COSO

Komitet Organizacji Sponsorujących Komisję Treadwaya

Ład organizacyjny i kontrola wewnętrzna

WYKORZYSTANIE COSO W TRZECH LINIACH OBRONY

Instytut Audytorów Wewnętrznych

Douglas J. Anderson | **Gina Eubanks**

Autorzy

Instytut Audytorów Wewnętrznych

Douglas J. Anderson, CIA, CPA, CRMA, CMA,
Zarządzający audytem wewnętrznym, Konsultant
w Centrum zarządzających audytem przy
Instytucie Audytorów Wewnętrznych.

Gina Eubanks, CIA, CISA, CRMA, CCSA,
wiceprezes Profesjonalnych Usług
w Instytucie Audytorów Wewnętrznych.

Podziękowania

Chcielibyśmy podziekować Richard J. Anderson, Richard Chambers, Sally Dix, Jim DeLoach,
Hal Garyn, and Paul Marshall za ich pomoc i wsparcie w przygotowaniu tej publikacji.

Członkowie Rady COSO

Robert B. Hirth, Jr.
Przewodniczący Rady COSO

Douglas F. Prawitt
Amerykańskie Stowarzyszenie Księgowości

Richard F. Chambers
Instytut Audytorów Wewnętrznych

Mitchell A. Danaher
Międzynarodowe Zrzeszenie Dyrektorów Finansowych

Charles E. Landes
Amerykański Instytut Biegłych Rewidentów

Sandra Richtermeyer
Instytut Rachunkowości Zarządczej

Przedmowa

Publikacja powstała na zlecenie Komitetu Organizacji Sponsorujących Komisję Treadwaya (COSO). Dążeniem COSO jest zapewnienie przywództwa, poprzez stworzenie systemowych ram i wytycznych w zakresie zarządzania ryzykiem przedsiębiorstwa, kontroli wewnętrznej i przeciwdziałania nadużyciom w celu poprawy funkcjonowania organizacji, ładu organizacyjnego oraz ograniczenia nadużyć w organizacjach.
COSO został utworzony i sfinansowany z inicjatywny następujących organizacji z sektora prywatnego:

Amerykańskie Stowarzyszenie Księgowości (AAA)

Amerykańskiego Instytutu Biegłych Rewidentów (AICPA)

Międzynarodowe Zrzeszenie Dyrektorów Finansowych (FEI)

Instytut Rachunkowości Zarządczej (IMA)

Instytut Audytorów Wewnętrznych (IIA)

COSO
Komitet Organizacji Sponsorujących
Komisję Treadwaya

www.coso.org

Spis treści

Grafikę zaczerpnięto z publikacji Trzy linie obrony w efektywnym zarządzaniu ryzykiem i kontroli, Instytutu Audytorów Wewnętrznych, Styczeń 2013.

Wprowadzenie

Niniejsza publikacja jest efektem współpracy pomiędzy COSO i Instytutem Audytorów Wewnętrznych. Jej celem jest pomoc organizacjom w ulepszeniu ich struktury organizacyjnej poprzez wytyczne określające i przypisujące konkretne role i obowiązki w zakresie kontroli wewnętrznej poprzez odniesienie wskazane w dokumencie Kontrola Wewnętrzna – Zintegrowana Struktura Ramowa – COSO[1] do modelu trzech linii obrony[2].

Streszczenie

Każda organizacja posiada cele oraz dąży do ich osiągnięcia. W trakcie ich realizacji występują zdarzenia i okoliczności, które mogą zagrozić osiągnięciu tych celów. Te potencjalne zdarzenia i okoliczności tworzą ryzyko, które należy zidentyfikować, przeanalizować, zdefiniować i odnieść się do niego. Niektóre rodzaje ryzyka mogą zostać zaakceptowane (w całości lub w części), a niektóre z nich mogą być całkowicie lub częściowo ograniczone do akceptowalnego przez organizację poziomu. Istnieje wiele sposobów ograniczania ryzyka, z jedną podstawową metodą polegającą na zaprojektowaniu i wdrożeniu skutecznej kontroli wewnętrznej.

Kontrola Wewnętrzna – Zintegrowana Struktura Ramowa – COSO I (Struktura Ramowa) określa komponenty, zasady i czynniki niezbędne dla organizacji, w celu skutecznego zarządzania ryzykiem poprzez wdrożenie systemu kontroli wewnętrznej. Nie jest jednak do końca sprecyzowane, kto jest odpowiedzialny za konkretne obowiązki wynikające ze Struktury Ramowej. Jasno określone obowiązki muszą być tak zdefiniowane, aby każda grupa rozumiała swoją rolę w adresowaniu ryzyka i kontroli, kwestie, za które jest odpowiedzialna oraz zasady i sposoby współpracy z innymi grupami. W adresowaniu ryzyka i kontroli nie powinny pojawiać się luki ani niepotrzebne lub niezamierzone powielanie wysiłków.

Model Trzech linii obrony (Model) opisuje, w jaki sposób konkretne zadania związane z ryzykiem i kontrolą mogą być przypisane i koordynowane w ramach organizacji, niezależnie od jej wielkości i złożoności. Rada[3] i kierownictwo powinni zrozumieć istotne różnice pomiędzy rolami i odpowiedzialnością za obowiązki oraz sposobów optymalnego ich przypisani w organizacji, aby zwiększyć prawdopodobieństwo osiągnięcia celów. W szczególności Model wyjaśnia różnicę i zależność pomiędzy zapewnieniem, a innymi działaniami monitorującymi; Działaniami, które mogą być nieprawidłowo rozumiane, jeśli nie zostaną jasno zdefiniowane.

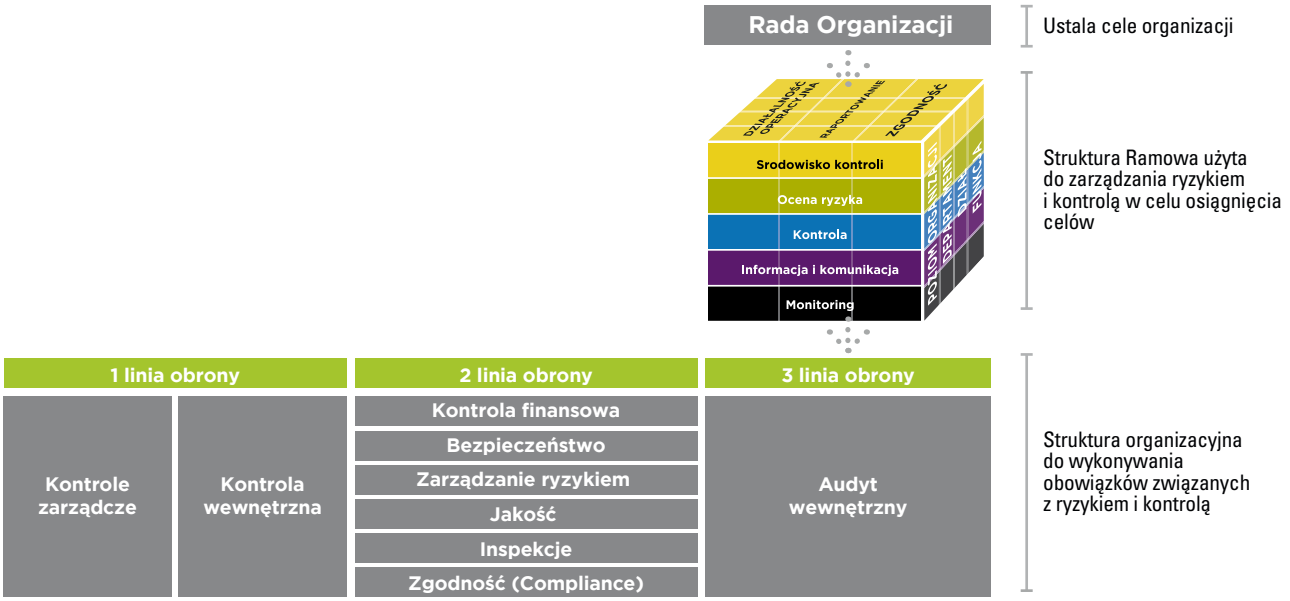
Zakładamy, że czytelnik posiada podstawową wiedzę na temat Struktury Ramowej oraz Modelu. Dla tych, którzy nie są zaznajomieni ze Strukturą Ramową, więcej informacji można znaleźć na stronie COSO.org. Model jest opisany bardziej szczegółowo w sekcji I, w dalszej części tego dokumentu.

[1] Kontrola Wewnętrzna – Zintegrowana Struktura Ramowa – COSO I (ang. COSO Internal Control — Integrated Framework Jersey City, NJ: Amerykańskiego Instytutu Biegłych Rewidentów, Maj 2013). Dostępna na stronie coso.org)

[2] Trzy linie obrony w efektywnym zarządzaniu ryzykiem i kontroli ((ang. The Three Lines of Defense in Effective Risk Management and Control)), (Altamonte Springs, FL: Instytutu Audytorów wewnętrznych, Styczeń 2013). Dostępne na stronie: 3LinesofDefenseinEffectiveRiskManagementandControl (https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

[3] Podobnie jak w innych publikacjach COSO, w tym dokumencie termin „Rada dyrektorów" odnosi się do organów odpowiedzialnych za ład organizacyjny, w skład których wchodzi niezależna grupa dyrektorów jak: rada dyrektorów, rada powierników, komplementariusze, właściciele lub rada nadzorcza. Zgodnie z definicją Rady, użytą w standardach IIA, Rada jest to organ zarządzający, do obowiązków którego należy kierowanie działaniami i kierownictwem organizacji i/lub nadzór nad nimi.
przypis tłumacza: Kierownictwo wyższego szczebla obejmuje zazwyczaj: zarząd oraz kluczowych pracowników niebędących członkami zarządu np. dyrektora finansowego, dyrektora ds. informatyki, dyrektora zespołu radców prawnych, dyrektora sprzedaży, dyrektora operacji, dyrektora zarządzania ryzykiem (Chief Risk Officer), dyrektora ds. zgodności (Compliance Officer).

Rysunek 1. Zależności pomiędzy celami, założeniami Struktury Ramowej COSO i Modelem



I. Model trzech linii obrony

Model pozwala na lepsze zrozumienie zarządzania ryzykiem i kontroli poprzez wyraźne zdefiniowanie ról i obowiązków. Podstawowe założenie modelu mówi, że do skutecznego zarządzania ryzykiem i efektywnej kontroli konieczne są trzy grupy (linie obrony) funkcjonujące pod nadzorem kierownictwa wyższego szczebla i Rady.
Do obowiązków każdej z grup (linii) należą:

1. **Zarządzanie ryzykiem** i kontrola (zarządzanie operacyjne pierwszej linii).

2. **Monitorowanie** ryzyka i kontroli w celu wspierania kierownictwa (funkcje ryzyka, kontroli i zgodności wprowadzone przez kierownictwo).

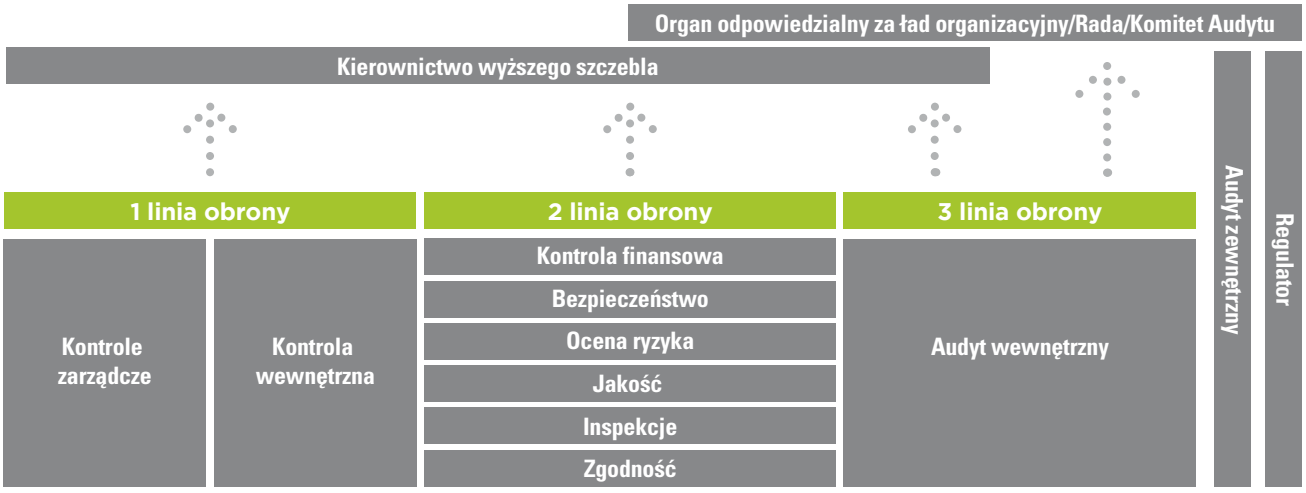
3. **Dostarczanie** niezależnego zapewnienia Radzie i kierownictwu wyższego szczebla dotyczącego skuteczności zarządzania ryzykiem i kontroli (audyt wewnętrzny).

Każda z trzech linii odgrywa odmienną rolę w ramach szeroko rozumianej struktury ładu organizacyjnego jednostki. Skuteczne wykonywanie przypisanych im ról, zwiększa prawdopodobieństwo, że organizacja zrealizuje swoje cele.

Każdy w organizacji jest w pewnym zakresie odpowiedzialny za kontrolę wewnętrzną. W celu zapewnienia, że istotne/kluczowe obowiązki są wykonywane tak jak powinny, Model wprowadza wyraźnie określone role i zakres odpowiedzialności. Jeżeli organizacja prawidłowo ustrukturyzuje trzy linie, a ich działania są skuteczne, to nie powinno być żadnych luk ani niepotrzebnego powielania wysiłków. Dodatkowo większe jest prawdopodobieństwo efektywnego zarządzania ryzykiem i kontrolą. Dla Rady oznacza to zwiększone możliwości uzyskania bezstronnej informacji na temat najistotniejszych ryzyk w organizacji oraz w jaki sposób kierownictwo odpowiada na te ryzyka.

Model zapewnia elastyczną strukturę, która może zostać wdrożona jako wsparcie Struktury Ramowej. Funkcje w każdej z linii obrony będą się różnić w zależności od organizacji. Niektóre funkcje mogą być łączone lub dzielone w poszczególnych liniach obrony. Na przykład, w niektórych organizacjach część funkcji zgodności w drugiej linii może być zaangażowana w projektowanie kontroli pierwszej linii, podczas gdy inne części drugiej linii będą, przede wszystkim, koncentrować się na monitorowaniu tych kontroli.

Rysunek 2. Model trzech linii obrony
Trzy linie obrony w skutecznym zarządzeniem ryzykiem i kontroli, Instytutu Audytorów Wewnętrznych, Styczeń 2013.



Niezależnie od tego, jak dana jednostka zorganizuje trzy linie obrony, istnieje kilka istotnych zasady charakteryzujących ten Model:

1. Pierwsza linia obrony opiera się na biznesie i właścicielach procesów, których działalność tworzy ryzyka i/lub zarządza ryzykami, które mogą sprzyjać lub stać na przeszkodzie w osiągnięciu celów przez daną organizację. Obejmuje to działania na właściwych ryzykach. Pierwsza linia obrony jest właścicielem ryzyk, jak również należy do niej zaprojektowanie i realizacja kontroli w odpowiedzi na te ryzyka.

2. Druga linia istnieje w celu wspierania kierownictwa swoim doświadczeniem, doskonaleniem procesów i monitorowaniem pierwszej linii, w celu zapewnienia, że ryzyko i kontrola są skutecznie zarządzane. Druga linia obrony jest oddzielona od pierwszej linii, ale nadal jest nadzorowana przez kierownictwa wyższego szczebla i zwykle wykonuje niektóre funkcje zarządcze. Druga linia pełni w istocie funkcję zarządczą i/lub nadzorczą oraz posiada wiele aspektów zarządzania ryzykiem.

3. Trzecia linia dostarcza kierownictwu wyższego szczebla i Radzie zapewnienia, że działania pierwszej i drugiej linii są zgodne z ich oczekiwaniami. Trzecia linia obrony nie jest zazwyczaj upoważniona do wykonywania funkcji zarządczych, co ma chronić jej obiektywność i niezależność organizacyjną. Ponadto, trzecia linia raportuje bezpośrednio do Rady i pełni funkcje zapewniające, a nie zarządcze, co odróżnia ją od drugiej linii obrony.

Dążeniem każdej organizacji jest osiągnięcie swoich celów. Realizacja tych celów wymaga wykorzystania pojawiających się możliwości, podążania drogą wzrostu, podejmowania ryzyka i zarządzania tym ryzykiem – wszystko, aby rozwijać organizację.
Brak podejmowania działań dla odpowiednich ryzyk i brak właściwego zarządzania i kontrolowania ryzyka, może przeszkodzić organizacji w realizacji jej celów.
Od zawsze istnieją, i będą istniały, rozbieżne interesy pomiędzy działaniami zmierzającymi do wytworzenia wartości przedsiębiorstwa i działaniami, których celem jest zachowanie jego wartości. Struktura Ramowa dostarcza ram do przeanalizowania ryzyka i kontroli, w celu zapewnienia, że są one właściwe i odpowiednio zarządzane.
Model zawiera wskazówki dotyczące struktury organizacyjnej do wykorzystania przy wdrożeniu, przypisaniu ról i obowiązków osobom, które zwiększą sukces skutecznego zarządzania ryzykiem i kontroli.

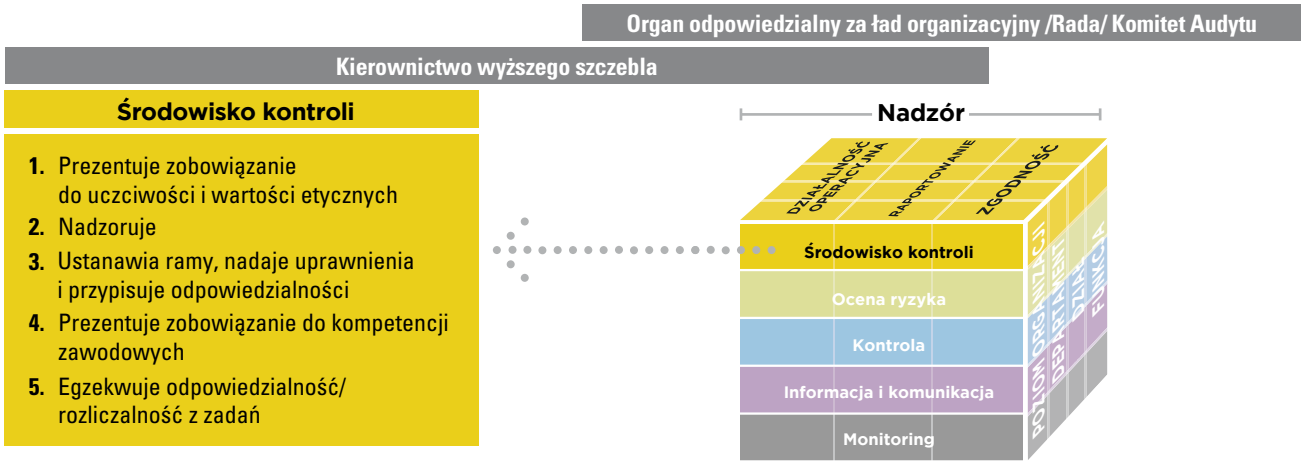
Rola kierownictwa wyższego szczebla i Rady w Modelu trzech linii obrony

Kierownictwo wyższego szczebla i Rada mają kluczowe role w Modelu. Kierownictwo wyższego szczebla jest odpowiedzialne i rozliczane za wybór, rozwój i ocenę systemu kontroli wewnętrznej pod nadzorem Rady. Mimo, że ani kierownictwo wyższego szczebla, ani Rada nie są uważani za część jednej z trzech linii, obie grupy wspólnie ponoszą odpowiedzialność za określenie celów danej organizacji, zdefiniowanie ogólnej strategii pozwalającej osiągnąć te cele oraz ustanowienie struktur organizacyjnych, w celu skutecznego zarządzania ryzykiem.
Stanowią one najlepsze organy, do zapewnienia optymalnej struktury organizacyjnej dla przypisania ról i obowiązków związanych z ryzykiem i kontrolą. Kierownictwo wyższego szczebla musi w pełni wspierać silny ład organizacyjny, kontrolę i zarządzanie ryzykiem. Ponadto Kierownictwo wyższego szczebla i Rada ponoszą ostateczną odpowiedzialność za działania pierwszej i drugiej linii obrony. Ich zaangażowanie decyduje o powodzeniu całego modelu.

Struktura Ramowa pomaga jasno określić odpowiedzialność Rady i kierownictwa wyższego szczebla. Jak pokazano na poniższym **Rysunku 3**, głównie te organy są odpowiedzialne za środowisko kontroli wsparte przez pięć zasad, a swoją postawą nadają one ton w organizacji.

Model dostarcza ramowe zasady na bazie Struktury Ramowej, uszczegóławiając przypisanie ról i odpowiedzialności. Model jest najlepiej wdrażany przy aktywnym wsparciu i doradztwie Rady oraz kierownictwa wyższego szczebla.

Rysunek 3. Funkcje nadzorcze w środowisku kontroli.



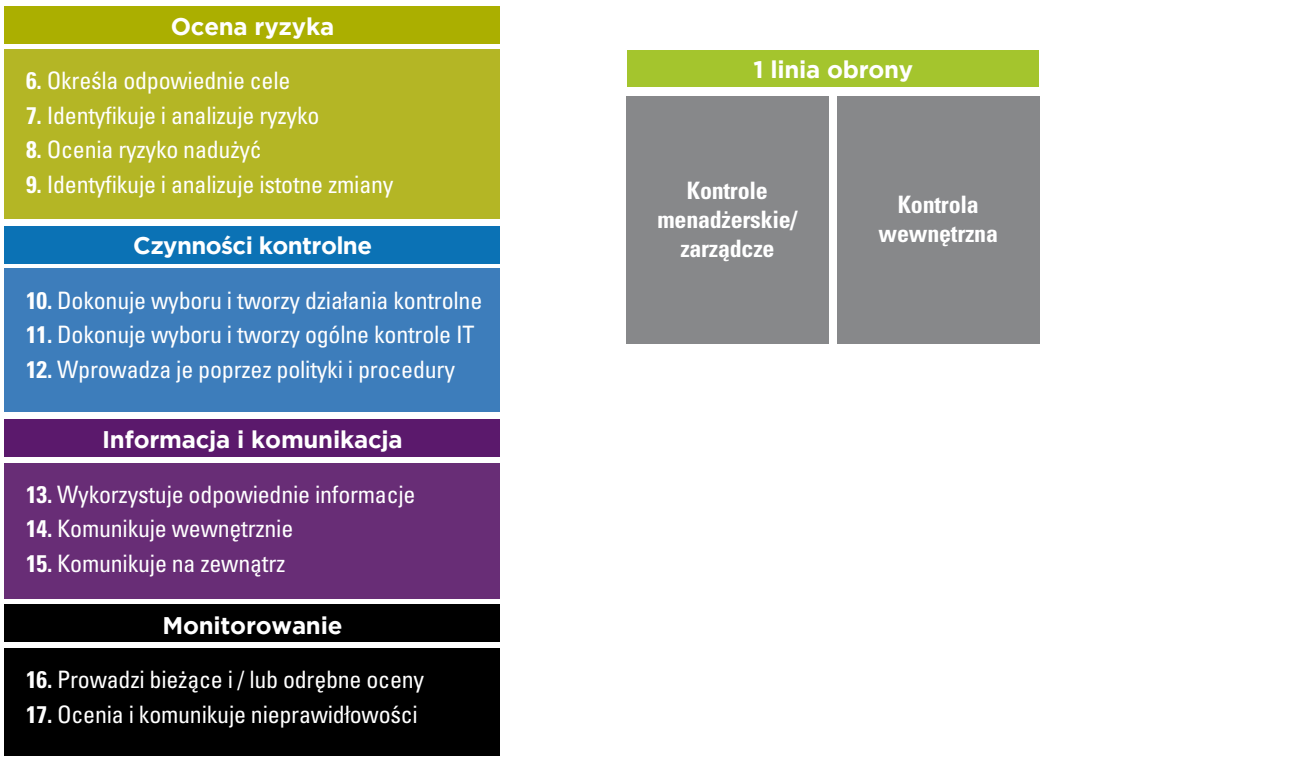
Pierwsza linia obrony: zarządzanie operacyjne

Pierwsza linia obrony to głównie menedżerowie niższego i średniego szczebla, którzy zarządzają ryzykiem i kontrolą w codziennych działaniach. Managerowie operacyjni tworzą i wdrażają kontrolę w procesach i zarządzaniu ryzykiem w organizacji. Obejmują one procesy kontroli wewnętrznej służące do identyfikacji i oceny istotnych czynników ryzyka, właściwego wykonania czynności i zadań, wskazania nieodpowiednich procesów, rozwiązywania problemu nieskutecznej kontroli i komunikowania się z głównymi osobami zaangażowanymi w proces. Menedżerowie operacyjni muszą być odpowiednio wykwalifikowani do wykonywania zadań w zakresie swoich obszarów działalności.

Kierownictwo wyższego szczebla ponosi ogólną odpowiedzialność za wszystkie działania pierwszej linii. W niektórych obszarach wysokiego ryzyka może również sprawować bezpośredni nadzór nad menadżerami niskiego i średniego szczebla lub nawet wykonywać samemu niektóre obowiązki pierwszej linii.

Pracownicy pierwszej linii obrony mają znaczące obowiązki dotyczące oceny ryzyka, wykonywa kontroli oraz informacji i komunikacji wynikające ze Struktury Ramowej. Jak wskazano na **Rysunku 4** poniżej, 12 zasad kontroli wewnętrznej przedstawionych w Strukturze Ramowej jest podstawowym obowiązkiem menadżerów operacyjnych:

Rysunek 4. COSO i 1 linia obrony



Druga linia obrony: wewnętrzny monitoring i nadzór

Druga linia obrony obejmuje różne funkcje zarządzania ryzykiem i zgodności stworzone przez kierownictwo w celu zapewnienia, że kontrole i procesy zarządzania ryzykiem wdrożone przez pierwszą linię obrony są odpowiednio zaprojektowane i działają zgodnie z przeznaczeniem. Są to funkcje zarządzania, oddzielone od zarządzania operacyjnego pierwszej linii, ale nadal pod kontrolą i wpływem kierownictwa wyższego szczebla. Podstawowym obowiązkiem funkcji z drugiej linii jest bieżące monitorowanie kontroli i ryzyka. Często ściśle współpracują z menadżerami operacyjnymi, wspierając ich w zdefiniowaniu strategii wdrożenia celów dostarczając wiedzy nt. ryzyka, wdrażaniu polityk i procedur oraz zbieraniu informacji w celu stworzenia mapy ryzyka i kontroli z perspektywy całego przedsiębiorstwa.

Skład drugiej linii może się znacznie różnić w zależności od rozmiaru organizacji i branży w jakiej działa. W dużych, notowanych na giełdzie, złożonych i/lub silnie regulowanych organizacjach wszystkie te funkcje mogą być wydzielone i działać odrębnie. W mniejszych, zarządzanych przez właścicieli, mniej złożonych i/lub mniej regulowanych organizacjach, niektóre funkcje drugiej linii mogą być połączone lub nie istnieją. Na przykład, niektóre organizacje mogą łączyć funkcje prawne i zgodności w jednym dziale lub mogą łączyć dział BHP z działem ochrony środowiska. W niektórych organizacjach wybrane lub wszystkie obowiązki drugiej linii mogą również leżeć w gestii menadżerów pierwszej linii obrony.

Typowe funkcje drugiej linii obejmują wyspecjalizowane grupy, takie jak:

- Zarządzanie ryzykiem
- Bezpieczeństwo informacji
- Kontroling finansowy
- Bezpieczeństwo fizyczne
- Jakość
- BHP
- Inspekcja
- Zgodność
- Prawne
- Ochrona środowiska
- Łańcuch dostaw
- Inne (w zależności od potrzeb branżowy lub samej firmy)

Pod nadzorem kierownictwa, personel drugiej linii monitoruje wybrane kontrole, w celu ustalenia czy działają one zgodnie z ich przeznaczeniem. Monitoring wykonywany przez drugą linię obejmuje zazwyczaj wszystkie trzy cele, przedstawione w Strukturze Ramowej: operacyjne, raportowania i zgodności.

Obowiązki osób w ramach drugiej linii obrony są bardzo zróżnicowane, ale zazwyczaj obejmują:

- Wspieranie zarządzania w zakresie projektowania i rozwoju procesów i kontroli w celu zarządzania ryzykiem.
- Definiowanie działań w celu monitorowania i określenia sposobu pomiaru postępów w stosunku do oczekiwań kierownictwa.
- Monitorowanie adekwatności i skuteczności kontroli wewnętrznej.
- Eskalację krytycznych problemów, pojawiających się zagrożeń i odchyleń.
- Dostarczenie ramowych zasad zarządzania ryzykiem.
- Identyfikację i monitorowanie znanych i pojawiających się problemów, które wpływają na ryzyko i kontrole w organizacji.
- Identyfikację zmian w poziomie apetytu na ryzyko i tolerancji ryzyka w organizacji.
- Dostarczenie wytycznych i szkolenia w zakresie procesów zarządzania ryzykiem i kontroli.

Monitorowanie przez drugą linię obrony powinno być dostosowane do specyficznych potrzeb organizacji. Zazwyczaj te działania są niezależne od codziennych działań operacyjnych. W wielu przypadkach działania monitorujące są rozproszone w całej organizacji. W niektórych organizacjach jednak, funkcje kontrolne mogą być ograniczone do jednego lub kilku obszarów.

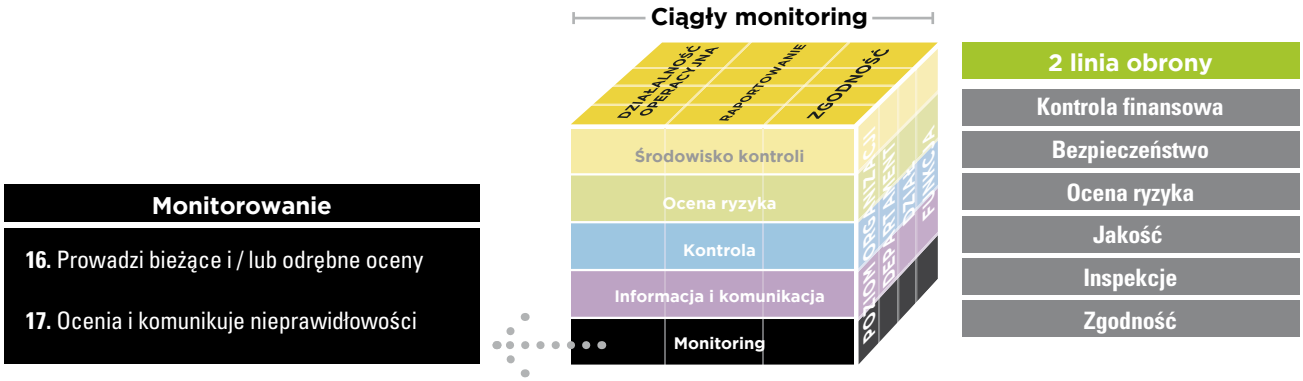
Struktura drugiej linii może się znacznie różnić w zależności od wielkości organizacji i branży.

Struktura drugiej linii może się znacznie różnić w zależności od wielkości organizacji i branży.

Działania drugiej linii są pewnym sensie niezależne od działań pierwszej linii obrony, ale są one, z natury, wciąż funkcjami zarządczymi. Funkcje drugiej linii mogą bezpośrednio rozwijać, wdrażać i/lub modyfikować kontrolę wewnętrzną i procesy ryzyka w organizacji. Mogą również podejmować decyzje w przypadku niektórych działań operacyjnych. Rola drugiej linii obrony może wymagać bezpośredniego jej zaangażowania w działania pierwszej linii obrony. W takim przypadku, nie można mówić o pełnej niezależności drugiej linii od pierwszej.

Znaczenie silnej, skutecznej drugiej linii jest nie do przecenienia, chociaż nie jest ona w pełni niezależna. Oczekuje się, że druga linia będzie działać z odpowiednim stopniem obiektywizmu i będzie dostarczać ważne i przydatne informacje dla kierownictwa wyższego szczebla i Rady w zakresie zarządzania ryzykiem i kontroli wykonywanych przez pierwszą linię obrony. Druga linia może również dostarczyć kierownictwu wyższego szczebla i Radzie informacje na temat całokształtu kontroli i ryzyka w organizacji, które nie są oczekiwane od pierwszej linii. W celu osiągnięcia skuteczności przez drugą linię obrony, musi ona mieć wystarczającą rangę wśród liderów i menadżerów operacyjnych w całej organizacji. Ranga tej funkcji jest związana z jej umiejscowieniem, uprawnieniami oraz bezpośrednim raportowaniem do kierownictwa wyższego szczebla.

Rysunek 5. COSO i 2 linia obrony



Trzecia linia obrony: Audyt wewnętrzny

Audyt wewnętrzny służy organizacji jako trzecia linia obrony. Instytut Audytorów Wewnętrznych definiuje audyt wewnętrzny jako „działalność niezależną i obiektywną, której celem jest przysporzenie wartości i usprawnienie działalności operacyjnej organizacji. Polega na systematycznej i dokonywanej w uporządkowany sposób ocenie procesów: zarządzania ryzykiem, kontroli i ładu organizacyjnego, i przyczynia się do poprawy ich działania. Pomaga organizacji osiągnąć cele dostarczając zapewnienia o skuteczności tych procesów, jak również poprzez doradztwo”[4].

Wśród wielu ról, audyt wewnętrzny dostarcza zapewnienia co do efektywności i skuteczności ładu organizacyjnego, zarządzania ryzykiem i kontroli wewnętrznej. Zakres audytu wewnętrznego może obejmować wszystkie aspekty działalności organizacji.

[4] Międzynarodowe ramowe zasady praktyki zawodowej (IPPF) Altamonte Springs, FL: Instytutu Audytorów Wewnętrznych, 2013. https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20Polish.pdf

Wysoki poziom organizacyjnej niezależności i obiektywizmu odróżnia audyt wewnętrzny od pozostałych dwóch linii obrony. Audytorzy wewnętrzni nie projektują i nie wdrażają kontroli w ramach swoich normalnych obowiązków i nie są odpowiedzialni za działalność operacyjną. W większości organizacji, niezależność audytu wewnętrznego jest dodatkowo wzmocniona przez bezpośrednie raportowanie przez zarządzającego audytem wewnętrznym do Rady. Ze względu na wysoki poziom niezależności, audytorzy wewnętrzni są najlepiej umocowani do dostarczenia Radzie i kierownictwu wyższego szczebla wiarygodnego i obiektywnego zapewnienia o skuteczności ładu organizacyjnego, ryzyka i kontroli.

Rysunek 6. COSO i trzecia linia obrony

Ocena zaprojektowania i wdrożenia

Środowisko kontroli

1. Prezentuje zobowiązanie do uczciwości i wartości etycznych
2. Nadzoruje
3. Ustanawia ramy, nadaje uprawnienia i przypisuje odpowiedzialności
4. Prezentuje zobowiązanie do kompetencji zawodowych
5. Egzekwuje odpowiedzialność / rozliczalność z zadań

Ocena ryzyka

6. Określa odpowiednie cele
7. Identyfikuje i analizuje ryzyko
8. Ocenia ryzyko nadużyć
9. Identyfikuje i analizuje istotne zmiany

Czynności kontrolne

10. Dokonuje wyboru i tworzy działania kontrolne
11. Dokonuje wyboru i tworzy ogólne kontrole IT
12. Wprowadza kontrole poprzez polityki i procedury

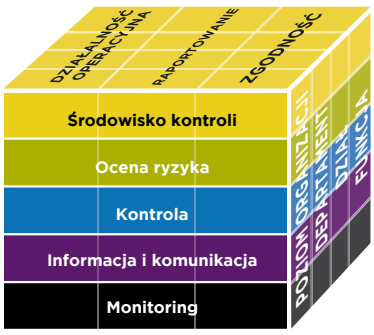
Informacja i komunikacja

13. Wykorzystuje odpowiednie informacje
14. Komunikuje wewnętrznie
15. Komunikuje na zewnątrz

Monitorowanie

16. Prowadzi bieżące i / lub odrębne oceny
17. Ocenia i komunikuje nieprawidłowości

Zapewnienie skuteczności



3 linia obrony

Audyt wewnętrzny

Audyt wewnętrzny aktywnie przyczynia się do skutecznego ładu organizacyjnego przy założeniu, że określone warunki sprzyjające jego niezależność i profesjonalizmowi są spełnione. Stworzenie profesjonalnego działu audytu wewnętrznego powinno być priorytetem dla każdej organizacji. Jest to ważne nie tylko dla większych organizacji, ale także dla mniejszych podmiotów. Mniejsze organizacje mogą funkcjonować bardzo złożonym otoczeniu, posiadając mniej formalną, ale sprawną strukturę organizacyjną, której celem jest zapewnienie skuteczności ładu organizacyjnego i zarządzania ryzykiem. Mniejsze organizacje mogą również nie posiadać skutecznej drugiej linii obrony. Każda organizacja powinna ustanowić i utrzymywać niezależny, odpowiedni i kompetentny personel audytu wewnętrznego. Raportowanie powinno odbywać się na wystarczająco wysokim poziomie w organizacji, aby funkcja audytu mogła wykonywać swoje obowiązki z zachowaniem niezależności. Jednocześnie jej działanie winno odbywać się zgodnie z uznanymi na całym świecie standardami (takich jak Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego).

Audytorzy zewnętrzni, regulatorzy i inne organy zewnętrzne

Mimo, że podmioty spoza organizacji nie są formalnie zaliczane do jej trzech linii obrony, audytorzy zewnętrzni czy regulatorzy często odgrywają ważną rolę w zakresie ogólnego ładu organizacyjnego i schematów kontroli. Regulatorzy często ustanawiają wymogi mające na celu wzmocnienie ładu organizacyjnego i kontroli. Aktywnie przeprowadzają przeglądy i raportują o organizacjach, które nadzorują. Audytorzy zewnętrzni mogą dostarczyć ważnych spostrzeżeń i ocen kontroli dotyczących sprawozdawczości finansowej oraz ryzyk z nią związanych.

Audytorów zewnętrznych, regulatorów i inne grupy spoza organizacji można uznać za dodatkowe linie obrony, jeżeli ich działania są skutecznie koordynowane. Dostarczają oni merytorycznych opinii i spostrzeżeń interesariuszom, w tym Radzie i kierownictwu wysokiego szczebla.

Jednakże ich praca ma inne, bardziej ukierunkowane lub sprecyzowane cele. Dlatego też kwestie podlegające weryfikacji są mniej obszerne niż te, oceniane przez funkcjonujące w organizacji linie obrony.
Na przykład, szczegółowe audyty regulatora mogą być skoncentrowane wyłącznie na kwestii zgodności, bezpieczeństwa lub innych tematach o ograniczonym zakresie, podczas gdy trzy linie obrony z natury rzeczy obejmują cały zakres ryzyk związanych z działalnością operacyjną, sprawozdawczością i zgodnością.
Pomimo, że audytorzy zewnętrzni i regulatorzy przekazują cenne informacje, nie powinni być traktowani jako substytut linii obrony w organizacji. Odpowiedzialnością organizacji, a nie podmiotów zewnętrznych, jest zarządzanie jej ryzykami.

II. Strukturyzacja i koordynacja trzech linii obrony

Kształtowanie się trzech linie obrony

Model Trzech Linii Obrony został zaprojektowany w sposób zapewniający elastyczność w jego stosowaniu. Każda organizacja, wdrażając ten model, powinna uwzględnić branżę, w której działa, wielkość, strukturę operacyjną i podejście do zarządzania ryzykiem. Jednakże ład organizacyjny i środowisko kontroli są najsilniejsze jeśli trzy linie obrony są wyodrębnione i jasno zdefiniowane. Organizacje powinny dążyć do wdrożenia struktury ładu organizacyjnego spójnego z Modelem, tak aby w dowolnych formach istniały wszystkie trzy linie obrony, niezależnie od wielkość i złożoności organizacji. Linie obrony powinny być wydzielone, charakteryzować się odrębnością ról i obowiązków, które zostały jasno zdefiniowane w odpowiednich politykach i procedurach oraz wzmocnione przez spójny i konsekwentny przekaz kierownictwa.

Określenie specyfiki linii obrony jest uzależnione od indywidualnych potrzeb organizacji. W pewnych sytuacjach, np. małych firmach, lub jeśli pewne funkcje są w okresie przejściowym linie obrony mogą nie być jednoznacznie wydzielone. Na przykład, w przypadku wprowadzenia funkcji zarządzania ryzykiem po raz pierwszy, niektóre organizacje mogą wykorzystywać istniejące struktury jako czynnik przyspieszający wdrożenie. W sytuacjach, w których kompetencje poszczególnych linii obrony nie są wyraźnie oddzielone od siebie, Rada powinna dokładnie rozważyć możliwe konsekwencje takiego rozwiązania. O ile to możliwe, rozwiązanie takie sytuacje powinny być krótkotrwałe, a wraz z procesem dojrzewania linii obrony należy rozdzielić ich kompetencje.

Jeśli tak się nie dzieje, Rada powinna zdać sobie sprawę z wpływu braku rozdzielenia funkcji operacyjnych od funkcji zapewniających w kontekście niepowodzenia w stworzeniu trzech oddzielnych linii obrony.
Przy rozważaniu lub przypisywaniu konkretnych obowiązków oraz koordynowaniu działań dotyczących kontroli i ryzyka w organizacji, pomocna może być znajomość podstawowych ról poszczególnych grup w Modelu.

Rysunek 7. Różnice pomiędzy trzema liniami obrony

Funkcje zarządcze		Zapewnienie
Pierwsza linia obrony	**Druga linia obrony**	**Trzecia linia obrony**
Zarządzenie operacyjne	Ograniczona niezależność Raportowanie głównie do kierownictwa Zapewnienie	Audyt wewnętrzny Większa niezależności Raportowanie do Organu odpowiedzialnego za ład organizacyjny / Rady

Ponieważ niezależność organizacyjna i obiektywizm są zasadniczymi cechami trzeciej linii obrony, należy zachować szczególną ostrożność w przypadku, kiedy organizacja łączy funkcję audytu wewnętrznego z jakąkolwiek rolą drugiej linii obrony. Jeśli funkcja audytu wewnętrznego jest połączona z jakąkolwiek funkcją drugiej linii, Rada powinna upewnić się, że to połączenie lub sposób zarządzania tymi funkcjami nie naruszają niezależności i/lub obiektywności funkcji audytu wewnętrznego. Zwykle audytorzy wewnętrzni nie powinni przyjmować żadnych obowiązków kierownictwa w zakresie audytowanego obszaru, a w organizacjach gdzie audyt wewnętrzny jest włączony w działania drugiej linii obrony, zaangażowanie w kwestie pozaaudytowe powinno być dopuszczone krótkoterminowo, natomiast konfliktowe role powinny być delegowane na inne jednostki lub grupy. Jeśli zaangażowanie audytu w zadania drugiej linii obrony nie ma charakteru krótkoterminowego, Rada powinna uwzględnić ograniczoną zdolność dostarczania przez audyt wewnętrzny niezależnego i obiektywnego zapewnienia w stosunku do tych działań i, w konsekwencji, z koniecznością pozyskania od podmiotów zewnętrznych zapewnienia w zakresie przekazanych audytowi wewnętrznemu obowiązków drugiej linii obrony.

Koordynacja trzech linii obrony

Trzy linie obrony mają ostatecznie takie same zadania: pomóc organizacji w osiąganiu jej celów z wykorzystaniem skutecznego zarządzania ryzykiem. Obsługują również tych samych końcowych interesariuszy i często mają te same spostrzeżenia w zakresie ryzyka i kontroli. Kierownictwo wyższego szczebla i Rada powinny jasno zakomunikować, że oczekują wymiany informacji i koordynacji pomiędzy trzema liniami obrony, zapewniając w ten sposób ogólną skuteczność działań, bez umniejszania roli żadnej z kluczowych funkcji. Na przykład, w celu wyrażenia tych oczekiwań wiele organizacji wydaje polityki w zakresie zarządzania ryzykiem z poziomu kierownictwa wyższego szczebla lub Rady.

Nie należy mylić pojęcia koordynacji i komunikacji ze strukturą organizacyjną. Mimo posiadania tych samych celów, każda linia obrony ma swoją odrębną rolę i zakres obowiązków. Pomimo, że linie obrony są rozłączne, nie powinny działać w izolacji. Powinny dzielić się informacjami i koordynować działania w zakresie ryzyk, kontroli i ładu organizacyjnego. Niejednokrotnie linie obrony mogą mieć wspólną wizję ryzyk i kontroli.

Staranna koordynacja jest niezbędna do uniknięcia powielania czynności mających na celu zapewnienie, że wszystkie istotne ryzyka są właściwie zaadresowane. Koordynacja jest również istotna z uwagi na Standard 2050, który stanowi, że: „w celu zapewnienia odpowiedniego zakresu audytu i minimalizacji powielania wysiłków, zarządzający audytem wewnętrznym powinien wymieniać informacje i koordynować działania zarówno z wewnętrznymi, jak i zewnętrznymi wykonawcami usług zapewniających i doradczych” [5].

Przy wprowadzaniu w życie działań korygujących najistotniejsze jest, aby kluczowe funkcje wykonawcze takie jak członek zarządu nadzorujący ryzyko lub dyrektor zarządzający ryzykiem), członek zarządu nadzorujący zgodność lub dyrektor ds. zgodności, lub zarządzający audytem wewnętrznym, były uważnie przeanalizowane i ustrukturyzowane tak, aby umożliwić im wykonywanie jedynych w swoim rodzaju obowiązków podczas koordynacji i komunikacji z innymi dyrektorami zajmującymi się ryzykiem i kontrolą.

Pierwsza linia obrony jest podstawowym właścicielem ryzyka i metod zarządzania nim. Druga linia obrony dostarcza wiedzy eksperckiej w zakresie ryzyka, pomaga ustalić wdrożenie strategii i wspomaga implementację polityk i procedur. Pomimo, że obie linie obrony różnią się zakresem obowiązków odnośnie ryzyk i kontroli, kluczowe jest, aby pracowały wspólnie, używały tej samej terminologii, rozumiały przygotowane przez siebie oceny ryzyk występujących w organizacji i, jeśli jest to możliwe, wykorzystywały wspólny zestaw narzędzi i procesów.

[5] Międzynarodowe ramowe zasady praktyki zawodowej (IPPF) Altamonte Springs, FL: Instytutu Audytorów Wewnętrznych, 2013. https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20Polish.pdf

Przy wprowadzaniu w życie działań korygujących najistotniejsze jest, aby kluczowe funkcje wykonawcze takie jak członek zarządu nadzorujący ryzyko lub dyrektor zarządzający ryzykiem[6], członek zarządu nadzorujący zgodność lub dyrektor ds. zgodności[7], lub zarządzający audytem wewnętrznym (ang. Chief Audit Executive (CAE)), były uważnie przeanalizowane i ustrukturyzowane tak, aby umożliwić im wykonywanie jedynych w swoim rodzaju obowiązków podczas koordynacji i komunikacji z innymi dyrektorami[8] zajmującymi się ryzykiem i kontrolą.

Pierwsza linia obrony jest podstawowym właścicielem ryzyka i metod zarządzania nim. Druga linia obrony dostarcza wiedzy eksperckiej w zakresie ryzyka, pomaga ustalić wdrożenie strategii i wspomaga implementację polityk i procedur. Pomimo, że obie linie obrony różnią się zakresem obowiązków odnośnie ryzyk i kontroli, kluczowe jest, aby pracowały wspólnie, używały tej samej terminologii, rozumiały przygotowane przez siebie oceny ryzyk występujących w organizacji i, jeśli jest to możliwe, wykorzystywały wspólny zestaw narzędzi i procesów.

Funkcja audytu wewnętrznego w organizacji stanowi trzecią linię obrony i w swoim zakresie działania powinna obejmować wszystkie istotne ryzyka i czynności kontrolne w organizacji. Komunikacja z pierwszą i drugą linią obrony pomoże audytowi wewnętrznemu wykorzystywać podobną terminologię w zakresie ryzyka i rozumieć sposób postrzegania ryzyka przez obie linie.

Audyt wewnętrzny powinien również koordynować swoje działania z drugą linią obrony. Koordynacja może przybrać wiele form w zależności od organizacji, określonych zadań wykonywanych przez każdą ze stron, poziomu organizacyjnej niezależności drugiej linii obrony oraz oczekiwań kierownictwa wyższego szczebla i Rady. W pewnych przypadkach audyt wewnętrzny może wykorzystać prace wykonane przez funkcje z drugiej linii obrony i częściowo oprzeć na nich swoją opinię. W takich okolicznościach audyt wewnętrzny powinien upewnić się, aby prace wykonane przez drugą linię obrony były odpowiednio zaprojektowane, zaplanowane, nadzorowane, udokumentowane i sprawdzone. Zakres wykorzystania i poziom zaufania do prac wykonywanych przez inne funkcje może się różnić w zależności od okoliczności. Audyt wewnętrzny powinien także zwracać szczególną uwagę na niezależność organizacyjną funkcji z drugiej linii obrony, której prace planuje wykorzystać w części swojego zadania. Audyt wewnętrzny jest umiejscowiony w strukturze organizacyjnej tak, aby móc przedstawiać bezstronną i obiektywną ocenę. Funkcja, na której pracy audyt zamierza polegać, powinna odznaczać się dostatecznie wysokim poziomem niezależności i obiektywności.

Potencjał i efektywność nie są jedynymi kryteriami, którymi należy się kierować przy korzystaniu z wyników działań innych funkcji. Możliwości pierwszej linii obrony do wykonywania pracy na rzecz audytu wewnętrznego nie oznacza potrzeby zapewnienia jej niezależności i obiektywności. Podobnie, możliwość wykonywania przez audyt wewnętrzny prac na rzecz pierwszej lub drugiej linii obrony nie oznacza, że nie zostaje zapewniona organizacyjna niezależność i obiektywność audytu wewnętrznego podczas wykonania tych zadań.

W celu zapewnienia efektywnej koordynacji, Karta Audytu Wewnętrznego powinna zawierać zapisy o odpowiedzialności audytu wewnętrznego za przeprowadzenie oceny wydajności i efektywności działania funkcji z drugiej linii obrony lub działań podmiotu zewnętrznego, które mają być wykorzystane przez audyt wewnętrzny.
Koordynacja może rozciągać się poza trzy linie obrony włączając inne podmioty zewnętrzne, takie jak audytorzy zewnętrzni. Audytorzy wewnętrzni mogą polegać na pracy wewnętrznych lub zewnętrznych dostawców, w zakresie zapewnienia dotyczącego ładu organizacyjnego, zarządzania ryzykiem i kontroli, o ile mają niezbędny poziom zrozumienia wykonanej pracy, szczegółowych rezultatów, niezależności i kompetencji podmiotów zewnętrznych. Odwrotnie, audyt wewnętrzny może planować i wykonywać prace na rzecz podmiotów zewnętrznych. Koordynacja współpracy z podmiotami zewnętrznymi może wpływać na wzrost wydajności, jednakże zarządzający audytem wewnętrznym i Rada powinni rozważyć zarówno koszty jak i możliwe korzyści z wykorzystania działań audytu wewnętrznego przez podmioty zewnętrzne.

[6] dyrektor zarządzający ryzykiem (ang. Chief Risk Oficer (CRO))

[7] członek zarządu nadzorujący zgodność lub dyrektor ds. zgodności (ang. Chief Compliance Oficer (CCO))

[8] dyrektorami (ang. executives)

III. Wykorzystanie COSO w modelu Trzech linii obrony

Założenia koncepcyjne definiują pięć komponentów kontroli wewnętrznej oraz 17 zasad prezentujących podstawowe koncepcje związane z tymi komponentami. Publikacja Kontrola Wewnętrzna – Zintegrowana Struktura Ramowa – COSO I stanowi, że skoro 17 zasad wynika bezpośrednio z pięciu komponentów kontroli wewnętrznej, skuteczna kontrola wewnętrzna może być zapewniona dzięki wdrożeniu każdej z tych zasad.
Kierownictwo odpowiada za wyznaczenie kluczowych zadań w odniesieniu do wskazanych 17 zasad i upewnienie się, że zadania te są wykonywane zgodnie z założeniami.

Aneks zawiera przykłady, w jaki sposób obowiązki wynikające z 17 zasad mogą być podzielone pomiędzy trzy linie obrony. Kontrola Wewnętrzna – Zintegrowana Struktura Ramowa – COSO I wskazuje także różne zagadnienia odnoszące się do 17 zasad. Ponieważ wiele z tych punktów odnosi się do kluczowych obowiązków osób z trzech linii obrony, czytelnicy którzy znają dokument Kontrola Wewnętrzna – Zintegrowana Struktura Ramowa – COSO I zauważą, że wiele z zagadnień zostało uwzględnionych w następnej sekcji.

Informacje zawarte w aneksie maja służyć zilustrowaniu przykładów, jak zadania mogą zostać rozdzielone pomiędzy trzy linie obrony. Ponieważ każda organizacja jest inna więc role i obowiązki mogą być zdefiniowane odmiennie niż zaprezentowano. Bez względu na to, jak zadania zostały podzielone w organizacji, szczególne role i obowiązki odnoszące się do 17 zasad powinny być jasno zdefiniowane i przekazane odpowiednim jednostkom w celu uniknięcia luk w pokryciu procesów kontrolami wewnętrznymi i niepotrzebnego duplikowania zadań.

IV Wnioski

Każda organizacja powinna jasno określić zakresy odpowiedzialności w odniesieniu do ładu organizacyjnego, ryzyka i kontroli, w celu zminimalizowania luk w kontrolach i wyeliminowania zbędnych czynności odnoszących się do zarządzania ryzykiem i kontroli. Model Trzech Linii Obrony wyjaśnia kluczowe role i zadania w organizacji i jest skutecznym narzędziem wspierającym komunikację w zakresie ryzyk i kontroli. Model może być wykorzystywany do wyjaśniania, w jaki sposób obowiązki w zakresie ryzyka i kontroli mogą być koordynowane wewnątrz organizacji.

Bazowym założeniem modelu jest to, że pod nadzorem i przewodnictwem kierownictwa wyższego szczebla i Rady, trzy oddzielne linie obrony są niezbędne do skutecznego zarządzania ryzykiem i skutecznej kontroli.
Trzy linie:

- **Są właścicielami i zarządzają** ryzykami i kontrolą (kierownictwo operacyjne).

- **Monitorują** ryzyka i kontrolę wspierając kierownictwo (powołane przez kierownictwo funkcje zarządzania ryzykiem, kontrolne i zgodności).

- **Dostarczają Radzie i kierownictwu** wyższego szczebla niezależnego zapewnienia o skuteczności zarządzania ryzykiem i kontrolą (audyt wewnętrzny).

Każda z tych trzech „linii" ma szczególną rolę w strukturze ładu organizacyjnego organizacji i jeśli skutecznie wykonują one swoje role, prawdopodobieństwo wystąpienia istotnej słabości systemu kontroli jest ograniczone. Powyższa struktura także wspiera Radę dostarczając jej bezstronnej informacji o najistotniejszych ryzykach, na które narażona jest organizacja oraz w jaki sposób kierownictwo z nimi postępuje.

Model Trzech Linii Obrony może być wykorzystywany w połączeniu z dokumentem Kontrola Wewnętrzna – Zintegrowana Struktura Ramowa – COSO I, aby ułatwić osobom z każdej z linii obrony zrozumienie pełnego zakresu ich odpowiedzialności w odniesieniu do ryzyka i kontroli oraz. jak ich zadania odnoszą się do ogólno organizacyjnej struktury zarządzania ryzykiem i kontrolą.

Kluczowe obserwacje

1. Kierownictwo wyższego szczebla i Rada ponoszą ostateczną odpowiedzialność w zakresie zapewnienia wydajności i skuteczności ładu organizacyjnego, zarządzania ryzykiem i procesów kontrolnych.

2. Zarządzanie ryzykiem jest pełniejsze w tych organizacjach, w których trzy linie obrony są jednoznacznie wyodrębnione i identyfikowalne. Wszystkie trzy linie obrony powinny istnieć w określonych formach w każdej organizacji, niezależnie od jej wielkości i złożoności.

3. Każda linia obrony powinna odznaczać się jasno określoną rolą i zakresem obowiązków wspieranych przez odpowiednie polityki, procedury i mechanizmy raportowania.

4. Powinna następować wymiana informacji pomiędzy wszystkimi liniami obrony w celu poprawy skuteczności i uniknięcia duplikowania wysiłków w dostarczaniu zapewniania, że istotne ryzyka zostały odpowiednio zaadresowane.

5. Linie obrony nie powinny być łączone, a koordynacja ich zadań nie powinna negatywnie wpływać na ich skuteczność. Każda z linii obrony ma unikalne miejsce w organizacji i odrębny zakres zadań. Należy zwrócić szczególną uwagę na przypadki łączenia funkcji w ramach trzech linii obrony. Skuteczność drugiej i trzeciej linii obrony może ucierpieć, jeżeli zostanie naruszona unikalność linii. Potencjał i wydajność nie są jedynymi kryteriami, którymi należy się kierować. Niezależność i obiektywizm są równie ważnymi kwestiami.

Załącznik

Zasada 1 Organizacja zobowiązuje się do uczciwości w działaniu i poszanowania wartości etycznych			
Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
Wszystkie linie obrony, poprzez wydawane przez nie dyspozycje, działania i postawy powinny wskazywać na istotność uczciwości i poszanowania wartości etycznych.			
• Zarządza poprzez dawanie przykładu we wdrażaniu wartości i filozofii oraz styl kierowania organizacją. • Wdraża cele, programy i działania wspierające postawy etyczne. • Tworzy i wdraża procesy służące ocenie jednostek i zespołów z punktu widzenia standardów postępowania.	• Określeni członkowie drugiej linii obrony mogą być proszeni o wsparcie „gorących linii" telefonicznych, podejmowanie działań wyjaśniających ewentualne działania niepożądane lub pełnienie określonych zadań związanych z zachowaniem uczciwości i wartości etycznych	• Ocenia poziom etyki w organizacji oraz efektywność strategii, taktyk, komunikacji i innych procesów służących osiąganiu pożądanego poziomu przestrzegania norm prawnych i etycznych. • Ocenia sposób zaprojektowania, wdrażania i skuteczności realizacji celów, programów i działań związanych z etyką. • Dostarcza zapewnienia, że programy promujące wartości etyczne osiągają zamierzone cele, kluczowe ryzyka są skutecznie zarządzane, a kontrole działają prawidłowo. • Dostarcza usług doradczych, aby wspomóc organizację w tworzeniu trwałych programów promowania wartości etycznych i podnoszących efektywność przestrzegania norm etycznych do oczekiwanego poziomu.	• Rada odpowiada za określenie kultury organizacyjnej podmiotu. W związku z tym, przekazuje informacje odnośnie oczekiwanych postaw w kwestii uczciwości, wartości etycznych i standardów zachowań.

Zasada 2 Rada jest niezależna od kierownictwa i sprawuje nadzór nad rozwojem i działaniem kontroli wewnętrznej.			
Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
• Wyposaża zarząd w odpowiednie informacje dotyczące rozwoju i działania kontroli wewnętrznej, w celu umożliwienia mu spełnienia powierzonych obowiązków.	• Rada jest wspierana przez struktury i procesy stworzone przez kierownictwo na szczeblu wykonawczym. Powyższe wsparcie może być zapewnione zarówno przez pierwszą, jaki i drugą linię obrony. Na przykład albo komitet stworzony przez kierownictwo, albo druga linia obrony mogą koncentrować się na aspektach takich jak IT lub zgodność.	• Dostarcza zapewnienia w zakresie rozwoju i działania kontroli wewnętrznych, oceniając czy kontrole są odpowiednio zaprojektowane, skutecznie wdrożone i działają zgodnie z zamierzeniami.	• Rada jest odpowiedzialna za zapewnienie w swoim składzie, odpowiednich członków niezależnych od kierownictwa i obiektywnych w ocenach i podejmowaniu decyzji. • Rada zachowuje odpowiedzialność w zakresie kształtowania struktur kierownictwa, wdrażania i sterowania kontrolą wewnętrzną. - **Środowisko Kontroli** – ustala zasady uczciwości i wartości etyczne, struktury nadzorcze, mianuje osoby odpowiedzialne, wyznacza zakresy ich odpowiedzialności, oczekiwane kompetencje i zasady rozliczania przez Radę. - **Ocena Ryzyka** – Wraz z kierownictwem określa akceptowalny poziom ryzyka, nadzoruje szacunki ryzyka nieosiągnięcia celów przeprowadzone przez kierownictwo i dołącza ocenę prawdopodobnego wpływu zmian, oszustw i obchodzenia kontroli przez kierownictwo. - **Działania Kontrolne** – nadzoruje kierownictwo wyższego szczebla w zakresie rozwijania i wykonywania działań kontrolnych. - **Informacja i Komunikacja** – analizuje i omawia informacje odnoszące się do osiągania celów przez organizację. - **Monitoring** – ocenia i nadzoruje naturę oraz zakres monitoringu wykonywanego przez kierownictwo, a także wyniki i podejmowane działania. • Rada spotyka się z audytem wewnętrznym i potencjalnie także z osobami z drugiej linii obrony niezależnymi od kierownictwa.

[10] *Przypis tłumacza:* W polskim systemie prawnym Walne Zgromadzenie wybiera skład Rady Nadzorczej, w tym niezależnych członków, obiektywnych w ocenie i podejmowaniu decyzji.

Zasada 3. Dla osiągnięcia celów organizacji kierownictwo, pod nadzorem Rady ustala struktury, linie raportowania, odpowiednie uprawnienia i zakresy odpowiedzialności.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
Wszystkie linie obrony, poprzez wydawane przez nie dyspozycje, działania i postawy powinny wskazywać na istotność uczciwości i poszanowania wartości etycznych.			
• Dla osiągania celów ustala struktury, linie raportowania, udziela umocowania i określa zakresy kompetencji. • Umożliwiając Radzie sprawowanie nadzoru, przekazuje mu informacje o strukturach, liniach raportowania, uprawnieniach i zakresie odpowiedzialności.	• Podczas realizacji swoich zadań współpracuje z kierownictwem, komórkami organizacyjnymi, funkcjami eksperckimi i nadzorczymi, a jej zakres odpowiedzialności jest odpowiednio dostosowany do realizacji jej zadań.	• W zakresie realizacji swoich celów dostarcza zapewnienia, że struktury operacyjne organizacji, linie raportowania, uprawnienia i zakresy odpowiedzialności są odpowiednie i skuteczne. W celu realizacji swoich zadań, zgodnie z Kartą Audytu Wewnętrznego, wdraża procedury i praktykę oraz uwzględnia odpowiednie linie raportowania i umocowane funkcje. • Okresowo dostarcza Radzie potwierdzenie swojej niezależności i obiektywności.	• W ramach swoich obowiązków Rada zatwierdza cele ogólne organizacji i jest odpowiedzialna za nadzór nad rozwojem i utrzymywaniem struktur, linii raportowania oraz uprawnieniami i zakresem odpowiedzialności. • Rada wydaje odpowiednie regulaminy w celu powołania swoich komitetów, w tym również komitetu audytu. • Komitet audytu zatwierdza odpowiednie regulaminy funkcji zajmujących się analizą ryzyka i kontrolą, w tym również audytu wewnętrznego.

Zasada 4. Organizacja, zgodnie z jej celami, zobowiązuje się do pozyskiwania, rozwoju i utrzymywania kompetentnych osób.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
• Zgodnie z wyznaczonymi celami pozyskuje kompetentne osoby, dba o ich rozwój i zatrzymanie w organizacji.	• Aby zrealizować cele pozyskuje kompetentne osoby i dba o rozwój ich talentów. • Zapewnia, że pracownicy i ich zadania są odpowiednio dostosowane do poziomu zarządzania; • Uwzględniając rotację pracowników na poziomie różnych funkcji kierowniczych.	• W celu realizacji misji i celów statutowych pozyskuje, zatrudnia, dba o rozwój i utrzymuje kompetentnych i utalentowanych pracowników. • Może oceniać i dostarczać zapewnienia odnośnie wydajności i skuteczności polityk i procedur takich jak: - Polityki kadrowe - Programy szkoleniowe rozwoju - Plany wynagradzania - Plany sukcesji.	• Rada sprawuje nadzór, w celu zapewnienia, że kierownictwo zobowiązuje się do pozyskiwania, zapewnienia rozwoju i utrzymywania zatrudnienia kompetentnych osób zgodnie z celami. • Komitety wchodzące w skład Rady zapewniają, że nadzorowane funkcje dysponują kompetentną i utalentowaną kadrą. • Komitet do spraw wynagrodzeń zapewnia, że plany premiowania i wynagradzania są spójne z poziomem apetytu na ryzyko i długofalowymi celami organizacji.

Zasada 5. Organizacja zatrudnia osoby odpowiedzialne za realizację obowiązków kontrolnych w dążeniu do osiągnięcia celu.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
• Zapewnia zatrudnienie osób odpowiedzialnych za wykonanie kontroli, za które są odpowiedzialne w procesie realizacji celów. • Odpowiedzialność ta dotyczy komunikowania określonych obowiązków, wdrożenia systemu ocen oraz wdrożenia procesu zarządzania zasobami ludzkimi nakierowanego na utrzymywanie zatrudnienia osób odpowiedzialnie wykonujących swoje zadania.	• Na podstawie delegacji kierownictwa pracownicy drugiej linii obrony monitorują i raportują wykonanie określonych obowiązków kontrolnych.	• Dostarcza zapewnienia odnośnie wykonania określonych obowiązków kontrolnych. • Audytorzy wewnętrzni mogą wydawać rekomendacje w kwestii odpowiedzialności, jednak standardowo nie mają bezpośredniego umocowania do wydawania decyzji odnośnie działań personelu lub procesów zaprojektowanych tak, aby utrzymać odpowiedzialność pracowników za wykonanie obowiązków kontrolnych.	• Rada jest odpowiedzialna za zapewnienie, że kierownictwo zatrudnia osoby odpowiedzialne za wykonywanie obowiązków kontrolnych. • Komitet do spraw wynagrodzeń jest odpowiedzialny za powiązanie planów premiowania i wynagrodzenia z celami organizacji.

Zasada 6. Organizacja określa wystarczająco czytelne cele umożliwiając identyfikację i ocenę ryzyk związanych z tymi celami.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
Wszystkie podmioty będące częścią systemu kontroli wewnętrznej powinny rozumieć ogólne strategie i cele wyznaczone przez organizację.			
• Wyznaczanie celów jest kluczowym procesem zarządzania zawiązanym z planowaniem strategicznym. • Pod nadzorem Rady wyznacza cele na poziomie jednostek organizacyjnych, które są spójne z misją, wizją oraz strategiami organizacji. • Wyznacza odpowiednie cele, z uwzględnieniem koniecznych szczegółów, tak aby ryzyko ich nieosiągnięcia było identyfikowalne i mogło podlegać ocenie. • Dla określonych ryzyk nakłada poziomy tolerancji. • Celom wyznaczonym na poziomie podmiotu podporządkowuje cele szczegółowe, które są kaskadowane na niższe szczeble organizacji. • Zarówno cele na poziomie podmiotu, jak i powiązane z nimi cele szczegółowe, powinny być konkretne, mierzalne, osiągalne, istotne i określone w czasie.	• Nie odpowiada za wyznaczanie lub zatwierdzanie celów na poziomie podmiotu jako całości, ale może być zobowiązana do opracowania, wdrażania, monitorowania i raportowania celów ogólnych i szczegółowych związanych z konkretnymi dziedzinami specjalizacji, dotyczących zgodności (compliance) lub kontroli jakości. • Ocenia, czy rozważono odpowiedni poziom apetytu na ryzyko i poziomy akceptacji ryzyk.	• Sprawdza, czy wyznaczono cele są konkretne, mierzalne, osiągalne, istotne i określone w czasie. - Przegląd procesu wyznaczania celów na – poziomie podmiotu może być przeprowadzony jako samodzielne zadanie audytowe. - Konkretne cele lub cele szczegółowe mogą być również przedmiotem przeglądów audytu wewnętrznego w ramach wypełniania jego innych zadań. • W celu zachowania niezależności organizacyjnej, audytorzy wewnętrzni zwykle nie wyznaczają celów innych niż dotyczące funkcji audytu wewnętrznego.	• Rada odpowiada za nadzór nad wyznaczaniem celów, pomaga zapewnić, że cele ogólne odzwierciedlają decyzje odnośnie tego, jak organizacja będzie tworzyć, utrzymywać oraz realizować wartość dla interesariuszy. • Rada wraz z kierownictwem ustala odpowiednie poziomy tolerancji i apetytu na ryzyko oraz zapewnia ich komunikację wewnątrz organizacji.

Zasada 7. Organizacja identyfikuje wewnętrzne ryzyka zagrażające osiągnięciu celów i analizuje sposób zarządzania nimi.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
• Identyfikuje i kontroluje ryzyka zagrażające osiągnięciu celów. • Definiuje poziom tolerancji i apetyt na ryzyko organizacji, tworzy system zarządzania ryzykiem, definiuje zakresy odpowiedzialności w obszarze kontroli określonych ryzyk nadzorowanych przez zarząd.	• Funkcja zarządzania ryzykiem korporacyjnym[11] może otrzymać istotne uprawnienia w zakresie zarządzania ryzykiem i jego kontrolą. Typowe zadania mogą zawierać: - Stworzenie wspólnego języka ryzyka lub słownika terminów związanych z ryzykiem. - Opis apetytu na ryzyko i poziomu tolerancji ryzyk w organizacji. - "Rejestr/mapa ryzyk" zawierający zidentyfikowane i opisane ryzyka. - Wdrożenie metodologii kwantyfikowania ryzyka, w celu ustalenia hierarchii ryzyk wewnątrz konkretnej funkcji oraz pomiędzy poszczególnymi funkcjami. - Utworzenie komitetu zarządzania ryzykiem i/lub powołanie dyrektora zarządzającego ryzykiem do koordynacji określonych działań innych funkcji zarządzających ryzykiem. - Wyznaczenie właścicieli ryzyk i ich kompetencji. - Utworzenie planu działań zapewniających, że ryzyka są odpowiednio zarządzane. - Stworzenie skonsolidowanego raportowania dla różnych interesariuszy. - Monitorowanie wyników działań podjętych w celu ograniczenia ryzyk. - Zapewnianie efektywnego pokrycia ryzyk przez audytorów wewnętrznych, zespoły konsultingowe oraz inne podmioty oceniające. - Rozwinięcie ramowych zasad zarządzania ryzykiem umożliwiających uczestnictwo podmiotom trzecim i zdalnym pracownikom. • Określone grup, takich jak bezpieczeństwo (security) czy zgodność (compliance), które mogą wspierać kierownictwo w identyfikacji ryzyk w ich obszarach odpowiedzialności, z uwzględnieniem poziomu apetytu na ryzyko wyznaczonym przez kierownictwo dla określonych działań lub części organizacji.	• Opracowuje plan audytu oparty na ryzyku i uwzględnia ramowe zasady ryzyka organizacji. • Może wspierać pewne działania dotyczące zarządzaniem ryzykami o ile nie naruszają one zachowania niezależności i obiektywności. • Przy tworzeniu planu audytu wewnętrznego może wziąć pod uwagę: - Identyfikację i ocenę ryzyk nieodłącznych i rezydualnych. - Kontrole ograniczające ryzyko, plany ciągłości i działania monitorujące określone ryzyka. - Dokładność i kompletność rejestrów ryzyk. - Prawidłowość dokumentacji w zakresie zarządzania ryzykiem i działań kontrolnych.	• Rada opracowuje strategię ogólną organizacji i jej cele, z uwzględnieniem zrozumienia ryzyk powiązanych ze strategią. • Rada nadzoruje i zapewnia odpowiednie kierownictwo, odpowiedzialne za identyfikację i zarządzanie ryzykami w sposób zapewniający osiągnięcie celów.

[11] zarządzanie ryzykiem korporacyjnym (ang. Enterprise Risk Management (ERM))

Zasada 8. W ocenie ryzyka nieosiągnięcia celów organizacja uwzględnia możliwość wystąpienia oszustw.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
• Wdraża procesy służące identyfikacji, zapobieganiu i wykrywaniu oszustw. • Razem z audytem wewnętrznym i zewnętrznym przeprowadza przeglądy mające na celu określenie poziomu ryzyka wystąpienia oszustw, na jakie jest narażona organizacja.	• Upewnia się, że ocena ryzyk i kontroli uwzględnia ryzyko wystąpienia oszustw.. • Grupy jednostek biorących udział w wyjaśnianiu oszustw odgrywają kluczową rolę w zapobieganiu ich występowania i wykrywania. Powyższe jednostki mogą być zobowiązane do tworzenia i monitorowania polityk i procedur mówiących o zapobieganiu oszustwom w organizacji.	• Standardy wymagają od audytorów wewnętrznych działania z należytą starannością zawodową i z uwzględnieniem prawdopodobieństwa wystąpienia oszustw w obszarach objętych przeglądem. • Audytorzy wewnętrzni są zobowiązani do posiadania wystarczającej wiedzy w zakresie oceny ryzyka wystąpienia oszustw, a także znajomości metod zarządzania ryzykiem wystąpienia oszustw w organizacji. Jednakże, nie oczekuje się od nich posiadania wiedzy specjalistycznej wymaganej od osób, których podstawowym obowiązkiem jest wykrywanie i prowadzenie dochodzeń w sprawie zaistniałych oszustw.	• Rada jest odpowiedzialna za nadzór nad systemami i procesami służącymi prewencji i wykrywaniu oszustw. • Postawa Rady i kierownictwa wyższego szczebla stanowi wzór dla innych w zakresie prewencji i wykrywania oszustw. • Rada powinna okresowo otrzymywać raporty o poziomie ryzyka wystąpienia oszustw wraz z wymiarem finansowym.

Zasada 9. Organizacja identyfikuje i dokonuje oceny zmian mogących w istotny sposób wpływać na system kontroli wewnętrznej.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
Ponieważ zmiany mogą być konsekwencją zdarzeń zarówno wewnętrznych jak i zewnętrznych, osoby ze wszystkich trzech linii obrony powinny być uwrażliwione na zdarzenia mogące istotnie wpłynąć na system kontroli wewnętrznej.			
• Jest bezpośrednio odpowiedzialna za system kontroli wewnętrznej oraz za identyfikację i ocenę zmian mogących w istotny sposób na niego wpłynąć. • Przekazuje Radzie informacje o zmianach, mogących w istotny sposób wpłynąć na system kontroli wewnętrznej. Szczegółowość tych informacji powinna być ustanowiona na poziomie, który umożliwi Radzie wypełnianie funkcji nadzorczych.	• Może zostać poproszona o wsparcie w procesie oceny wpływu zmian na system kontroli wewnętrznej. • Wykazuje aktywność w działaniach dostosowawczych do zmian. • Regularnie analizuje i rozważa zmiany wpływające na ryzyko prawne, regulacyjne i zgodności danej organizacji.	• Identyfikuje i ocenia zmiany mogące w istotny sposób wpłynąć na system kontroli wewnętrznej podczas okresowych ocen ryzyka i wykonywania zadań audytowych. • Regularnie komunikuje się z kierownictwem, aby przewidywać zmiany i ich wpływ na ocenę ryzyka organizacji.	• Rada odpowiada za zapewnienie, że kierownictwo stworzyło procesy umożliwiające identyfikację i ocenę zmian mogących w istotny sposób wpłynąć na system kontroli wewnętrznej.

Zasada 10. Organizacja wyznacza i rozwija działania kontrolne, które przyczyniają się do ograniczania ryzyk do akceptowalnego poziomu pozwalającego zrealizować cele.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
• Utrzymuje efektywne kontrole wewnętrzne i wykonuje bieżące procedury kontroli i zarządzania ryzykiem. Kierownictwo operacyjne identyfikuje, ocenia, kontroluje, a także zapobiega występowaniu ryzyk, objaśniając potrzeby rozwoju i wdrażania polityk oraz procedur wewnętrznych. Upewnia się, że działania są spójne z wyznaczonymi celami. Poprzez przekazanie odpowiedzialności w głąb struktury, kierownictwo średniego poziomu tworzy i wdraża szczegółowe procedury, które służą jako kontrole, a także sprawuje nadzór nas swoimi pracownikami, którzy te procedury wykonują. • W sposób naturalny stanowi pierwszą linię obrony, ponieważ kontrole są włączone w systemy, a procesy włączone do zakresu działania kierownictwa operacyjnego. W celu zapewnienia zgodności i wychwycenia błędów w kontroli, błędnych procesów i niespodziewanych zdarzeń, powinny istnieć właściwe kontrole nadzorcze.	• Funkcje z drugiej linii obrony są zwykle odpowiedzialne za śledzenie określonych kontroli w imieniu kierownictwa. • Osoby z drugiej linii obrony, wyznaczone przez kierownictwo, mogą także uczestniczyć w dokonywaniu wyboru i rozwoju określonych kontroli, niemniej jednak to kierownictwo zachowuje odpowiedzialność w zakresie systemu kontroli wewnętrznej.	• Dostarcza zapewnienia, że zaimplementowane kontrole są prawidłowo zaprojektowane, efektywnie wdrożone i działają zgodnie z założeniami skutecznie minimalizując ryzyko nieosiągnięcia celów. • Proponuje usprawnienia w zakresie efektywności i skuteczności kontroli wewnętrznych. Jednakże kierownictwo zachowuje odpowiedzialność w zakresie funkcjonowania systemu kontroli wewnętrznej.	• Rada dokonuje oceny informacji i wykonuje działania nadzorcze pomagając upewnić się, że system kontroli wewnętrznej stworzony przez kierownictwo jest skuteczny w redukcji ryzyk do poziomu zapewniającego osiągnięcie celów.

Zasada 11. W celu wsparcia realizacji celów, organizacja wyznacza i opracowuje ogólne działania kontrolne z wykorzystaniem technologii.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
• Projektuje i wdraża działania kontrolne w odniesieniu do technologii. Oznacza to tworzenie i zakomunikowanie polityk i procedur odnoszących się do technologii i zapewnienie, że kontrole informatyczne odpowiednio wspierają osiąganie celów. • Tworzy procesy analizy monitorowania i oceny pojawiających się obszarów ryzyka związanego z nowymi technologiami.	• Osoby z drugiej linii obrony są często zobowiązane do analizy określonych kontroli odnoszących się do technologii. • Zgodnie z delegacją kierownictwa, funkcje takie jak departament bezpieczeństwa informacji również odgrywają istotną rolę w doborze, rozwoju i utrzymywaniu kontroli nad technologią.	• Ocenia czy procesy ładu organizacyjnego IT wspierają strategie i cele organizacji. • Dostarcza zapewnienia w zakresie efektywności, skuteczności i kompletności kontroli technologii. W razie potrzeby może rekomendować usprawnienia określonych czynności kontrolnych. Dla zachowania niezależności i obiektywności audytu wewnętrznego, audytorzy wewnętrzni zwykle nie wskazują i nie projektują ogólnych czynności kontrolnych odnoszących się do technologii, jednak mogą wydawać rekomendacje w zakresie tych kontroli. • W celu realizacji wyznaczonego zadania, audytorzy wewnętrzni muszą posiadać dostateczną wiedzę w zakresie kluczowych ryzyk i kontroli informatycznych. Jednakże, nie wszyscy audytorzy wewnętrzni muszą posiadać taką wiedzę ekspercką, jak audytorzy zajmujący się głównie audytem informatycznym i technologiami informatycznymi.	• Rada ma szczególny obowiązek nadzorczy w zakresie kierowania, oceny i monitorowania kontroli. Nadzór ten powinien również uwzględniać aspekty ładu organizacyjnego w zakresie informatyki, np.: - Organizacja i struktura ładu organizacyjnego. - Kierownictwo wykonanwcze i wsparcie. - Planowanie strategiczne i organizacyjne. - Dostarczanie usług i pomiar. - Organizacja i zarządzanie informatyką.

Zasada 12. Organizacja wdraża działania kontrolne w ramach polityk, które opisują stan oczekiwany i procedury, które realizują polityki

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
• Ustala działania kontrolne wbudowane w procesy i codzienne zadania pracowników. W politykach wskazuje oczekiwania, a w odpowiednich procedurach definiuje poszczególne działania. • Ustala odpowiedzialność za czynności kontrolne z kierownictwem (lub innym wyznaczonym personelem) jednostki lub funkcji, której dotyczą określone ryzyka. • Zapewnia, że kompetentny personel, z odpowiednim umocowaniem w organizacji przeprowadza kontrole z należytą starannością i uwagą, w odpowiednich terminach, zgodnie z politykami i procedurami. Zapewnia, że personel, któremu powierzono odpowiedzialność, podejmuje działania w związku z nieprawidłowościami stwierdzonymi w procesie kontroli. • Okresowo dokonuje przeglądu czynności kontrolnych, aby ocenić ich skuteczność i aktualizuje je jeśli zachodzi konieczność.	• Zgodnie z wytycznymi kierownictwa monitoruje zgodność z określonymi politykami i procedurami. • Wspiera kierownictwo w rozwijaniu i komunikowaniu polityk i procedur. • Zapewnia, że ryzyka są nadzorowane z uwzględnieniem poziomu apetytu na ryzyko zdefiniowanym w organizacji.	• Dostarcza zapewnienia odnośnie kształtu i wdrożenia polityk, procedur i innych kontroli. • Wydaje rekomendacje w zakresie polityk i procedur, jednakże nie odpowiada za kształt i wdrażanie polityk i procedur w innych obszarach niż funkcja audytu wewnętrznego.	• Rada odpowiada za nadzór, który ma zapewnić, że stabilny system polityk i procedur funkcjonuje kształtując działalność operacyjną i wspiera osiąganie celów.

Zasada 13. Organizacja pozyskuje lub sama tworzy i wykorzystuje odpowiednie informacje, w celu wsparcia funkcjonowania kontroli wewnętrznej.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	Druga Lina Obrony (Ryzyko, kontrola i zgodność (Compliance))	Trzecia Lina Obrony (Audyt wewnętrzny)	Inne
• Zbiera i gromadzi dane w celu analizy codziennych aktywności, a następnie przekazuje informacje wyższym i niższym szczeblom organizacji. • Bierze pod uwagę koszty i zyski upewniając się, że natura, ilość i jakość przekazywanych informacji są racjonalne i wspierają osiągnięcie celów. • Kierownictwo odpowiada za wiarygodność i spójność informacji. Ta odpowiedzialność dotyczy całej krytycznej informacji w organizacji, niezależnie od tego, jak informacja jest przechowywana. Wiarygodność i spójność informacji obejmuje dokładność, kompletność i bezpieczeństwo.	• Zbiera informacje z wewnątrz organizacji w celu monitorowania działań.	• Dostarcza zapewnienia w zakresie wiarygodności i spójności informacji, a także powiązanych z tym ryzyk. Obejmuje zarówno ryzyka wewnętrzne jak i zewnętrzne, a także ekspozycję ryzyk w stosunku do relacji organizacji z podmiotami zewnętrznymi. • Okresowo ocenia praktyki organizacji w zakresie zapewniania rzetelności i spójności informacji oraz w razie potrzeby rekomenduje usprawnienia lub wdrożenie nowych kontroli bądź zabezpieczeń. Takie oceny mogą być przeprowadzane jako oddzielne zadania audytowe lub mogą być włączone do innych zadań wynikających z planu audytów. • Ocenia, czy naruszenia wiarygodności i spójności informacji, mogące stanowić zagrożenie dla organizacji, będą bez zbędnej zwłoki komunikowane kierownictwu wyższego szczebla, Radzie i audytowi wewnętrznemu.	• Kierownictwo wyższego szczebla i Rada waliduje informacje w celu dokonania oceny czy organizacja odnosi sukcesy, przewiduje ryzyka i komunikuje się z zewnętrznymi interesariuszami i inwestorami. • Okresowo otrzymuje raporty dotyczące funkcjonowania i efektywności systemu kontroli wewnętrznej organizacji.

Zasada 14. Celem wsparcia funkcji kontroli wewnętrznej, organizacja przekazuje pracownikom informacje o celach, zakresie i odpowiedzialności kontroli wewnętrznej.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	Druga Lina Obrony (Ryzyko, kontrola i zgodność (Compliance))	Trzecia Lina Obrony (Audyt wewnętrzny)	Inne
• Rozwija i utrzymuje procesy służące przekazywaniu wymaganych informacji, ułatwiając całemu personelowi zrozumienie i należyte wykonywanie ich obowiązków w ramach kontroli wewnętrznej. • Dostarcza Radzie właściwych (odpowiednich) informacji, które umożliwiają Radzie wypełnienie jej roli w osiągnięciu celów organizacji. • Tworzy oddzielne kanały komunikacji takie jak gorące linie[12], które służą jako awaryjne mechanizmy wspierające anonimową lub poufną komunikację, w sytuacjach gdy zwykłe kanały komunikacji są niesprawne lub nieskuteczne.	• W zakresie określonych kontroli monitoruje i opracowuje informacje, komunikuje podsumowanie informacji pierwszej i trzeciej linii obrony oraz Radzie. • Może być odpowiedzialna za śledzenie niektórych kanałów komunikacji, jak na przykład gorącej linii.	• Dostarcza zapewnienia w zakresie kompletności, dokładności i jakości komunikacji, zgodnie z potrzebami Rady i kierownictwa wyższego szczebla.	• Rada ustala i komunikuje sposób zachowań oczekiwanych w organizacji. • Rada i kierownictwo wyższego szczebla powinno dostarczyć wytycznych w zakresie natury komunikacji oczekiwanej od osób z każdej z linii obrony.

[12] gorące linie (ang. whistleblower hotlines)

Zasada 15. Organizacja komunikuje się z podmiotami zewnętrznymi w kwestiach dotyczących funkcjonowania kontroli wewnętrznej.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
• Zapewnia istnienie procesów pozwalających na terminowe komunikowanie istotnych informacji podmiotom zewnętrznym, uwzględniając akcjonariuszy, partnerów, właścicieli, regulatorów, klientów, a także analityków finansowych oraz inne podmioty zewnętrzne. • Tworzy i zapewnia funkcjonowanie otwartych kanałów komunikacji celem zbierania informacji od klientów, konsumentów, dostawców, audytorów zewnętrznych, regulatorów, analityków finansowych i innych oraz przekazywania właściwych (odpowiednich) informacji kierownictwu i Radzie. • Przekazuje Radzie odpowiednie informacje z przeglądów przeprowadzanych przez podmioty zewnętrzne. • Wybiera odpowiednie metody komunikacji i zapewnia, że uwzględniają one terminowość, właściwych odbiorców i naturę komunikacji, a także prawne, regulacyjne oraz powiernicze wymagania i oczekiwania. • Tworzy odpowiednie polityki uwzględniając takie aspekty jak: uprawnienia do raportowania informacji poza organizację, wytyczne w zakresie informacji dopuszczalnych i niedozwolonych w raportowaniu, osoby spoza organizacji upoważnione do otrzymywania informacji oraz zakresy informacji, które mogą one otrzymać, powiązane regulacje w zakresie prywatności, wymagań regulatorów, prawnych aspektów raportowania informacji poza organizację oraz rodzaj działań zapewniających, doradztwa, rekomendacji, opinii, wytycznych i innych informacji mogących wchodzić w skład komunikacji poza organizację.	• Za wyjątkiem pewnej komunikacji z regulatorami, audytorami zewnętrznymi i innymi określonymi grupami, zwykle druga linia obrony, nie komunikuje się z podmiotami zewnętrznymi w kwestiach dotyczących funkcjonowania kontroli wewnętrznej. • Jeśli organizacja raportuje na zewnątrz w zakresie funkcjonowania jej kontroli wewnętrznych funkcje z drugiej linii obrony dostarczają kierownictwu informacji o rezultatach podejmowanych przez nie działań, wspierając w ten sposób opinie kierownictwa.	• Dostarcza zapewnień, że kluczowa komunikacja w organizacji jest odpowiednia. • Zwykle funkcja audytu nie komunikuje się z podmiotami zewnętrznymi w zakresie dotyczącym funkcji kontroli wewnętrznej.	• Rada powinna otrzymywać informacje i raporty od kierownictwa w zakresie funkcjonowania i efektywności kontroli wewnętrznych, ponieważ są one podstawą kształtowania się opinii Rady przed jego przekazaniem podmiotom zewnętrznym. • Rada powinna omawiać z audytorami zewnętrznymi ich poglądy i opinie na temat stanu kontroli wewnętrznej, które mogą być przedstawione w raportach udostępnianych na zewnątrz organizacji.

Zasada 16. Organizacja dobiera, rozwija i przeprowadza ciągłą i selektywną ocenę komponentów system kontroli wewnętrznej pod kątem ich istnienia i funkcjonowania.

Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
• Wybiera i rozwija zrównoważone ciągłe i odrębne analizy zmian w działalności i procesach organizacji, dostosowując zakres i częstotliwość wybranych ocen do poziomu ryzyka. (Te oceny mogą być wykonywane przez drugą linię obrony). • Zapewnia, że przeprowadzający analizy w trybie ciągłym i odrębne analizy mają dostateczną wiedzę i rozumieją naturę ocenianych procesów. • Struktura i aktualny stan systemu kontroli wewnętrznej może być wykorzystywany jako punkt wyjścia dla ciągłych i odrębnych ocen. • Okresowo raportuje do Rady działania związane z zarządzaniem ryzykiem.	• Zgodnie z wytycznymi kierownictwa przeprowadza ciągłe i odrębne oceny w celu monitorowania statusu różnych komponentów systemu kontroli wewnętrznej. • Przeprowadza ciągłe i odrębne oceny w celu śledzenia czy osiąganie celów mieści się w ustalonych poziomach akceptacji ryzyka.	• Dostarcza zapewnienia, że ciągła ocena wykonywana przez kierownictwo jest włączona w procesy organizacji i jeśli zachodzi potrzeba dostosowuje się do zmieniających się warunków. • Dostarcza zapewnienia, że informacja dostarczona w rezultacie przeprowadzanych przez kierownictwo analiz jest prawdziwa i właściwie przedstawiania. • Dostarcza zapewnienia, że system kontroli wewnętrznej działa zgodnie z założeniami, a ryzyka są zarządzane w granicach apetytu na ryzyko i granicach tolerancji.	• Rada nadzoruje i utrzymuje kierownictwo odpowiedzialne za dobór, rozwój i przeprowadzanie ocen komponentów kontroli wewnętrznej. • Okresowo otrzymuje raporty o ryzykach organizacji i skuteczności zarządzania ryzykiem.

Zasada 17. Organizacja ocenia i terminowo komunikuje nieprawidłowości kontroli wewnętrznej do jednostek odpowiedzialnych za podejmowanie działań naprawczych, informując odpowiednio kierownictwo wyższego szczebla i/lub Radę.			
Pierwsza Lina Obrony (Właściciele ryzyk/zarządzający ryzykiem)	**Druga Lina Obrony** (Ryzyko, kontrola i zgodność (Compliance))	**Trzecia Lina Obrony** (Audyt wewnętrzny)	**Inne**
• Przekazuje informacje o nieprawidłowościach jednostkom odpowiedzialnym za podejmowanie działań naprawczych oraz odpowiednio kierownictwu wyższego szczebla i/lub Radzie. • Monitoruje czy nieprawidłowości są terminowo usuwane.	• Osoby z drugiej linii obrony mogą zostać zobowiązane do monitorowania i raportowania określonych typów zidentyfikowanych nieprawidłowości w kontroli.	• Audytorzy wewnętrzni tworzą i utrzymują system monitorowania obserwacji i zaleceń audytowych przekazanych kierownictwu. System ten zwykle zawiera: - Ramy czasowe, w których kierownictwo jest zobowiązane do wypowiedzenia się odnośnie obserwacji poczynionych podczas badania audytowego i wydanych zaleceń. - Ocenę odpowiedzi udzielonej przez kierownictwo. - Weryfikację odpowiedzi kierownictwa (jeśli zachodzi taka potrzeba). - Zweryfikowanie działań wdrożonych przez kierownictwo (jeśli zachodzi taka potrzeba). - Proces eskalacji do kierownictwa wyższego szczebla lub Rady w przypadku uzyskania niesatysfakcjonujących odpowiedzi/podjęcia niewystarczających działań przez kierownictwo wraz ze wskazaniem potencjalnych ryzyk z nich wynikających.	• Rada powinna upewnić się, że otrzymuje bez zbędnej zwłoki informacje o stwierdzonych nieprawidłowościach w funkcjonujących kontrolach oraz działania naprawcze są podejmowane terminowo i odnoszą się do zidentyfikowanych nieprawidłowości. • Kierownictwo i/lub Rada ocenia wyniki ciągłych i odrębnych ocen.

O autorach

Douglas J. Anderson, CIA, CPA, CRMA, CMA, jest Dyrektorem Departamentu Audytu, Konsultantem Centrum Wykonawczego IIA, Dyrektorem Wykonawczym w Saginaw Valley State University oraz konsultantem w zakresie ładu oranizacyjnego, ryzyka i kontroli. Ma ponad 30-letnie doświadczenie w audycie wewnętrznym, audycie zewnętrznym, księgowości i finansach.
Jego obowiązki służbowe poprowadziły go przez świat i zaowocowały doświadczeniem z wielu różnych organizacji.

Douglas J Anderson pełnił w Instytucie Audytorów Wewnętrznych szereg ról na zasadzie wolontariatu, w tym trenera, członka/przewodniczącego Komitetu Profesjonalnego Doradztwa i wiceprzewodniczącego Profesjonalnego Doradztwa Komitetu Rady Dyrektorów Wykonawczych.

Pracował także dla Grupy Doradczej Rady Nadzoru nad Rachunkowością Spółek Publicznych oraz był członkiem grup nadzorujących dwa projekty COSO.

Gina Eubanks, CIA, CISA, CRMA, CCSA, jest wiceprezesem Profesjonalnych Usług w IIA, gdzie przewodzi obszarowi jakości pełniąc funkcję Dyrektora Departamentu Audytu i Programom Usług Branżowych. Ma ponad 20-letnie doświadczenie w audycie wewnętrznym, w tym 15 lat w Wielkiej Czwórce i usługach zarządzania ryzykiem dla podmiotów o globalnym zasięgu. Gina Eubanks zdobyła doświadczenie zarówno w Stanach Zjednoczonych jak i za granicą, wiele czasu spędzając w Indiach. Była praktykiem i dyrektorem w sektorach handlu detalicznego i usług finansowych. Pełni również funkcję członka komitetu audytu lokalnej instytucji finansowej, a w ramach wolontariatu była liderem w IIA przez prawie 15 lat.

O COSO

Założone w 1985 roku, COSO to wspólna inicjatywa pięciu organizacji sektora prywatnego, której głównym celem jest zapewnienie przywództwa, poprzez rozwój ramowych zasad i wytycznych dotyczących zarządzania ryzykiem przedsiębiorstwa, kontroli wewnętrznej i zapobiegania oszustwom.

Organizacjami wspierającymi COSO są: Instytut Audytorów Wewnętrznych (IIA), Amerykańskie Stowarzyszenie Księgowości (AAA), Amerykańskiego Instytutu Biegłych Rewidentów (AICPA), Międzynarodowe Zrzeszenie Dyrektorów Finansowych (FEI), oraz Instytut Rachunkowości Zarządczej (IMA).

O Instytucie IIA

Instytut Audytorów Wewnętrznych (IIA) powstał w 1941 roku. Jest to międzynarodowe stowarzyszenie zawodowe, którego światowa siedziba znajduje się w USA, w mieście Altamonte Springs na Florydzie. Instytut jest globalnym przedstawicielem profesji audytuwewnętrznego oraz uznawanym autorytetem, liderem, głównym orędownikiem oraz edukatorem w tej dziedzinie.Więcej informacji o organizacji na stronie internetowej www.theiia.org.

Centrum Dyrektorów Departamentu Audytu Instytutu Audytorów Wewnętrznych (The Institute of Internal Auditors' Audit Executive Center®) jest podstawowym zasobem wzmacniającym dyrektorów departamentów audytu w podnoszeniu skuteczności podejmowanych przez nich działań. Zasoby Centrum w zakresie informacji, produktów i usług umożliwiają dyrektorom departamentów audytu odpowiedzenie na szczególne wyzwania i ryzyka zawodowe. Więcej informacji na temat Centrum znajduje się na stronie internetowej www.theiia.org/cae.

O Instytucie IIA Polska

Instytut Audytorów Wewnętrznych IIA Polska

IIA jest reprezentowany w Polsce przez Instytut Audytorów Wewnętrznych IIA Polska. IIA Polska jest stowarzyszeniem osób fizycznych, zarejestrowanym w Krajowym Rejestrze Sądowym 9 maja 2002 r. oraz uznanym przez światową organizację IIA w dniu 27 czerwca 2003 roku. Do Instytutu Audytorów Wewnętrznych IIA Polska należy aktualnie ponad 1500 osób z całego kraju. Instytut nie prowadzi działalności gospodarczej i opiera się na aktywności społecznej członków i wolontariuszy realizujących cele Instytutu.

Nadzór na projektem tłumaczenia:
Sebastian Burgemejster, CISA, CGAP, CCSA, CRMA

Kontrola jakości tłumaczenia:
Małgorzata Lorenz, ACCA, CIA, CISA, biegły rewident
Maria Kucharska – Fiałkowska
Sebastian Burgemejster, CISA, CGAP, CCSA, CRMA

Tłumaczenie:
Karol Majewski
Marta Wojciechowska, CIA, CCSA

Skład DTP:
Marcin Boguś

COSO

Komitet Organizacji Sponsorujących
Komisję Treadwaya

www.coso.org

WYKORZYSTANIE COSO W TRZECH LINIACH OBRONY

COSO

Komitet Organizacji Sponsorujących Komisję Treadwaya

www.coso.org