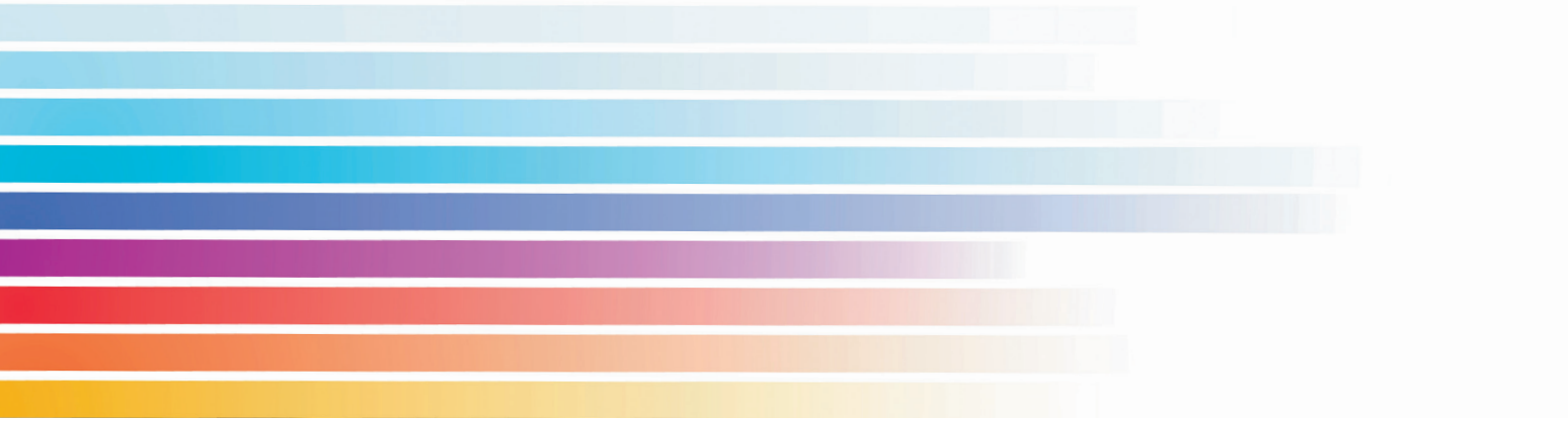
PIU

Polska Izba Ubezpieczeń

# Audyt – Compliance – Zarządzanie Ryzykiem – Aktuariat

Modele współpracy w zakładach ubezpieczeń



KPMG

cutting through complexity

Listopad 2013

PIU

Polska Izba Ubezpieczeń

# Audyt – Compliance – Zarządzanie Ryzykiem – Aktuariat

## Modele współpracy w zakładach ubezpieczeń

Autorzy opracowania – członkowie Podkomisji ds. Audytu i Kontroli Wewnętrznej PIU, pracownicy firmy KPMG oraz przedstawiciele Urzędu Komisji Nadzoru Finansowego

Jolanta Antczak
Katarzyna Jenerał
Ewa Kornacka
Jerzy Lenard
Robert Popadyniec
Bogusław Rajca
Beata Sambora
Wojciech Stasiak
Elżbieta Szambelan-Bakuła
Aneta Tomaszkiewicz
Anna Wawrzeniecka
Tomasz Wiącek
Artur Chądzyński
Radosław Kowalski
Piotr Wrzesiński – sekretarz

Listopad 2013

PIU
Polska Izba Ubezpieczeń

ul. Wspólna 47/49
00–684 Warszawa
tel. +48 22 420 51 05 (06)
fax +48 22 420 51 07
e-mail: office@piu.org.pl
www.piu.org.pl

# Spis treści

Szanowni Państwo,

Podkomisja ds. Audytu i Kontroli Wewnętrznej działająca w ramach Komisji Ekonomiczno-Finansowej Polskiej Izby Ubezpieczeń przygotowała na potrzeby rynku ubezpieczeniowego broszurę pt.: „Audyt – Compliance – Zarządzanie Ryzykiem – Aktuariat. Modele współpracy w zakładach ubezpieczeń". Prezentowane opracowanie przedstawia proponowane rozwiązania wypracowane na bazie opinii wszystkich stron biorących udział w jego tworzeniu, a mianowicie: członków Podkomisji ds. Audytu i Kontroli Wewnętrznej PIU, przedstawiciela Urzędu Komisji Nadzoru Finansowego oraz ekspertów KPMG.

Implementacja dyrektywy Solvency II niesie za sobą potrzebę wdrożenia w zakładach ubezpieczeń skutecznego systemu zarządzania, który zapewnia prawidłowe i ostrożne zarządzanie prowadzoną działalnością[1]. Wymagania te odnoszą się w szczególności do funkcji zarządzania ryzykiem, compliance, aktuarialnej oraz audytu wewnętrznego. Prezentowany materiał ma na celu pomoc w dostosowaniu organizacji zakładu ubezpieczeń do tych nowych wymagań. Osiągnąć to można poprzez pełne zrozumienie zadań poszczególnych funkcji oraz relacji między nimi, obecnych realiów ich funkcjonowania w organizacji oraz określenie najbardziej skutecznego sposobu działania w przyszłości.

Jednym z podstawowych zadań stojących przed zakładami ubezpieczeń jest jasne określenie zakresu odpowiedzialności poszczególnych funkcji oraz wypracowanie szczegółowych zasad współpracy pomiędzy nimi. Opracowanie przedstawia proponowane przez autorów modelowe role funkcji zarządzania ryzykiem, compliance, aktuariatu i audytu wewnętrznego oraz propozycje organizacji współpracy między nimi w taki sposób, aby mogły one uzupełniać swoje działania i polegać wzajemnie na ich wynikach.

1 Art. 41 ust. 1 Dyrektywy Parlamentu Europejskiego i Rady 2009/138/WE z dnia 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II).

# 1. System zarządzania ryzykiem

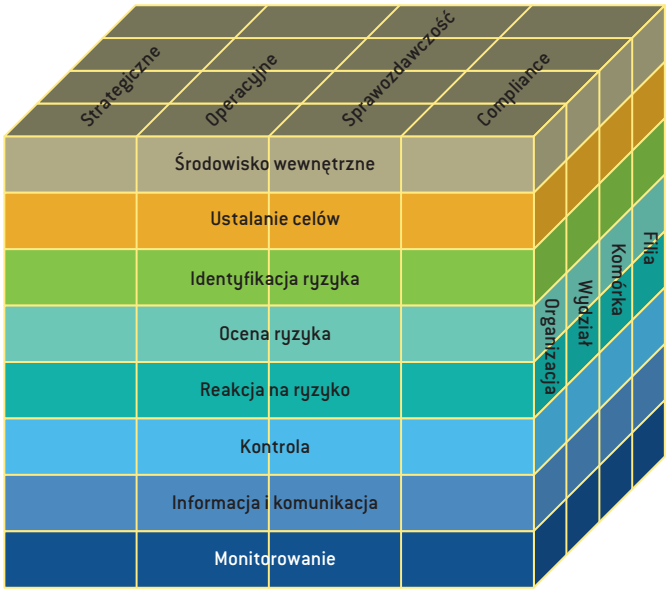
Generalną zasadą dla wszystkich zakładów ubezpieczeń jest utworzenie takiego systemu zarządzania ryzykiem, który będzie spójny wewnętrznie i będzie wspomagał kierownictwo w podejmowaniu kluczowych decyzji oraz pomagał identyfikować wszelkiego rodzaju istotne, z perspektywy realizacji celów strategicznych, zagrożenia i nieprawidłowości.

Przedstawiony poniżej model kompleksowego zarządzania ryzykiem COSO II, opracowany przez The Committee of Sponsoring Organizations of the Treadway Commission, łączy cele jednostki z procesem zarządzania ryzykiem na wszystkich poziomach organizacyjnych.

Model COSO II zakłada, że cele każdej organizacji powinny być określone w czterech wymiarach:

- Strategicznym – zapewnienie zgodności celów strategicznych na wszystkich poziomach organizacyjnych, wsparcie misji firmy i odzwierciedlenie wyboru kierownictwa w sprawie sposobu tworzenia wartości dla interesariuszy organizacji;
- Działalności operacyjnej – zapewnienie efektywności działalności organizacji, w tym celów operacyjnych i finansowych, wydajne wykorzystywanie zasobów organizacji, obejmujące wyniki, zyski, zabezpieczenie zasobów przed ich stratą;
- Sprawozdawczości – jakość i terminowość raportowania finansowego i niefinansowego (wewnętrzne i zewnętrzne);
- Compliance – przestrzeganie prawa i regulacji.

**Rysunek 1. Model COSO II kompleksowego zarządzania ryzykiem**




*Źródło: „Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa", www.coso.org.*

W powyższy model wpisują się wymagania Solvency II, które rekomendują, by zakłady ubezpieczeń dysponowały skutecznym systemem zarządzania ryzykiem, który będzie wspomagał podejmowanie przez przedsiębiorstwo kluczowych decyzji. System powinien obejmować przejrzystą strukturę organizacyjną z wyraźnym podziałem odpowiedzialności, a także zapewniać sprawny przepływ informacji.

Wdrożenie kompleksowego systemu zarządzania ryzykiem związane jest z wprowadzeniem całościowego rozwiązania, opartego na systematycznym podejściu do identyfikacji, kategoryzacji i optymalizacji wszystkich grup ryzyka, na jakie narażone jest zakład ubezpieczeń, w celu budowy wartości firmy.

Kompletny system zarządzania ryzykiem obejmuje następujące elementy:

- Politykę i procedury definiujące proces zarządzania ryzykiem i jego komponenty;
- Zasady nadzoru nad procesem zarządzania ryzykiem;
- Zasady oceny ryzyka;
- Zasady agregacji i kwantyfikacji ryzyka;
- Zasady raportowania i monitorowania ryzyka;
- Proces optymalizacji wykorzystania mechanizmów kontrolnych służących ograniczaniu ryzyka.

Dodatkowo w zakładzie ubezpieczeń system powinien uwzględniać:

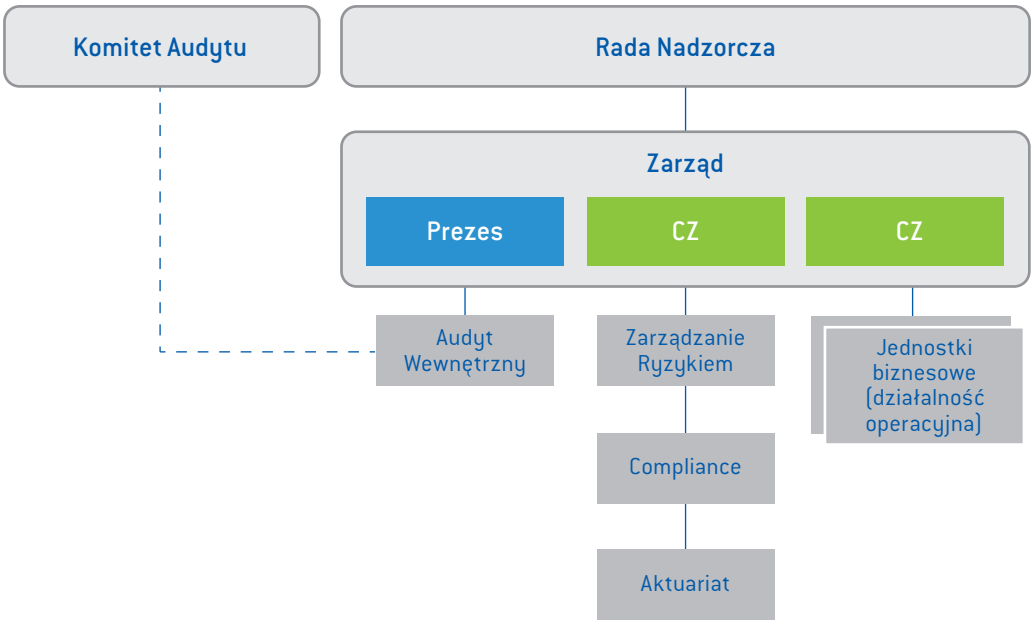
- Podejście do oceny ryzyka przyjmowanego do ubezpieczenia i tworzenie rezerw;
- Zarządzanie aktywami i pasywami;
- Zarządzanie płynnością i ryzykiem koncentracji;
- Zarządzanie ryzykiem operacyjnym;
- Reasekurację i inne techniki ograniczania ryzyka.

Rola właściciela procesu zarządzania ryzykiem, zgodnie z prezentowanym podejściem, jest następująca:

- Powiązanie zarządzania ryzykiem ze strategią zakładu ubezpieczeń;
- Opracowanie procedur zarządzania ryzykiem;
- Doradzanie i koordynowanie działań właścicieli biznesowych;
- Racjonalizacja i usystematyzowanie procesu oceny ryzyka i raportowania;
- Nadzorowanie, monitorowanie i koordynowanie działań właścicieli ryzyk w procesie zarządzania ryzykiem;
- Współpraca z zarządem w zakresie działań w obszarze zarządzania ryzykiem.

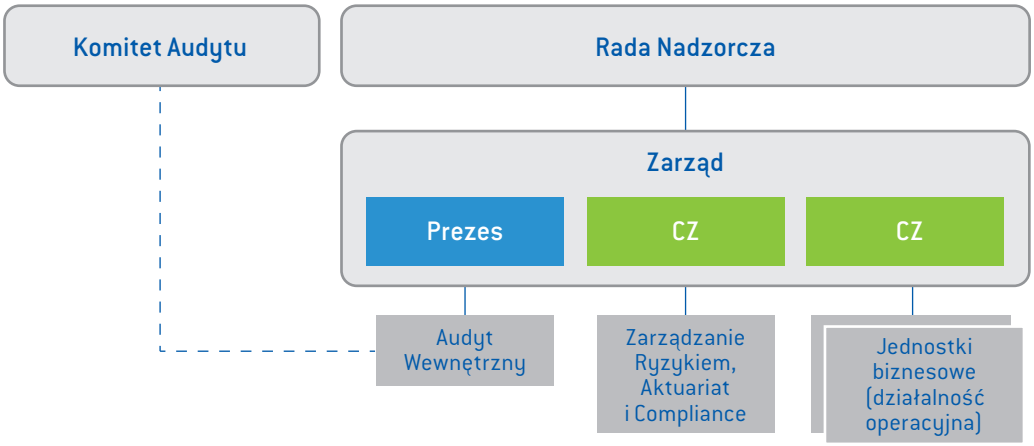
Przykładowe struktury organizacyjne w zakładzie ubezpieczeń przedstawiają poniższe diagramy:

**Rysunek 2. Model 1 – przykładowa struktura organizacyjna**



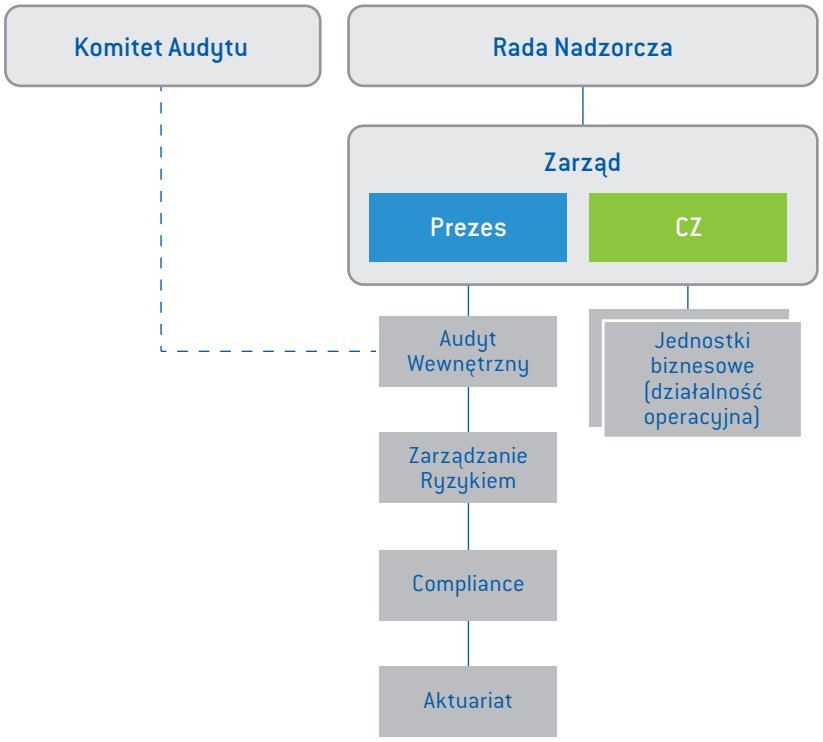

*Źródło: Opracowanie własne.*

**Rysunek 3. Model 2 – przykładowa struktura organizacyjna**




*Źródło: Opracowanie własne.*

Rysunek 4. Model 3 – przykładowa struktura organizacyjna




*Źródło: Opracowanie własne.*

## 2. Trzy linie obrony i ich znaczenie w systemie zarządzania – model

Zgodnie z dyrektywą Parlamentu Europejskiego w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Solvency II), funkcja audytu wewnętrznego wraz z funkcją zarządzania ryzykiem, funkcją compliance oraz funkcją aktuarialną wchodzi w skład systemu zarządzania w zakładzie ubezpieczeń. Funkcje należące do systemu zarządzania w zakładzie ubezpieczeń uważa się za kluczowe i podstawowe. W przypadku funkcji audytu wewnętrznego sformułowano szczególne wymagania dotyczące niezależności, wskazując, że ta sama osoba lub jednostka organizacyjna nie może łączyć wykonywania funkcji audytu wewnętrznego z innymi funkcjami. Wynika to z faktu, iż do zadań audytu należy obiektywna ocena adekwatności i efektywności systemu kontroli wewnętrznej i innych elementów systemu zarządzania ryzyka, więc jakiekolwiek łączenie tych funkcji stałoby w sprzeczności z ww. wymogiem.

Relacje funkcji audytu wewnętrznego z funkcją compliance i funkcją zarządzania ryzykiem, jak również innymi, powoływanymi w ramach zakładu ubezpieczeń dla wsparcia procesu zarządzania ryzykiem, prezentuje model trzech linii obrony.

Zgodnie z założeniami modelu, funkcja audytu wewnętrznego stanowi trzecią linię obrony. Pozostałe, opisane poniżej funkcje (zarządzania ryzykiem, aktuarialna oraz compliance) działają w ramach drugiej linii obrony.

Model struktury organizacyjnej w procesie zarządzania ryzykiem, jak również podział zadań pomiędzy poszczególne funkcje, przedstawiony został w ramach poniższego schematu:

**Rysunek 5. Model trzech linii obrony**

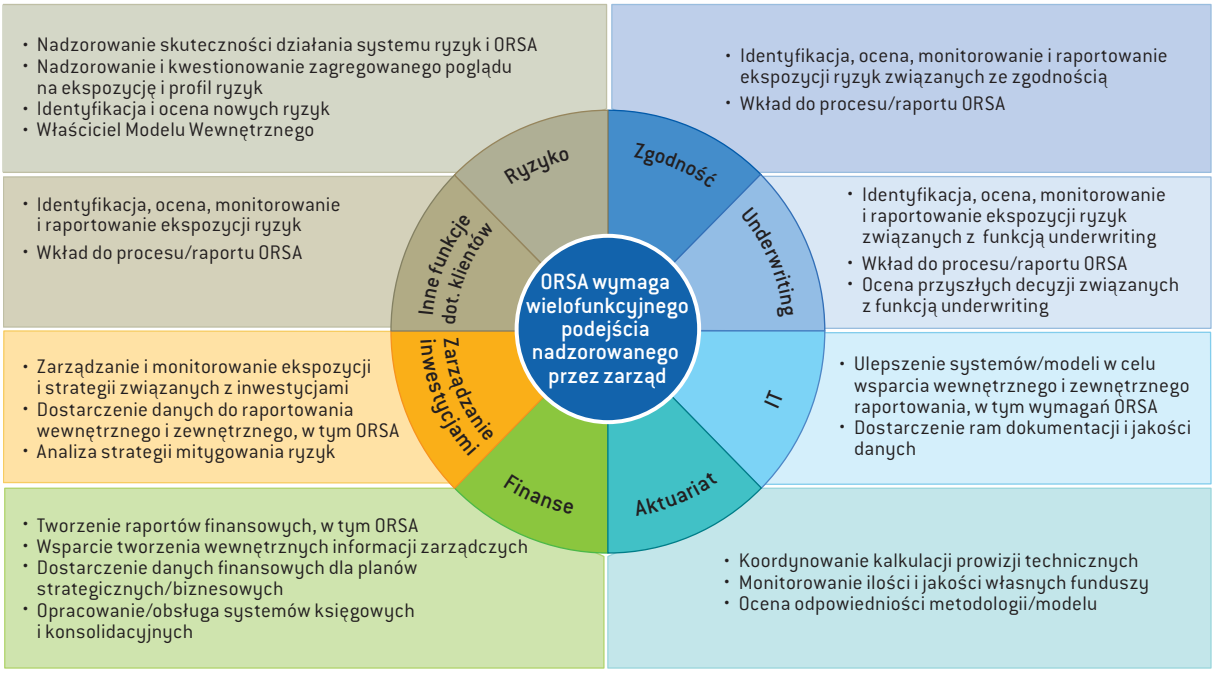

*Źródło: Opracowanie własne.*

Zgodnie z modelem trzech linii obrony, funkcje należące do drugiej linii obrony należy traktować jako funkcje bezpośrednio wspierające działania operacyjne, których zadaniem jest spojrzenie na ryzyka z perspektywy całej organizacji i inicjowanie określonych działań zarządczych związanych z zarządzaniem ryzykiem i systemem kontroli wewnętrznej. Z kolei rolą audytu jest całościowe spojrzenie na organizację, niezależna ocena działań podejmowanych przez pierwszą i drugą linię obrony, identyfikacja szans i zagrożeń w celu zapewnienia synergii oraz poprawy efektywności procesów zarządzania ryzykiem i kontroli wewnętrznej.

W ramach trzech linii obrony specyficznym obszarem dla zakładów ubezpieczeń jest także proces własnej oceny ryzyka i wypłacalności ORSA – Own Risk and Solvency Assessment. W ramach tego procesu wszystkie funkcje powinny być zaangażowane w efektywny i skuteczny przebieg

procesu. Poniższe schematy prezentują zarówno czynności dostarczane przez poszczególne funkcje, jak i podział obowiązków w ramach trzech linii obrony.

### Rysunek 6. ORSA – podział obowiązków




*Źródło: Opracowanie własne.*

### Rysunek 7. ORSA – model trzech linii obrony

| ORSA | Zarząd | Biznes | Finanse (w tym Aktuariat) | Zarządzanie ryzykiem | Audyt wewnętrzny |
|---|---|---|---|---|---|
| | *Pierwsza linia obrony* | | | *Druga linia obrony* | *Trzecia linia obrony* |
| Biznesplan | Ostateczna odpowiedzialność | **Właściciel procesu** | Odpowiedzialni za rezultaty | Odpowiedzialni za rezultaty | Niezależna ocena |
| Plan finansowy | Ostateczna odpowiedzialność | Odpowiedzialni za rezultaty | **Właściciel procesu** | Odpowiedzialni za rezultaty | Niezależna ocena |
| Ocena ryzyk niefinansowych | Ostateczna odpowiedzialność | Odpowiedzialni za rezultaty | Odpowiedzialni za rezultaty | **Właściciel procesu** | Niezależna ocena |
| Ocena ryzyk finansowych | Ostateczna odpowiedzialność | – | Odpowiedzialni za rezultaty | **Właściciel procesu** | Niezależna ocena |
| Określenie apetytu na ryzyko | Ostateczna odpowiedzialność | Odpowiedzialni za rezultaty | Odpowiedzialni za rezultaty | **Właściciel procesu** | Niezależna ocena |
| Kalkulacja kapitałowego wymogu wypłacalności (SCR) | Ostateczna odpowiedzialność | – | Odpowiedzialni za rezultaty | **Właściciel procesu** | Niezależna ocena |
| Identyfikacja ryzyka | Ostateczna odpowiedzialność | – | Odpowiedzialni za rezultaty | **Właściciel procesu** | Niezależna ocena |

*Źródło: Opracowanie własne.*

Powyższe modele wskazują również na interakcję i współpracę między poszczególnymi liniami obrony. Międzynarodowe Standardy Praktyki Zawodowej Audytu Wewnętrznego podkreślają rolę funkcji audytu wewnętrznego w koordynowaniu działań zarówno z wewnętrznymi, jak i zewnętrznymi dostawcami usług poświadczających i doradczych. Koordynacja ta ma na celu uzyskanie pełnej efektywności działań, m.in. poprzez zapewnienie odpowiedniego zakresu audytu i uniknięcie dublowania wysiłków oraz zapewnienie, że wszystkie istotne ryzyka zostały zidentyfikowane i odpowiednio zaraportowane do zarządu, Komitetu Audytu lub rady nadzorczej[1].

## 3. Solvency II – wymogi

Filar I Solvency obejmuje kwantyfikowalne rodzaje ryzyka działania zakładu ubezpieczeń i opracowanie wymagań kapitałowych uwzględniających wszystkie mierzalne rodzaje ryzyka działalności zakładu ubezpieczeń, a także określenie zasad i zakresu stosowania tak zwanych modeli wewnętrznych oceny ryzyka zakładu ubezpieczeń.[2] Filar II definiuje wymagania dotyczące zarządzania ryzykiem organizacji. Dodatkowo, filar II określa wymagania organów nadzoru w odniesieniu do zakładów ubezpieczeń, a w szczególności w zakresie zarządzania ryzykiem, i systemu kontroli wewnętrznej. Filar III obejmuje narzędzia samoregulacji rynku poprzez tworzenie warunków jego transparentności, określenie obowiązków informacyjnych oraz wypracowanie odpowiednich rozwiązań w zakresie rachunkowości[3].

Wymogi dyrektywy Solvency II związane z zarządzaniem ryzykiem korporacyjnym w dużym stopniu wpływają na rynek ubezpieczeniowy. Solvency II wymaga formalnego podejścia do zarządzania, organizacji i podejmowania decyzji, co zmusza zakłady ubezpieczeń do wdrożenia kultury i praktyk zarządzania ryzykiem w całej organizacji oraz przeprowadzania bieżącej analizy, a także systematycznego podejścia do zarządzania ryzykiem.

Na poniższym wykresie wyszczególniono najważniejsze aspekty filaru II dyrektywy Solvency II. Zgodnie z ramami dyrektywy, wymagania jakościowe oparte są na trzech głównych założeniach:

1. Odpowiedzialność kluczowego kierownictwa za zarządzanie ryzykiem;
2. Jasno określona strategia ryzyka, która jest spójna ze strategią biznesową;
3. Bieżące zarządzanie i monitorowanie poziomu ryzyk.

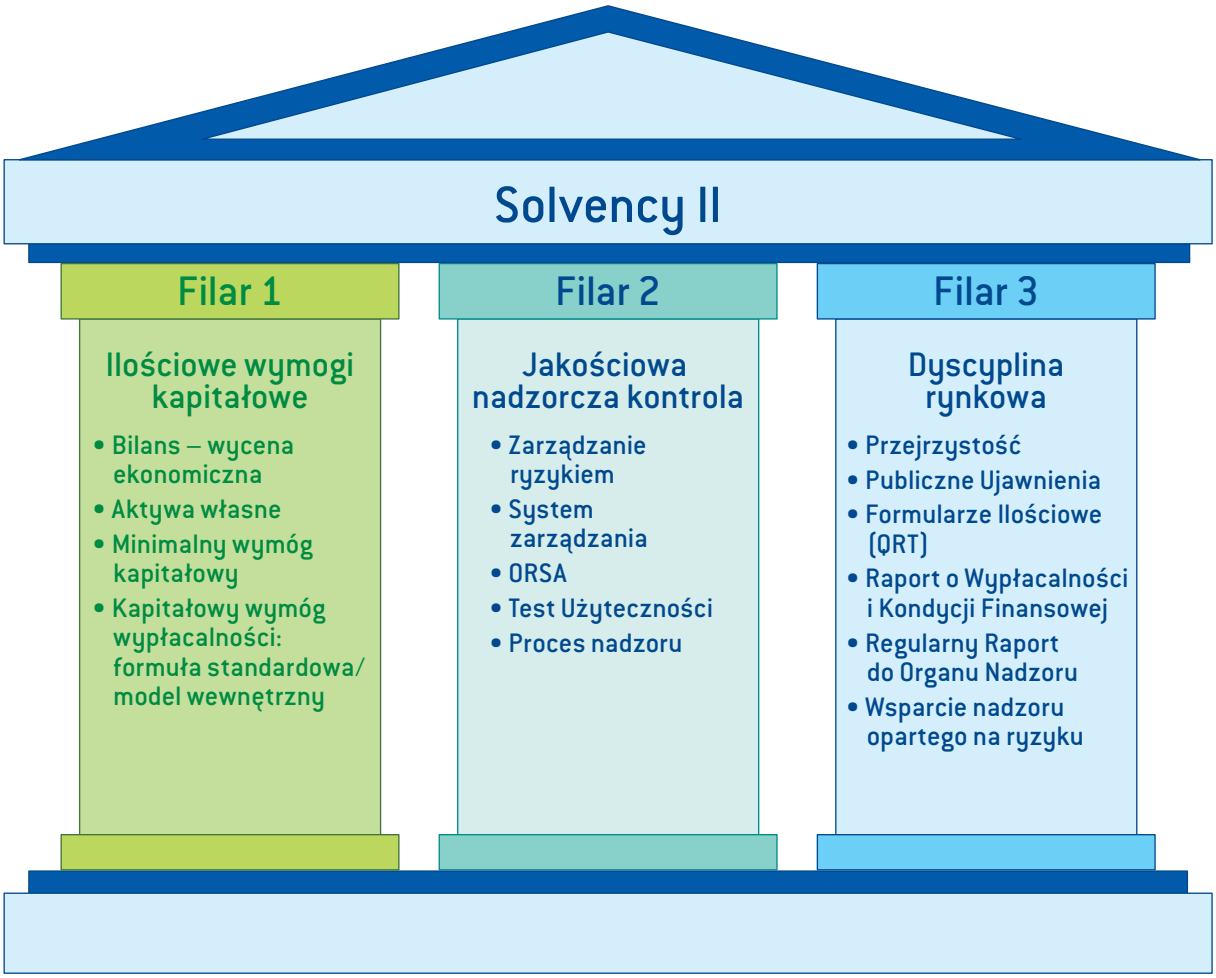
---

1 *Standard 2050 oraz poradniki,* ang. *Practice advisories, 2050–1, 2050–2.*

2 http://www.knf.gov.pl/o_nas/wspolpraca_miedzynarodowa/unia/regulacje_i_dokumenty_powiazane/historia_zalozenia_projektu.html

3 Ibidem.

Rysunek 8. Struktura Solvency II

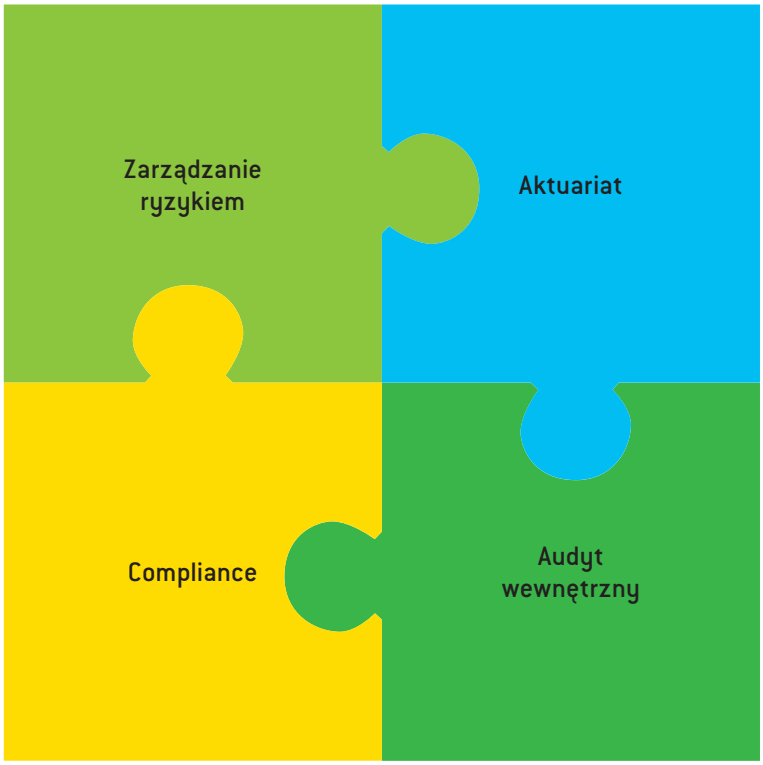



*Źródło: Opracowanie własne.*

Zgodnie z Solvency II, zakłady ubezpieczeń ustanawiają i wpisują w poszczególne wymiary modelu COSO II cztery kluczowe funkcje, składające się na system zarządzania:

- Funkcja zarządzania ryzykiem;
- Funkcja compliance;
- Funkcja aktuarialna;
- Funkcja audytu wewnętrznego.

**Rysunek 9. Kluczowe funkcje w systemie zarządzania**




*Źródło: Opracowanie własne.*

Głównym problemem z zakresu skutecznej współpracy wszystkich przywołanych funkcji w ramach kompleksowego systemu zarządzania jest takie ustanowienie poszczególnych komórek, by zakres ich obowiązków nie powodował wzajemnych konfliktów.

Dyrektywa Solvency II nie precyzuje, w jakiej formie organizacyjnej powinny być wdrożone poszczególne funkcje. Dana funkcja – z wyjątkiem funkcji audytu wewnętrznego – nie musi, ale może być utożsamiana z wydzieloną jednostką organizacyjną – pod warunkiem, że nie zostaną naruszone zasady niezależności ani nie dojdzie do konfliktu interesów. W mniejszych, mniej złożonych organizacjach, poszczególne zadania mogą być włączone w inne obszary działalności. Spotykane są na przykład rozwiązania, gdzie funkcja compliance realizowana jest przez dział prawny. Należy jednak podkreślić, iż podział obowiązków, jak i zakres odpowiedzialności powinien być dobrze udokumentowany w postaci odpowiednich polityk i procedur. W szczególności uważamy za najbardziej właściwe opisanie całości procesu zarządzania ryzykiem i jego komponentów w zakładzie ubezpieczeń, a następnie naniesienie na zdefiniowany proces zakresu odpowiedzialności poszczególnych komórek organizacyjnych. Kolejnym krokiem powinna być eliminacja ewentualnych powielonych zadań i zakresów odpowiedzialności oraz odpowiednie przypisanie odpowiedzialności za wszelkie pozostałe funkcje systemu zarządzania ryzykiem.

Co oczywiste, za poszczególne funkcje powinny odpowiadać osoby posiadające odpowiednią wiedzę (*fit and proper*), kwalifikacje i doświadczenie. Jednocześnie dla zapewnienia właściwego poziomu niezależności i ograniczenia ryzyka konfliktu interesów osoby stojące na czele każdej z tych funkcji mogą raportować bezpośrednio do zarządu, Komitetu Audytu lub rady nadzorczej.

Zapewnienie niezależności poszczególnych funkcji i jednoczesne niedopuszczenie do potencjalnego konfliktu interesów jest jednym z najtrudniejszych zadań stojących przed organizacją. W celu zapewnienia operacyjnej niezależności poszczególnych funkcji systemu zarządzania ryzykiem, zakład ubezpieczeń powinien zadbać, by odpowiedni podział obowiązków z zakresu zarządzania ryzykiem został określony na każdym poziomie zarządzania – także na poziomie zarządu, szczególnie jeśli chodzi o oddzielenie funkcji operacyjnych od kontrolnych.

W celu zagwarantowania operacyjnej niezależności zakład ubezpieczeń powinien zapewnić warunki takie, aby:

- W przypadku, gdy zostanie zidentyfikowany konflikt pomiędzy poszczególnymi funkcjami, potencjalnie zagrażający całościowemu procesowi zarządzania ryzykiem, osoba odpowiedzialna za jego identyfikację była w stanie podjąć decyzję, czy łączenie danych funkcji jest nadal uzasadnione i możliwe w kontekście istniejących lub możliwych do wprowadzenia mechanizmów kontrolnych.
- W przypadku, gdy poszczególne funkcje łączone są w jednej komórce organizacyjnej i pojawia się konflikt interesów, osoba, która zidentyfikowała dany konflikt, miała bezpośredni dostęp do najwyższego kierownictwa, tak by możliwa była właściwa reakcja ze strony władz zakładu ubezpieczeń.
- Na osobę identyfikującą problem niezależności lub konflikt interesów nie były wywierane wpływy mające na celu rozmycie lub złagodzenie poczynionych obserwacji, gdyż może to prowadzić do niewłaściwej percepcji identyfikowanego zagrożenia i reakcji najwyższego kierownictwa.

Zarówno regulacje zewnętrzne (Solvency II), jak i ogólne praktyki wyraźnie pokazują, iż po uwzględnieniu powyższych zasad sprawowanie przez osobę lub komórkę/dział więcej niż jednej funkcji nie jest zagrożeniem dla działalności operacyjnej, przy czym możliwość łączenia funkcji nie dotyczy funkcji audytu wewnętrznego, która zawsze musi działać jako odrębna i niezależna komórka.

# 4. Rola funkcji audytu wewnętrznego, funkcji compliance, funkcji zarządzania ryzykiem i funkcji aktuarialnej w systemie zarządzania

## 4.1. Trzecia linia obrony

*Funkcja audytu wewnętrznego*

Funkcja audytu wewnętrznego wspiera kierownictwo w monitorowaniu i ocenie skuteczności i adekwatności systemu kontroli wewnętrznej i innych elementów systemu zarządzania ryzykiem. Obszar oddziaływania funkcji audytu wewnętrznego obejmuje wszystkie działania i procesy systemu zarządzania ryzykiem.

Funkcja audytu wewnętrznego bada i ocenia w sposób niezależny i obiektywny adekwatność i efektywność systemu kontroli wewnętrznej, w tym skuteczność zarządzania ryzykiem zakładu ubezpieczeń, w celu:

- Upewnienia się, że organizacja właściwie zdefiniowała cele procesów w kontekście celów przedsiębiorstwa;
- Oceny procesu identyfikacji ryzyk w zaprojektowanych i wdrożonych procesach;
- Oceny skuteczności zaprojektowanych i wdrożonych mechanizmów kontrolnych.

W związku z powyższym, funkcja audytu wewnętrznego musi być niezależna od wszystkich pozostałych funkcji w zakładzie ubezpieczeń i spełniać rolę trzeciej linii obrony w procesie zarządzania ryzykiem, czyli oceniającej poprawność zaprojektowania systemu i skuteczność jego funkcjonowania.

## 4.2. Druga linia obrony

*Funkcja zarządzania ryzykiem*

Istotną cechą działalności każdej organizacji, w tym zakładu ubezpieczeń, jest podejmowanie ryzyka. Ryzyko musi być właściwie zidentyfikowane, opisane, zmierzone, zredukowane lub zaakceptowane i, w końcu, kontrolowane w dopuszczalnych w ramach apetytu na ryzyko granicach. Celem procesu zarządzania ryzykiem jest ustanowienie kultury ryzyka w organizacji i znalezienie równowagi w działalności pomiędzy zyskiem a ryzykiem. Zarządzanie ryzykiem stanowi podstawę utworzenia właściwego ładu organizacyjnego – procesów oraz struktur wdrażanych przez kierownictwo dla uzyskania odpowiedniego przepływu informacji, zarządzania, kierowania oraz monitorowania działań nastawionych na realizację celów zakładu ubezpieczeń. Prawidłowe

wdrożenie funkcji zarządzania ryzykiem może pomóc zakładowi ubezpieczeń w poprawie jakości świadczenia usług i wykorzystaniu dostępnych możliwości. Może odgrywać aktywną rolę w zarządzaniu działalnością operacyjną, a także we wdrażaniu zmian, przed którymi stoi zakład ubezpieczeń. Proces ten stanowi narzędzie, które służy przedsiębiorstwu do osiągnięcia sukcesu.

Do głównych zadań funkcji zarządzania ryzykiem należą:

- Koordynacja zadań związanych z zarządzaniem ryzykiem na wszystkich szczeblach i we wszystkich obszarach działalności organizacji, odpowiedzialność za rozwój strategii, metod, procesów i procedur identyfikacji, oceny, monitorowania i kontroli zagrożeń.
- Przedstawienie ogólnej sytuacji ryzyka w zakładzie ubezpieczeń, uwzględnienie powiązań między poszczególnymi kategoriami ryzyka, stworzenie zagregowanego profilu ryzyka (UWAGA – funkcja zarządzania ryzykiem nie jest właścicielem ryzyk i mechanizmów kontroli – jest koordynatorem procesu);
- Jak najszybsze rozpoznawanie ryzyka i odpowiednie eskalowanie w organizacji;
- Doradzanie zarządowi w odniesieniu do zarządzania ryzykiem i wsparcie w wykorzystaniu systemu zarządzania ryzykiem w procesie podejmowania decyzji;
- Monitorowanie skuteczności systemu zarządzania ryzykiem;
- Propagowanie wewnątrz organizacji zarządzania ryzykiem, w tym wykorzystania systemu zarządzania ryzykiem poprzez działania mające na celu budowanie świadomości i edukację uczestników procesu podejmowania decyzji.

Tak jak zostało wspomniane we wcześniejszej części dokumentu, funkcja zarządzania ryzykiem nie musi być samodzielną funkcją i jej zadania mogą być wykonywane przez inne komórki. Sytuacja taka jest uzasadniona, gdy profil i skala działalności zakładu ubezpieczeń nie pozwalają na wydzielenie osobnej komórki oraz spełnione są następujące zasady:

- Zostaną opracowane i wdrożone odpowiednie polityki i procedury opisujące zakres obowiązków oraz definiujące ścieżkę raportowania do zarządu;
- Jednostka organizacyjna, do której zostanie przypisana odpowiedzialność za zarządzanie ryzykiem, nie będzie odpowiedzialna operacyjnie za inny obszar funkcjonowania zakładu ubezpieczeń – innymi słowy, **nie może być właścicielem ryzyka w procesach operacyjnych**, np. nie może być odpowiedzialna za zarządzanie inwestycjami, rozwój produktów ubezpieczeniowych, roszczenia, gwarancje, reasekurację, IT czy proces akwizycji.

Spotykanym w zakładach ubezpieczeń rozwiązaniem jest przypisanie odpowiedzialności za zarządzanie ryzykiem do funkcji aktuarialnej. Oczywiście, integracja taka może potencjalnie prowadzić do utraty niezależności osób odpowiedzialnych za zarządzanie ryzykiem w procesie oceny poprawności kalkulacji wypłacalności zakładu ubezpieczeń czy też rezerw techniczno-ubezpieczeniowych. Dlatego też procesy te powinny być oceniane przez inne komórki w ramach drugiej linii obrony.

*Funkcja compliance*

Funkcja compliance nie jest obecnie szerzej zdefiniowana w regulacjach prawnych dotyczących działalności ubezpieczeniowej, zakłady ubezpieczeń nie mają również obowiązku tworzenia komórki realizującej tę funkcję. Funkcja compliance została jednak przewidziana w art. 46 pkt. 1 dyrektywy Solvency II, według którego zakłady ubezpieczeń wprowadzają efektywny system kontroli wewnętrznej, a jednym z jego elementów jest kontrola zgodności z obowiązującym prawem, umowami i normami wewnętrznymi. Funkcja ta została także przewidziana w projekcie ustawy o działalności ubezpieczeniowej.

Do głównych zadań funkcji compliance należą:

- Identyfikacja i monitorowanie ryzyka wynikającego z nieprzestrzegania norm prawnych (do głównych obszarów prawa objętych wymaganiem compliance należą: Kodeks spółek handlowych, Ustawa o działalności ubezpieczeniowej, Regulacje rynku kapitałowego, Regulacje o przeciwdziałaniu praniu brudnych pieniędzy, Prawo konkurencji, Kodeks karny (przekupstwo, korupcja, przywłaszczenie, defraudacja, oszustwo etc.), regulacje IT i ochrona danych);
- Wczesne ostrzeganie: rozumiane jako ocena potencjalnego wpływu zmian pojawiających się w otoczeniu regulacyjnym na działalność zakładu ubezpieczeń (wytyczne, zalecenia Komisji Nadzoru Finansowego i Polskiej Izby Ubezpieczeń);
- Doradzanie zarządowi w sprawie przestrzegania przepisów przyjętych zgodnie z wytycznymi prawa, w tym wytycznymi dyrektywy Solvency II oraz w kwestiach nowych produktów, usług i rynków z punktu widzenia compliance;
- Identyfikowanie i opiniowanie wszelkich działań lub decyzji kierownictwa mogących powodować ryzyko niezgodności, wzrost ryzyka regulacyjnego lub ryzyka reputacji zakładu ubezpieczeń. W przypadku gdyby kwestie nie były niezwłocznie rozwiązywane, Compliance Oficer i kierownictwo powinno zastosować proces eskalacji adekwatny do danego ryzyka i zgodny z kulturą organizacji.

Funkcja compliance powinna mieć w każdym czasie bezpośredni dostęp do wszystkich działań w obszarze jej odpowiedzialności (zgodnie z lokalnymi prawami i regulacjami). Obejmuje to całą dokumentację, systemy (np. rejestr skarg, rejestr incydentów), informację udzielaną przez pracowników, członków zarządu, kadrę kierowniczą, co do których pracownicy odpowiedzialni za funkcję compliance mają podstawy sądzić, że są konieczne do efektywnej realizacji nałożonych na nich obowiązków.

Główne ograniczenia dotyczące funkcji compliance są takie same, jak dla funkcji zarządzania ryzykiem. Oznacza to, że funkcja compliance nie jest właścicielem ryzyka oraz muszą istnieć formalnie zaimplementowane procedury i polityki definiujące role oraz zakres odpowiedzialności tej funkcji. Dobrą praktyką jest, by osoba odpowiedzialna za zadania funkcji compliance posiadała wykształcenie prawnicze.

*Funkcja aktuarialna*

Do głównych zadań funkcji aktuarialnej należą:

- Koordynowanie wszelkich działań dotyczących wyceny rezerw techniczno-ubezpieczeniowych na potrzeby prawidłowego i bezpiecznego funkcjonowania zakładu ubezpieczeń, odpowiedzialność za rozwój właściwych metod, procesów i procedur, jakość statystyczną oceny aktuarialnej, jak również jakość wykorzystywanych danych i zatwierdzanie wyników oceny;
- Doradzanie zarządowi w sprawie rozwiązań w zakresie reasekuracji;
- Wsparcie funkcji zarządzania ryzykiem.

*Rola pozostałych funkcji w systemie zarządzania*

Złożoność zakładu ubezpieczeń i wzajemne przeplatanie się procesów realizowanych przez poszczególne funkcje, jak również potrzeba jasnego zdefiniowania odpowiedzialności za kwestie związane z zarządzaniem ryzykiem i kontroli powoduje, że coraz więcej zakładów ubezpieczeń, działając zgodnie z najlepszymi praktykami biznesowymi, decyduje się na powołanie dedykowanych funkcji odpowiedzialnych za koordynację działań odnoszących się do danego rodzaju ryzyka. Funkcje te definiowane są w ramach modelu trzech linii obrony. Najwyższe kierownictwo powołuje te funkcje, aby zapewnić, że pierwsza linia obrony jest zaprojektowana w odpowiedni sposób i działa zgodnie z przyjętymi założeniami. Służy to bezpośrednio budowaniu i podtrzymaniu zaufania ze strony klientów, partnerów biznesowych, pracowników, akcjonariuszy, jak również organów nadzoru.

Wśród tych funkcji, obok funkcji compliance czy funkcji zarządzania ryzykiem, można wymienić: **funkcję ds. bezpieczeństwa informacji** (odpowiada za zarządzanie programem bezpieczeństwa organizacji oraz compliance działania z regulacjami prawnymi w tym zakresie), **Administratora Bezpieczeństwa Informacji (ABI)** (nadzoruje kwestie związane z bezpieczeństwem przetwarzania danych osobowych, w tym zgodność tego procesu z obowiązującymi normami prawnymi), **funkcję inspektora jakości** (odpowiada za prawidłowe funkcjonowanie kontroli jakości w zakładzie ubezpieczeń), **funkcję ds. nadużyć** (odpowiada za zarządzanie procesem przeciwdziałania, wykrywania oraz wyjaśniania nadużyć), **funkcję zarządzania ciągłością działania i zarządzania kryzysowego** (odpowiada za nadzór nad procesem zarządzania ciągłością działania w organizacji oraz zapobieganie sytuacjom kryzysowym, reagowanie w przypadku ich wystąpienia, usuwanie ich skutków i odtwarzanie zasobów). Liczba funkcji powołanych przez poszczególne organizacje i wyznaczone w ich ramach zakresy odpowiedzialności zależą w dużej mierze od wielkości zakładów ubezpieczeń i złożoności procesów w nich zachodzących. W mniejszych zakładach ubezpieczeń pewne funkcje drugiej linii obrony mogą łączyć się z innymi funkcjami. Zadania wpisane w odpowiedzialność drugiej linii obrony nie powinny być realizowane w ramach funkcjonowania audytu wewnętrznego – ma to na celu zachowanie przez trzecią linię obrony niezależności i obiektywizmu.

# 5. Analiza stanu obecnego

W celu ustalenia obecnej praktyki dotyczącej sposobu organizacji i zasad działania funkcji audytu wewnętrznego, funkcji compliance oraz funkcji zarządzania ryzykiem wykorzystano zbiorcze odpowiedzi na wybrane pytania w ankiecie BION, dotyczące powyższych funkcji. Dane do analizy zostały udostępnione Polskiej Izbie Ubezpieczeń przez Komisję Nadzoru Finansowego. Odpowiedzi dotyczyły roku 2012 i pochodziły od 59 zakładów, tj. wszystkich działających na polskim rynku na dzień 31 grudnia 2012 r., z pominięciem oddziałów zagranicznych. Do zakładów przesłana została również ankieta z dodatkowymi, szczegółowymi pytaniami. Otrzymano 15 odpowiedzi, przy założeniu, że zakłady ubezpieczeń pochodzące z tej samej grupy kapitałowej udzielały wspólnej odpowiedzi. Wnioski z poniższej analizy można podzielić na trzy następujące części:

A. Funkcja audytu wewnętrznego
B. Funkcja compliance
C. Funkcja zarządzania ryzykiem

## 5.1. Funkcja audytu wewnętrznego

*a) Istnienie i zasady działania funkcji audytu wewnętrznego*

Funkcja audytu wewnętrznego istnieje w 55 zakładach ubezpieczeń. W 53 zakładach jest zorganizowana w postaci stanowiska lub komórki audytu. Z udzielonych odpowiedzi wynika również, że powszechną praktyką jest posiadanie dokumentacji dotyczącej audytu wewnętrznego – jej brak zadeklarowały jedynie 2 podmioty, natomiast 1 zakład uznał, że ten punkt go nie dotyczy. Dokumentacja ta obejmuje w szczególności proces wyboru audytowanego obszaru, proces przeprowadzania audytu, raportowanie wyników badania oraz wydawanie i monitorowanie rekomendacji i zaleceń po badaniu.

Jedynie 30 zakładów określiło natomiast konsekwencje niewykonania wydanych rekomendacji i zaleceń. Być może jest to uregulowane w procedurach dotyczących poszczególnych obszarów działalności zakładów, ponieważ 55 zakładów deklaruje monitorowanie i sporządzanie raportów odnośnie wykonywania rekomendacji i zaleceń audytowych (pozostałe nie udzieliły odpowiedzi na to pytanie).

*b) Niezależność funkcji audytu wewnętrznego*

Z odpowiedzi udzielonych przez zakłady wynika, że funkcja audytu wewnętrznego jest niezależna od innych funkcji operacyjnych. Jeśli przyjmiemy tę deklarację, oznacza to dobre przygotowanie

zakładów do spełnienia wymogów dyrektywy Solvency II. Jedynie w 2 zakładach funkcja audytu wewnętrznego jest zależna od innych funkcji, natomiast 4 zakłady nie udzieliły odpowiedzi na to pytanie.

*d) Współpraca z Komitetem Audytu*

Posiadanie Komitetu Audytu zadeklarowało 35 zakładów. W 34 z nich dyrektor komórki audytu uczestniczył w spotkaniach tego komitetu w 2012 roku. W 55 zakładach Komitet Audytu otrzymuje podsumowanie ustaleń z badania, w 44 zakładach otrzymuje informacje dotyczące działań podejmowanych w celu realizacji wydanych rekomendacji i zaleceń, a w 48 raporty z realizacji planu audytu. Z powyższego można wywnioskować, że w części zakładów informacje te przekazywane są organom o podobnym zakresie kompetencji. Być może odpowiedzi na pierwsze pytanie wynikają z jego interpretacji w ankiecie BION.

*f) Plan audytu i badane obszary*

W 52 zakładach ubezpieczeń na 54, które udzieliły odpowiedzi na to pytanie, plany audytów tworzone są w oparciu o zidentyfikowane kluczowe ryzyka. Stosunkowo niewielka liczba odpowiedzi (15) wskazywała na niezrealizowanie planu audytu w 2012 roku. Wyniki ankiety świadczą o tym, że w 17 zakładach na 55, które udzieliły odpowiedzi na to pytanie, audyt w poprzednim roku objął funkcję zarządzania ryzykiem, w 24 funkcję compliance, a w 31 zakładach badanie dotyczyło obszaru kontroli wewnętrznej. W roku 2013 i w kolejnych latach stosunkowo więcej zakładów zadeklarowało audyty w obszarach zarządzania ryzykiem i kontroli wewnętrznej, co może wynikać z zaawansowania procesów przygotowania do spełnienia wymogów Solvency II. Z udzielonych odpowiedzi wypływa także wniosek, że w dużej części zakładów nie zidentyfikowano ryzyk lub nieprawidłowości w obszarach funkcji zarządzania ryzykiem i compliance, natomiast w niecałej połowie zakładów pewne ryzyka lub nieprawidłowości pojawiły się w obszarze funkcji audytu wewnętrznego.

### 5.2. Funkcja compliance

*a) Istnienie funkcji compliance*

51 zakładów ubezpieczeń posiada w strukturze stanowisko lub komórkę organizacyjną odpowiedzialną za zapewnienie zgodności, nie wszystkie zakłady natomiast uregulowały zasady jej działania, a 19 podmiotów nie posiada dokumentacji dotyczącej funkcji compliance. Być może wynika to ze stosunkowo niedługiej historii istnienia funkcji compliance w zakładach ubezpieczeń oraz braku wymogów prawnych tworzenia takiej funkcji.

*b) Umiejscowienie funkcji compliance w strukturze*

Osoba lub komórka odpowiedzialna za funkcję compliance w 25 zakładach podlega bezpośrednio pod zarząd, w 2 zakładach podlega bezpośrednio pod dyrektora komórki zarządzania ryzykiem, a w 5 zakładach odpowiada bezpośrednio przed kierownikiem komórki prawnej. Pozostałe 22 zakłady zadeklarowały podległość funkcji compliance pod inne organy. W 29 zakładach osoba lub komórka compliance raportuje do zarządu. Taka liczba może wynikać ze zróżnicowania wielkości i specyfiki poszczególnych zakładów.

*c) Odpowiedzialność funkcji compliance*

W 48 zakładach na 50, które udzieliły odpowiedzi na to pytanie, zadania funkcji compliance obejmują doradzanie zarządowi lub radzie nadzorczej zakładu ubezpieczeń w kwestiach zgodności z przepisami prawa, oraz wskazanie i ocenę ryzyk związanych z przestrzeganiem prawa, a w 36 zakładach ocenę wpływu zmian otoczenia prawnego na działalność zakładu ubezpieczeń. W 30 zakładach na 50, komórka odpowiedzialna za funkcję compliance przeprowadza lub przeprowadziła szkolenia dla pracowników, co wskazuje na średni stopień zaangażowania tej funkcji w obszar podnoszenia świadomości pracowników związanej z przestrzeganiem przepisów wewnętrznych i przepisów prawa.

**5.3. Funkcja zarządzania ryzykiem**

*a) Istnienie funkcji zarządzania ryzykiem*

W 52 zakładach ubezpieczeń istnieje stanowisko lub komórka odpowiedzialna za zarządzanie ryzykiem, natomiast w 39 zakładach funkcjonuje komitet ds. ryzyka.

*b) Strategia i system zarządzania ryzykiem*

Spisaną strategię zarządzania ryzykiem ma 39 zakładów ubezpieczeń. 47 zakładów deklaruje posiadanie spisanych zasad omawiających system zarządzania ryzykiem. Z odpowiedzi udzielonych przez zakłady wynika jednak, że w niektórych przypadkach przyjęte zasady nie są zgodne ze strategią zarządzania ryzykiem. 55 zakładów ocenia, że system zarządzania ryzykiem jest adekwatny do charakteru, skali i złożoności ich działalności. Jedynie cztery zakłady odpowiedziały na to pytanie negatywnie. Przyjęty system zarządzania ryzykiem opisuje w szczególności kwestie identyfikacji, pomiaru, monitorowania i ograniczania ryzyka oraz w mniejszej liczbie zakładów współzależności pomiędzy rodzajami ryzyka.

*c) Przegląd skuteczności zarządzania ryzykiem*

51 zakładów dokonuje okresowych przeglądów skuteczności rozwiązań przyjętych w zakresie zarządzania ryzykiem. Pozostałe zakłady nie przeprowadzają takich przeglądów. W 57 zakładach zarząd przekazuje radzie nadzorczej informacje dotyczące najważniejszych rodzajów ryzyka, na jakie narażony jest zakład, oraz przyjętych mechanizmów kontrolnych.

## 6. Modele współpracy i synergia z nich płynąca

Współpraca poszczególnych funkcji w ramach systemu zarządzania ryzykiem jest kluczowa dla skuteczności całego procesu. Pierwszym i najważniejszym krokiem po opisaniu całości procesu jest identyfikacja i wydzielenie części wspólnych między poszczególnymi funkcjami – tak by nie rodziły one żadnych potencjalnych konfliktów interesów. Poniżej prezentujemy proponowane modele współpracy między poszczególnymi działami. W ramach tej współpracy uwzględniamy także ujęcie funkcji aktuarialnej, której sprawne działanie jest istotne z punktu widzenia zarządzania ryzykiem.

Często spotykanym zjawiskiem jest to, że poszczególne funkcje pracują oddzielnie i nie korzystają wzajemnie z wyników swoich prac. Tworzą na własne potrzeby osobne polityki i procedury, inaczej definiują ryzyka, mają osobne rejestry ryzyk i metodyki. Wzajemna współpraca pozwoli zapewnić lepsze wykorzystanie zasobów – brak duplikacji zadań, oraz stworzyć skuteczny system zarządzania ryzykiem. Poniżej prezentujemy obszary, w ramach których współpraca między poszczególnymi funkcjami przyniesie największe korzyści.

### 6.1. Funkcja compliance – Funkcja zarządzania ryzykiem

Funkcja compliance jest odpowiedzialna za monitorowanie przestrzegania regulacji wewnętrznych i przepisów prawa. Obejmuje to, na przykład, właściwe ustalenie funkcji zarządzania ryzykiem, zgodnie z wymaganiami odpowiednich norm i regulacji. Jednak zadaniem tej komórki nie jest projektowanie konkretnych procesów zarządzania ryzykiem w rozumieniu Solvency II. W przeciwnym razie doszłoby bowiem do pomieszania lub powielenia obowiązków. System zarządzania ryzykiem, a więc również funkcja zarządzania ryzykiem, odnosi się do ogólnej oceny i zrozumienia ryzyka w przedsiębiorstwie. Funkcja compliance natomiast odpowiada jedynie za ryzyko braku zgodności.

Niemniej jednak, powstają pewne obszary, w których funkcja compliance i zarządzania ryzykiem pokrywają się. Proponowane rozwiązanie w zakresie współpracy tych dwóch komórek jest takie, by funkcja compliance:

- Zasilała komórkę odpowiedzialną za zarządzanie ryzykiem w informacje niezbędne do identyfikacji i oceny/wyceny ryzyka zgodności;
- Poprzez definiowanie wytycznych i szkolenia pozwalała identyfikować i ograniczać ryzyka niezgodności;
- Wspomagała pierwszą linię obrony w identyfikacji wszelkich naruszeń prawa, zawartych umów oraz regulacji wewnętrznych, i w takim przypadku dzieliła się wynikami z pozostałymi funkcjami w celu oszacowania ryzyka na poziomie zakładu ubezpieczeń. Funkcja zarządzania ryzykiem natomiast uwzględnia ryzyko zgodności w analizie i ocenie, jako czynnik wpływający na profil ryzyka zakładu ubezpieczeń.

### 6.2. Funkcja compliance – Funkcja aktuarialna

Funkcja compliance jest odpowiedzialna za monitorowanie przestrzegania wszelkich wymogów prawnych, co dotyczy również prawidłowego ustanawiania i funkcjonowania aktuariatu w kontekście wymogów regulacyjnych. Zadaniem funkcji compliance nie jest jednak sprawdzanie procesów lub kwestii merytorycznych związanych z funkcją aktuarialną, lecz zapewnienie, że całościowy proces opiera się na aktualnych regulacjach. Podobnie jak w przypadku relacji funkcji compliance z funkcją zarządzania ryzykiem, doszłoby do mieszania lub powielania obowiązków.

### 6.3. Funkcja aktuarialna – Funkcja zarządzania ryzykiem

Funkcja aktuarialna w zakładach ubezpieczeń jest nieodzownym elementem systemu zarządzania ryzykiem. Pomiędzy funkcją aktuarialną a pozostałymi funkcjami istotnymi z perspektywy systemu zarządzania ryzykiem znajduje się wiele obszarów wspólnych.

Do obszarów wspólnych należy zaliczyć zarówno współpracę w zakresie analizy ryzyka, jak i sprawozdawczość do kierownictwa. Funkcja aktuarialna dostarcza funkcji zarządzania ryzykiem wsad w procesie oceny ryzyka. Wymaga to ścisłej współpracy między obiema funkcjami. Aby skutecznie korzystać z wiedzy aktuarialnej, funkcja zarządzania ryzykiem może być wspierana przez aktuariat w ramach realizowanych zadań – patrz model RACI. Odpowiedzialność za koordynację procesów zarządzania ryzykiem pozostaje jednak nadal w obrębie funkcji zarządzania ryzykiem.

W przeciwieństwie do funkcji aktuarialnej, która kontroluje proces wyliczania rezerw, funkcja zarządzania ryzykiem koncentruje się nie na poprawności obliczeń, ale na skuteczności środków kontroli mających za zadanie zapewnić właściwy wybór metod, poprawność wyliczenia oraz ujęcia w sprawozdawczości i wnioskowania.

Podział prac odnosi się również do raportowania do zarządu lub rady nadzorczej. Treść raportów funkcji aktuarialnej oraz funkcji zarządzania ryzykiem może się w określonych obszarach

pokrywać, nawet jeśli mają inny punkt ciężkości. Ważne jest, żeby oba raporty sporządzone były w ramach spójnej systematyki, terminologii, aby zapewnić porównywalność przekazywanych zarządowi informacji.

W mniejszych zakładach ubezpieczeń i tych o mniej skomplikowanych operacjach pełne lub częściowe sprzężenie funkcji aktuarialnej oraz funkcji zarządzania ryzykiem powinno być możliwe pod warunkiem zapewnienia odpowiednich mechanizmów redukujących kwestie konfliktu interesów oraz niezależności.

### 6.4. Funkcja audytu wewnętrznego – Funkcja compliance

Funkcja audytu wewnętrznego dokonuje przeglądu poprawności zaprojektowania, wdrożenia i skuteczności realizacji zadań funkcji compliance.

Tak jak pisaliśmy wcześniej, funkcja compliance jest odpowiedzialna za monitorowanie środowiska regulacyjnego, identyfikację wszelkich wymogów prawnych odnoszących się do działalności zakładu ubezpieczeń oraz zapewnienie przestrzegania przepisów prawa i regulacji wewnętrznych. Dotyczy to również prawidłowego ustanawiania funkcji audytu wewnętrznego w kontekście wymogów regulacyjnych. Celem funkcji compliance nie jest jednak sprawdzanie procesów lub kwestii merytorycznych związanych z audytem wewnętrznym.

Funkcja compliance powinna działać prewencyjnie i z wyprzedzeniem identyfikować ryzyko prawne, a także podejmować działania w celu zapobiegania niezgodności, np. poprzez szkolenia pracowników i przygotowanie wytycznych dotyczących compliance.

Funkcja audytu wewnętrznego jest w stanie wspierać inne jednostki w zakresie kontroli i monitorowania, w związku z tym może również wspierać funkcję compliance w ramach wdrażania środków zapobiegawczych w zakresie zgodności.

Wszelkie kwartalne i roczne sprawozdania obu funkcji powinny być nawzajem udostępniane/wymieniane. Funkcja compliance powinna być zaznajomiona z raportami funkcji audytu wewnętrznego, o ile dotyczą one funkcji compliance. Funkcja audytu wewnętrznego winna uwzględnić w planie audytu ocenę wykonaną przez funkcję compliance w zakresie ryzyka niezgodności i wykorzystać ją jako punkt wyjścia do własnej, niezależnej oceny.

Dla zapewnienia sprawnej współpracy warto również, aby funkcja compliance, dostarczała funkcji audytu wewnętrznego informacji do sporządzenia rocznego planu audytu. Funkcja audytu wewnętrznego powinna samodzielnie decydować, czy i jak tę informację wykorzystać. Jeżeli prace realizowane przez funkcję audytu wewnętrznego wykonywane są odpowiednio, funkcja

compliance powinna być w stanie wyciągać własne wnioski z wyników tych prac w zakresie zagadnień związanych ze zgodnością.

Podobnie, gdy funkcja audytu wewnętrznego w ramach testów zidentyfikuje nieprawidłowości lub naruszenia w zakresie zgodności, powinna zgłosić to funkcji compliance. Obie funkcje mogą współpracować przy ocenie ryzyka oraz opracowaniu propozycji działań naprawczych. Monitorowanie terminowego i prawidłowego wdrożenia tych działań, które wynikają z audytu, stanowi odpowiedzialność funkcji audytu wewnętrznego.

### 6.5. Funkcja audytu wewnętrznego – Funkcja zarządzania ryzykiem

Punkty styku pomiędzy funkcją audytu wewnętrznego a funkcją zarządzania ryzykiem powstają w szczególności w odniesieniu do monitorowania systemu zarządzania ryzykiem, przeprowadzania analizy ryzyka oraz raportowania do zarządu lub Komitetu Audytu/rady nadzorczej.

Zarówno funkcja zarządzania ryzykiem, jak i funkcja audytu wewnętrznego, musi monitorować system zarządzania ryzykiem i robić przegląd jego adekwatności i efektywności, przy czym ocena ta, dokonywana przez osoby odpowiedzialne za zarządzanie ryzykiem, stanowi element procesu samodoskonalenia (zgodnie chociażby z wymogami normy ISO 31000[4]), dokonywana natomiast przez funkcję audytu wewnętrznego jest elementem niezależnej oceny tego systemu. W przypadku gdy funkcja zarządzania ryzykiem dostrzega potrzebę przeprowadzenia badania w zakresie systemu zarządzania ryzykiem, może zaproponować umieszczenie danego zadania w planie audytu lub jego realizację w ramach audytu doraźnego/ad hoc. Funkcja audytu wewnętrznego niezależnie podejmuje decyzję, czy i jak uwzględnić dane zadanie. Innym punktem wspólnym funkcji audytu wewnętrznego i funkcji zarządzania ryzykiem jest identyfikacja i ocena ryzyk biznesowych. Zasadniczo, od obu funkcji Solvency II wymaga przeprowadzania kompleksowej analizy ryzyka. Dla funkcji zarządzania ryzykiem wynika to wprost z przepisów Solvency II. Dla funkcji audytu wewnętrznego analiza ryzyka jest kluczowym elementem pozwalającym na opracowanie opartego na ryzyku planu audytu. Opracowanie takiego planu stanowi wymóg bezpośrednio definiowany w standardzie IIA, przyjęty w środowisku audytu jako wytyczne, których stosowanie jest najlepszą praktyką funkcji audytu wewnętrznego. Plan audytu definiuje się przez funkcję audytu wewnętrznego, m.in. z uwzględnieniem efektów prac funkcji zarządzania ryzykiem, a uzgadnia po stronie zarządu.

Jednostki biznesowe – pierwsza linia obrony – odpowiedają za przeprowadzanie oceny ryzyka w procesach, za które są odpowiedzialne. Wyniki ich prac stanowią bazę do analizy funkcji zarządzania ryzykiem i funkcji audytu wewnętrznego. Niedopuszczalne jest, aby tylko jedna

4 ISO 31000:2009 Risk Management – Principles and guidelines, opublikowany 13 listopada 2009 r.

z dwóch funkcji przeprowadzała analizę ryzyka, a druga bezkrytycznie korzystała z jej wyników. Sytuacja, w której wykorzystując wyniki funkcji zarządzania ryzykiem, funkcja audytu wewnętrznego nie dokonywałaby samodzielnej oceny ryzyka – przeczyłaby niezależności funkcji audytu wewnętrznego. Wyniki uzyskane przez funkcję zarządzania ryzykiem mogą zostać wzięte pod uwagę/uwzględnione w ramach analizy ryzyka przez funkcję audytu wewnętrznego i odwrotnie. Wymiana informacji pomiędzy funkcjami jest konieczna, aby obie miały kompleksowy obraz profilu ryzyka zakładu ubezpieczeń. Współpraca może polegać na tym, że funkcje porozumieją się w sprawie jednolitego systemu/systematyki analizy ryzyka. Dotyczy to w szczególności kategoryzacji ryzyka oraz obrazu wewnętrznych procesów zakładu ubezpieczeń. Również przy ocenie ryzyka i określeniu istotności może zostać wprowadzona jednolita skala. Ale nie oznacza to, że działalność funkcji audytu wewnętrznego powinna koncentrować się wyłącznie na ryzykach, które są określone jako istotne w zakresie zarządzania ryzykiem. Zadaniem funkcji audytu wewnętrznego jest zasadniczo uwzględnienie wszystkich procesów w długoterminowym planie audytu (w ramach uniwersum audytu). Tylko w ten sposób funkcja audytu wewnętrznego może zidentyfikować ryzyka, które do tej pory nie zostały zauważone, a zatem spełnić funkcję wczesnego ostrzegania. Solvency II wymaga zarówno od funkcji zarządzania ryzykiem, jak i funkcji audytu wewnętrznego, raportowania do zarządu. Uważamy za absolutnie konieczne ujednolicenie definicji/terminologii stosowanej przez poszczególne komórki uczestniczące w procesie zarządzania ryzykiem, tak aby przekaz do najwyższego kierownictwa zakładu ubezpieczeń był spójny i jednoznaczny.

### 6.6. Funkcja audytu wewnętrznego – Funkcja aktuarialna

Punkty wspólne funkcji audytu wewnętrznego oraz funkcji aktuarialnej występują przy monitorowaniu wyceny rezerw techniczno-ubezpieczeniowych, oceny polityki ubezpieczeniowej oraz oceny adekwatności rozwiązań w zakresie reasekuracji, a także raportowania do zarządu. Mimo iż działania obu funkcji mają na celu kontrolę wyceny rezerwy, ich podejścia są różne. Podczas gdy funkcja aktuarialna koncentruje się na weryfikacji merytorycznej wyceny, przedmiotem audytu wewnętrznego jest głównie adekwatność procesu wyceny oraz funkcjonalność i skuteczność systemu kontroli wewnętrznej, w celu zapewnienia jego zgodności z odpowiednimi przepisami wewnętrznymi i zewnętrznymi.

Podstawy do wyceny rezerw (np. wybór technik modelowania lub szacowania) oraz przebieg procesu wyceny powinny być udokumentowane. W oparciu o tę dokumentację następuje badanie w ramach funkcji audytu wewnętrznego, podczas gdy funkcja aktuarialna zakłada stały monitoring procesu. Inne punkty wspólne mogą powstawać w ramach oceny polityki ubezpieczeniowej oraz badania adekwatności rozwiązań w zakresie reasekuracji. Funkcja aktuarialna skupia się na zależnościach między polityką ubezpieczeniową i reasekuracji oraz rezerwą. Funkcja audytu koncentruje się na funkcjonalności i skuteczności procedur kontroli wewnętrznej w celu zapewnienia dokładności

wyceny i związanych z nią procesów podejmowania decyzji. Funkcja aktuarialna przynajmniej raz w roku zobowiązana jest zgłosić do zarządu sprawozdanie z wyceny rezerw techniczno-ubezpieczeniowych (metody, założenia, jakość danych), jak również polityk ubezpieczeniowych i reasekuracyjnych, w celu przedstawienia istniejących braków proceduralnych i słabych stron. W tym samym czasie zagadnienia te mogą być też przedmiotem raportu z audytu, a więc pewne informacje mogą się powtarzać, niewykluczone są także odmienne opinie.

Wyżej opisane metody współpracy pozwolą nie tylko usprawnić proces zarządzania ryzykiem, ale także w sposób skuteczny wykorzystywać zasoby zakładu ubezpieczeń zarówno materialne, jak i osobowe, poprzez niedublowanie (tam, gdzie to możliwe) tych samych zadań przez różne funkcje w ramach tego samego procesu.

### 6.7. Funkcja audytu wewnętrznego – Komitet Audytu

Do zadań Komitetu Audytu w ramach współpracy z audytem wewnętrznym należą m.in.:

- Zapewnienie niezależności funkcji audytu wewnętrznego. Jednym z kluczowych czynników niezależności audytu wewnętrznego jest właściwe umiejscowienie w strukturze organizacyjnej. Funkcja audytu wewnętrznego powinna raportować bezpośrednio Komitetowi Audytu. Pod względem organizacyjnym audyt wewnętrzny powinien podlegać prezesowi zarządu;
- Zapewnienie, iż funkcja audytu wewnętrznego działa zgodnie z powszechnie przyjętymi i obowiązującymi standardami audytu wewnętrznego pod względem kwalifikacji, niezależności, organizacji i jakości pracy oraz zasobów;
- Okresowa ocena funkcji audytu wewnętrznego z uwzględnieniem jej niezależności i znaczenia/istotności jej raportów;
- Opiniowanie zaproponowanego planu audytów na kolejny rok;
- Analiza ewentualnych odstępstw od ustalonego planu audytu oraz analiza propozycji dotyczących usprawnienia procesu audytu;
- Wspieranie audytu wewnętrznego w sytuacjach zidentyfikowania nieprawidłowości i niemożności uzyskania odpowiednich wyjaśnień;
- Dokonywanie przeglądu wyników działania systemu kontroli wewnętrznej, audytu wewnętrznego, z uwzględnieniem uwag i rekomendacji pochodzących z okresowego niezależnego przeglądu funkcji audytu wewnętrznego wymaganego przez standardy IIA;
- Weryfikacja adekwatności i efektywności systemu kontroli wewnętrznej przy udziale: biegłego rewidenta, audytora wewnętrznego lub podmiotów zewnętrznych; proponowanie ulepszeń procedur w zakresie kontroli wewnętrznej lub wskazanie obszarów, które wymagają bardziej szczegółowej kontroli; zwrócenie szczególnej uwagi na kontrolę wewnętrzną: dokonywanych płatności, przeprowadzanych transakcji bądź przestrzegania obowiązujących procedur regulacji wewnętrznych, które mogą być niepoprawne lub niezgodne z prawem;

- Uzyskiwanie od kadry zarządzającej, biegłego rewidenta, funkcji audytu wewnętrznego oraz kierownictwa działu finansowego szczegółowych informacji w zakresie m.in. środowiska kontroli, oceny ryzyka, czynności kontrolnych, komunikacji i monitoringu.

### 6.8. Model RACI

Dobrą praktyką jest, by – tak jak to zostało wcześniej przedstawione – w ramach ustanawianych regulacji wewnętrznych zdefiniować kompetencje poszczególnych funkcji odnośnie całościowego systemu zarządzania ryzykiem. Skutecznym narzędziem wspomagającym ten proces jest model RACI (**R – Responsible**/odpowiedzialny, **A – Accepts**/akceptuje, **C – Consults**/konsultuje, **I – Informed**/informowany), który służy do wskazania wzajemnych relacji pomiędzy uczestnikami procesu w poszczególnych obszarach i zadaniach. Dodatkowo w ramach tego modelu wyodrębnić należy różne role w procesie ze względu na typy uprawnień oraz wymagany poziom zaangażowania.

Zasady działania modelu zostały zaprezentowane na poniższym schemacie.

**Rysunek 10. Model RACI – zasady działania**
**Macierz odpowiedzialności**


*Źródło: Opracowanie własne.*

W oparciu o ten model opracowano listę podstawowych procesów dotyczących zarządzania ryzykiem i współpracy między poszczególnymi funkcjami:

**Rysunek 11. Model RACI**

| Proces | Rola | | | |
|---|---|---|---|---|
| | Ryzyko | Audyt wewnętrzny | Compliance | Zarząd |
| Ocena ryzyka (R – za ocenę ryzyka odpowiedzialna jest pierwsza linia obrony, czyli komórki biznesowe) | A | C | I | A |
| Planowanie audytu | C | R | C | A |
| Budowanie świadomości nt. systemu zarządzania ryzykiem i kontroli wewnętrznej | R | R | I | A |
| Reakcja na ryzyko (R – odpowiedzialność za reakcję spoczywa na pierwszej linii obrony – jednostki biznesowe) | C | C | I | A |
| Monitorowanie zgodności | I | I | R | I |
| Przeprowadzanie zadań audytu | I | R | I | C |
| Raportowanie audytu | I | R | I | I |
| Wsparcie i informowanie o zmianach regulacyjnych | I | I | R | I |
| Zapewnienie uwzględniania kluczowych ryzyk w procesach planowania biznesowego i podejmowania decyzji | R | I | C | A |
| Zarządzanie informacją nt. ryzyk | R | I | C | A |
| Raportowanie ryzyka | R | I | I | A |
| Ustanowienie struktury zarządzania ryzykiem | R | C | C | A |

*Źródło: Opracowanie własne.*

W przypadku gdy nie wszystkie omawiane funkcje zostały ustanowione, zakres ich obowiązków w ramach tego modelu zostaje przejęty przez komórkę, która wykonuje dane zadania. Sprawdzonym i popularnym rozwiązaniem jest ustanowienie grup roboczych lub komitetów, w ramach których członkowie poszczególnych funkcji spotykają się i informują o zidentyfikowanych ryzykach oraz reakcji na nie.

## Słownik

**Adekwatność** – wierne ujęcie danego przedmiotu, wyczerpujące poznawczo wszelkie jego aspekty (opisujące jego części składowe i strukturę, właściwości, historię, relacje wewnętrzne i zewnętrzne itp.).

**Audyt** – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu.

**Audyt wewnętrzny** – rozumiany jako działalność niezależna i obiektywna, której celem jest ocena adekwatności i efektywności systemu kontroli wewnętrznej i innych elementów systemu zarządzania.

**Dokumentacja** – spisane informacje (cele, zadania) dotyczące poszczególnych obszarów działalności. W ramach dokumentacji zakład może mieć spisane strategie, zasady, procedury. Poszczególne strategie, zasady, procedury mogą być spisane jako oddzielne dokumenty lub stanowić części większych dokumentów:

a) Strategie dotyczące danego obszaru – zawierają spisane główne cele w danym obszarze, a także m.in. zatwierdzone limity tolerancji ryzyka, przypisanie odpowiedzialności dla obszarów działalności. Za ich uszanowanie i rozwój powinien odpowiadać zarząd.
b) Zasady dotyczące danego obszaru – zawierają m.in. cele ustanowionych zasad, zadania do wykonania i jednostki/stanowiska odpowiedzialne za ich wykonanie, podział obowiązków między poszczególnymi jednostkami organizacyjnymi, opis funkcji kluczowych z przypisaniem uprawnień i praw, w tym określenie stanowisk nadzorujących co najmniej funkcje należące do systemu zarządzania. Zatwierdzenie zasad i zmian w nich powinno być dokonywane przez zarząd.
c) Procedury dotyczące danego obszaru – szczegółowe określenie wykonywanych czynności, procesów.

**Efektywność** – relacja między osiągniętymi wynikami a wykorzystanymi zasobami.

**Funkcja compliance** – obejmuje doradzanie zarządowi i radzie nadzorczej w kwestiach zgodności z przepisami prawa oraz ocenę możliwego wpływu wszelkich zmian otoczenia prawnego na operacje danego zakładu, oraz wskazanie i ocenę ryzyka związanego z nieprzestrzeganiem prawa.

**Kluczowe kierownictwo** – Amsb (The administrative, management or supervisory body), kierownictwo odpowiedzialne za zapewnienie ciągłej adekwatności wewnętrznego modelu operacyjnego oraz za to, by model ten odpowiadał profilowi ryzyka zakładu ubezpieczeń.

**Komórka audytu wewnętrznego** – rozumiana jako wyodrębniona komórka wykonująca zadania przypisane audytowi wewnętrznemu. Jeżeli w zakładzie ubezpieczeń/reasekuracji istnieje „komórka kontroli wewnętrznej", która *de facto* wykonuje zadania przypisane audytowi wewnętrznemu, to powinna być ona traktowana jako komórka audytu wewnętrznego.

**Kontrola** – ogólnie porównywanie stanu faktycznego ze stanem założonym. W innym sensie nadzór nad czymś i dopilnowywanie, aby to funkcjonowało zgodnie z ustalonymi zasadami.

**System kontroli wewnętrznej** – rozumiany jako system obejmujący w szczególności procedury administracyjne i księgowe, organizację kontroli wewnętrznej, odpowiednie ustalenia w zakresie raportowania na wszystkich szczeblach struktury organizacyjnej zakładu oraz zgodności z przepisami (compliance). System kontroli wewnętrznej składa się z następujących ściśle powiązanych elementów: środowiska kontroli, czynności kontrolnych, komunikacji i informowania oraz monitorowania.

**Identyfikacja ryzyka** – proces, w wyniku którego powstaje całościowa i spójna wewnętrznie lista ryzyk, mogących powodować, przyspieszać, opóźniać czy ingerować w osiągnięcie celów spółki, bądź im zapobiegać. Lista ryzyk tworzona jest w odniesieniu do celów strategicznych spółki.

**Interesariusze** – strony podlegające wpływowi organizacji – udziałowcy, społeczność, w jakiej działa organizacja, pracownicy, klienci i dostawcy.

**Limity ryzyka** – akceptowane odchylenie w osiąganiu ustalonych celów.

**Mechanizm kontrolny** – działanie pozwalające na ograniczenie prawdopodobieństwa materializacji danego ryzyka.

**Niepewność** – niezdolność do przewidzenia dokładnego prawdopodobieństwa lub efektów przyszłych zdarzeń.

**Niezgodność** – niespełnienie wymagania (3.1.2, ISO 9000:2005). Wystąpienie niezgodności nie sprzyja jakości. Może być związane z niespełnieniem określonych wymagań dotyczących norm, dokumentacji jakości, przepisów prawnych, wymagań stron kontraktu czy wymagań klienta oraz innych zainteresowanych stron. Jako niezgodność można potraktować tylko to, co faktycznie zostało stwierdzone, czyli poparte dowodem obiektywnym.

**Ogólne środki kontroli** – polityki i procedury pomagające zapewnić ciągłość i prawidłowość działania systemów informatycznych.

**Polityka** – decyzje kierownictwa na temat sprawowania kontroli. Polityka stanowi punkt wyjścia dla procedur jej realizacji.

**Prawdopodobieństwo** – szansa lub zagrożenie, że dane zdarzenie wystąpi.

**Procedura** – szczegółowe określenie wykonywanych czynności, procesów.

**Proces zarządzania** – działania podejmowane przez kierownictwo w ramach kierowania organizacją. Zarządzanie ryzykiem korporacyjnym jest integralną częścią procesu zarządzania.

**Proces zarządzania ryzykiem** – synonim zarządzania ryzykiem w organizacji. Proces zarządzania ryzykiem jest procesem identyfikacji, oceny i przeciwdziałania występowaniu ryzyka.

**Raportowanie ryzyka** – przekazywanie informacji na temat ryzyk do interesariuszy wewnętrznych i/lub zewnętrznych.

**Ryzyko inherentne** – poziom ryzyka bez uwzględnienia działań podjętych w celu zminimalizowania prawdopodobieństwa jego wystąpienia (np. realizacji zabezpieczeń).

**Ryzyko rezydualne** – ryzyko, które zostaje po zastosowaniu przez spółkę strategii mitygującej ryzyko.

**Skuteczność** – stopień, w jakim planowane działania są realizowane i planowane wyniki osiągane.

**Strategia zarządzania ryzykiem** – technika minimalizowania prawdopodobieństwa wystąpienia potencjalnego ryzyka lub jego wpływu (np. strat) poprzez szkolenia, polityki i procedury finansowe oraz inne polityki, które mogą mieć wpływ na realizację celów firmy.

**Tolerancja ryzyka** – akceptowalny poziom ryzyka związanego z osiągnięciem danego celu.

**Zagraniczny oddział zakładu ubezpieczeń/reasekuracji** – rozumiany jako wyodrębniona i samodzielna organizacyjnie część działalności gospodarczej, wykonywana przez zakład ubezpieczeń/reasekuracji poza siedzibą zakładu ubezpieczeń/reasekuracji lub głównym miejscem wykonywania działalności.

PIU
Polska Izba Ubezpieczeń

ul. Wspólna 47/49
00-684 Warszawa
tel. +48 22 420 51 05 (06)
fax +48 22 420 51 07
e-mail: office@piu.org.pl
www.piu.org.pl