ryzyka, zgodności, bezpieczeństwa, jest dostarczenie zarządzającym komfortu (zapewnienia), że kontrola i zarządzanie ryzykiem działają skutecznie i zgodnie z intencją
- Ważne jest aby ciągle monitorować, czy funkcje te pozostają w odpowiedniej (dla danej organizacji) niezależności od zarządzania operacyjnego i biznesu
- Potencjalne dodatkowe zadania:
  - Wizjoner: ocenia nie tylko stan aktualny ale próbuje oszacować także stan przyszły szans i zagrożeń
  - Dietetyk: określa, czy aktualny poziom ryzyka odpowiada apetytowi
  - Agregator: ocenia, czy organizacja w sposób odpowiedni ocenia interakcje ryzyk
  - Optymalizator: poszukuje środków eliminujących brak efektywności
  - Champion: zwolennik zarządzania ryzykiem związanym z potencjalną nagrodą
  - Adwokat: zwraca uwagę na ryzyka, których zarządzanie wymaga dodatkowych zasobów
  - Ekspert: dostarcza głębokiej eksperckiej wiedzy w poszczególnych obszarach wiedzy
  - Złota rączka: angażuje się w rozwiązywanie problemów

Kontakt

Mariusz Warych
Dyrektor
Dział Zarządzania Ryzykiem Deloitte
E-mail: mwarych@deloittece.com
Tel.: 22 511 09 19

Lech Dąbrowski
Starszy Manager
Dział Zarządzania Ryzykiem Deloitte
E-mail: ldabrowski@deloittece.com
Tel.: 22 511 01 58
Kom.: 693 150 490