ECIIA

STANOWISKO

PODEJŚCIE DO PLANOWANIA AUDYTU

USPRAWNIANIE ŁADU POPRZEZ AUDYT WEWNĘTRZNY

Instytut Audytorów Wewnętrznych IIA Polska

2

O ECIIA

Europejska Konfederacja Instytutów Audytorów Wewnętrznych (ECIIA) jest profesjonalnym przedstawicielstwem 36 narodowych instytutów audytu wewnętrznego na obszarze Europy i basenu Morza Śródziemnego.
Misją ECIIA jest zgodny głos dla profesji audytu wewnętrznego w Europie poprzez współpracę z Unią Europejską, Parlamentem oraz Komisją Europejską, jak również każdą instytucją wpływu. ECIIA reprezentuje i rozwija profesję Audytu Wewnętrznego i dobrego Ładu Organizacyjnego w Europie.

Podstawowym celem jest wspieranie rozwoju ładu organizacyjnego i audytu wewnętrznego poprzez dzielenie się wiedzą oraz stałe monitorowanie środowisk regulowanych.

SPIS TREŚCI

3

WSTĘP

ECIIA utworzyła w 2015 roku Komisję Bankowości z udziałem Zarządzających audytem Banków nadzorowanych przez Europejski Bank Centralny[1]. Na stronie internetowej Europejskiego Banku Centralnego znajduje się pełna lista nadzorowanych podmiotów.

Misją Komisji Bankowości ECIIA jest:
„Pełnić funkcję skonsolidowanego głosu zawodu audytu wewnętrznego w Sektorze Bankowym w Europie, na drodze współpracy z europejskimi organami tworzącymi przepisy i wszelkimi innymi wpływowymi instytucjami, a także reprezentować i rozwijać zawód audytu wewnętrznego oraz ład organizacyjny w sektorze bankowym w Europie"

Dokument opisuje najlepsze stosowane praktyki, ale należy pamiętać, że w zależności od kultury, wielkości, wymagań biznesowych i lokalnych możliwe są inne rozwiązania.

Myśl przewodnia

Skuteczne zarządzanie ryzykiem jest istotną częścią dobrego ładu organizacyjnego.
Ważną rolę w każdej organizacji odgrywa identyfikacja wszystkich ryzyk biznesowych i niepewności, przed którymi stoi organizacja, szybkie wdrażanie środków ograniczających ryzyko i usprawnianie systemu kontroli wewnętrznej.
Funkcja audytu wewnętrznego, jako istotny element ram ładu organizacyjnego, dostarcza niezależnego zapewnienia o właściwym zarządzaniu tymi ryzykami. Ponieważ globalne środowisko biznesowe oraz wymogi finansowe i regulacyjne stały się bardziej złożone, użytkownicy audytowanych procesów domagali się bardziej trafnych informacji na potrzeby podejmowania decyzji.
Szybko zmieniające się środowisko (np. digitalizacja usług, zrównoważony rozwój, technologia informacyjna) oraz skrócenie cyklu życia produktów wymaga od organizacji nadążania za zmianami.
Zwinność i krótki czas reakcji są kluczowe dla przetrwania. Prowadzi to do nowych/zwiększonych ryzyk, z którymi organizacja musi sobie poradzić, jak również do nowego określenia apetytu na ryzyko. Aby w krótkim czasie dostarczyć zapewnienia kierownictwu wyższego szczebla, konieczne jest skoncentrowanie planu audytu zarazem na bieżących i przyszłych ryzykach oraz podejścia opartego na analizie ryzyka przy planowaniu audytu.

Kontekst

Wymagania dotyczące planowania w ramach funkcji audytu wewnętrznego opisano w - Standardzie IIA nr 2010 „Planowanie".
Zarządzający audytem wewnętrznym musi opracować plan oparty na analizie ryzyka, określający priorytety działań audytu wewnętrznego zgodne z celami organizacji.

Podejście oparte na analizie ryzyka koncentruje się na ustaleniu krótkookresowego planu audytu, jako że informacje dotyczące ryzyk stają się dostępne na bieżąco i powodują zmiany w zakresie potrzeb realizacji zadań audytowych w poszczególnych obszarach.
Informacje związane z ryzykiem obejmują między innymi zmiany w danej organizacji dotyczące działalności biznesowej, operacji, programów, systemów, ryzyk i istniejących kontroli, a także zmiany strategii, kluczowych celów biznesowych i powiązanych ryzyk, które są dostrzegane przez kierownictwo wyższego szczebla w kontekście czynników makroekonomicznymi (np. obszar niskiego zainteresowania).
W dzisiejszym szybko zmieniającym się środowisku organizacje muszą szybko reagować na ciągłe zmiany wymagań klientów, czynników środowiskowych, reguł rynkowych, wewnętrznych procesów biznesowych i wymogów regulacyjnych.
Organizacje muszą zarządzać ryzykiem wynikającym z różnic pomiędzy lokalnymi przepisami, które także ulegają zmianom wraz z transformacją zewnętrznych uregulowań (np. ostatnie zmiany w technologii finansowej, takie jak blockchain[2] i bitcoin[3]).
Podejście oparte na analizie ryzyka pozwala na ciągłe doskonalenie planu audytu, aby nadążać za zmianami ryzyk, z którymi organizacje muszą się zmierzyć. Dlatego też podejście oparte na ciągłym zarządzaniu ryzykiem powinno być traktowane priorytetowo w stosunku do tradycyjnego podejścia opartego na wieloletnim planowaniu, ponieważ tradycyjne podejście nie zapewnia skutecznego i bieżącego zarządzania ryzykiem.
Funkcja audytu wewnętrznego nie może dostarczyć w wymaganym czasie zapewnienia, że nowe/zwiększone/zmienione ryzyka są zarządzane we właściwy sposób, stosując wyłącznie podejście oparte na wieloletnim (długoterminowym) planowaniu audytu.
Ponadto tradycyjne podejście nie zapewnia podjęcia przez audyt wewnętrzny działań związanych z zarzadzaniem ryzykiem oraz wprowadzenia zmian w systemie kontroli wewnętrznej na odpowiednio wczesnym etapie.

---

[1] Zarządzający audytem z DZ Bank AG, Crédit Agricole SA, ABN AMRO, Grupo Santander, UniCredit S.p.A., KBL European Private Bankers, Nordea, National Bank of Greece

[2] blockchain (łańcuch bloków) – zdecentralizowana i rozproszona baza danych w modelu open source w sieci internetowej o architekturze peer-to-peer (P2P) bez centralnych komputerów i niemająca scentralizowanego miejsca przechowywania danych, służąca do zapisywania poszczególnych transakcji, płatności lub zapisów finansowych zakodowana za pomocą algorytmów kryptograficznych. (przyp. redakcji)

[3] bitcoin – kryptowaluta wprowadzona w 2009 roku (przyp. redakcji)

4

Wytyczne Komisji Bazylejskiej ds. Nadzoru Bankowego (BCBS)[4] poradnik „Funkcja audytu wewnętrznego w bankach" (BCBS 223)[5] obejmuje planowanie audytu zgodnie z zasadami 6[6] i 7[7].
Wymogi regulacyjne lokalnych organów regulacyjnych zazwyczaj zawierają postanowienia dotyczące okresu, w którym należy objąć działaniami audytu wszystkie obszary organizacji lub odnoszą się do planu wieloletniego (np. Niemiecki MaRisk BT 2.3[8] lub US SR 13-1 p10[9]).
Plan wieloletni jest przydatny do wizualizacji zasięgu całokształtu audytu w pożądanym okresie. Podejście to jest łatwe w zarządzaniu, a postępy można monitorować na podstawie rocznego planu. Jednak aspekty, które mogą ulec zmianie w przewidywanym okresie, nie mogą być w wystarczającym stopniu przewidziane.
Większość planów wieloletnich opiera się na prognozowaniu zapotrzebowania na kolejne zlecenie audytowe, wykorzystując jako punkt wyjścia datę ostatniego zlecenia i dodając cykl audytów z góry określoną liczbą lat, w zależności od szacowania ryzyka przez audyt wewnętrzny lub od danych wymogów regulacyjnych.
Takie statyczne podejście do planowania audytu może skutkować brakiem uwzględnienia znaczących zmian w uwarunkowaniach biznesowych, w których działa organizacja i w konsekwencji audyt wewnętrzny może nie być w stanie dostarczyć w odpowiednim czasie obiektywnego zapewnienia i doradztwa nakierowanych na dodanie wartości i usprawnienie działania organizacji.[10]
Podejście oparte na analizie ryzyka, jako metodzie dynamicznej, ułatwia koncentrację na nagłych, znaczących ryzykach, na które narażona jest organizacja i umożliwia działalności audytu wewnętrznego reagowanie w odpowiednim czasie na zmiany strategii biznesowej, struktury, procesów i ryzyk.
To podejście opiera się na analizie ryzyka i daje rezultat w postaci ogólnej oceny organizacji jako całości, a nie oceny poszczególnych procesów skutkującej myśleniem fragmentarycznym. Umożliwia terminowe wdrażanie wyników zewnętrznych audytów w zakresie nadzoru/regulacji.
Co więcej, istnieje potrzeba, aby kierownictwo wyższego szczebla angażowało funkcję audytu wewnętrznego na wczesnym etapie procesu zatwierdzania/zmiany nowego produktu. Podejście oparte na analizie ryzyka prowadzi do zmian w kulturze organizacyjnej koncentrując główną uwagę na zagadnieniach występowania ryzyk. Zadania audytowe zazębiają się z celami biznesowymi i prowadzeniem ciągłych analiz danych przy monitorowaniu ryzyk.
Wiarygodność i rzetelność statycznego, wieloletniego planu audytu w perspektywie średniookresowej (lub dłuższej) jest wątpliwa, biorąc pod uwagę stale zmieniające się otoczenie, w tym zmiany przepisów, których nie da się przewidzieć.

---

4 BCBS – The Basel Committee on Banking Supervision (przyp. redakcji)

5 BCBS 223 – "The internal audit function in banks" (przyp. redakcji)

6 Zasada 6: Każde działanie (w tym działania zlecone na zewnątrz) i każdy podmiot banku powinien być objęty ogólnym zakresem funkcji audytu wewnętrznego. [...] 31. Szef audytu wewnętrznego jest odpowiedzialny za ustalenie rocznego planu audytu wewnętrznego, który może stanowić część planu wieloletniego. Plan powinien opierać się na solidnej ocenie ryzyka (w tym danych wejściowych od kierownictwa wyższego szczebla i rady) i powinien być aktualizowany co najmniej raz w roku (lub częściej, aby umożliwić bieżącą ocenę, gdzie występują istotne ryzyka). Zatwierdzenie planu audytu przez radę oznacza, że będzie dostępny odpowiedni budżet na wsparcie działań audytu wewnętrznego. Budżet powinien być wystarczająco elastyczny, aby dostosowywać się do zmian w planie audytu wewnętrznego w odpowiedzi na zmiany w profilu ryzyk dla działalności banku.

7 Zasada 7: Zakres działalności audytu wewnętrznego powinien zapewniać odpowiednie ujęcie w ramach planu audytu spraw wymagających uregulowań formalnych.

8 Niemiecki MaRisk BT 2.3: Działania i procesy instytucji, w tym zlecane na zewnątrz, są audytowane w odpowiednich odstępach czasu, co do zasady w ciągu trzech lat. Audyt roczny przeprowadza się w miejscach występowania poszczególnych ryzyk. Trzyletni cykl audytu może zostać uchylony w przypadku działań i procesów, które są nieistotne z punktu widzenia występowania ryzyk.

9 US SR 13 - p10: Audyt wewnętrzny powinien opracowywać i okresowo korygować swój kompleksowy plan audytów oraz zapewniać objęcie audytem wszystkich zidentyfikowanych, możliwych do zaudytowania elementów, w ramach całokształtu audytu, w sposób odpowiedni dla wielkości i złożoności działań instytucji.
Powinno to zostać osiągnięte poprzez podejście oparte na tworzeniu wieloletniego planu, który jest aktualizowany co roku lub poprzez podejście oparte na planie obejmującym ocenę ryzyk w skali roku, z koncentracją na najbardziej znaczących ryzykach. W tym drugim podejściu powinien istnieć mechanizm pozwalający zidentyfikować sytuację, kiedy znaczące ryzyko nie zostanie poddane audytowi w określonych ramach czasowych, a także powinien istnieć wymóg powiadomienia o tym Komitetu Audytu i uzyskania jego zatwierdzenia dla wszelkich wyjątków od ramowych zasad. Ogólnie rzecz biorąc, powszechną praktyką dla instytucji, które mają określone cykle audytu, jest przeprowadzanie trzy- lub czteroletniego cyklu audytu; obszary wysokiego ryzyka powinny być poddawane audytowi przynajmniej co dwanaście do osiemnastu miesięcy.

10 Zgodnie z definicją IPPF audyt wewnętrzny jest działalnością 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. IPPF 2050 „W celu zapewnienia odpowiedniego zakresu audytu i minimalizacji powielania wysiłków, zarządzający audytem wewnętrznym powinien wymieniać informacje, koordynować działania i brać pod uwagę możliwość polegania na pracy innych zarówno wewnętrznych, jak i zewnętrznych wykonawców usług zapewniających i doradczych".

5

PODSTAWY

W pierwszym kroku należy ustalić podstawy i perspektywy podejścia opartego na analizie ryzyka. W większości instytucji podejście do oceny ryzyka (w tym metoda lub system) jest już wdrożone i wówczas może być udoskonalone przez funkcję audytu wewnętrznego, z uwzględnieniem zachowania niezależności (np. istniejące podejście w ramach zarządzania ryzykiem może być podniesione do poziomu podejścia opartego na analizie ryzyka funkcji audytu wewnętrznego).
W podejściu opartym na analizie ryzyka plan audytu jest oparty na rejestrze ryzyka organizacji[11] i ułatwia udoskonalenie ram zarządzania ryzykiem.
W związku z tym funkcja audytu wewnętrznego może koncentrować się na zwiększeniu dojrzałości organizacji w zakresie podejścia do ryzyka oraz jest w stanie dostarczyć zapewnienia dotyczącego procesów zarządzania ryzykiem, w tym zarządzania i raportowania o najistotniejszych ryzykach.
Wybrane podejście do oceny ryzyka powinno być konsekwentnie odzwierciedlone w strukturze całokształtu audytu, np. proces oceny ryzyka wymagałby również struktury zorientowanej na procesy w całokształcie audytu.

Zarówno orientacja na ryzyko jak i struktura całokształtu audytu powinny również uwzględniać wzajemne powiązania z istniejącym systemem kontroli wewnętrznej. W szczególności, tworzone kluczowe mechanizmy kontrolne mogą określić strukturę oraz informacje zwrotne na temat budowy i skuteczności istniejących mechanizmów kontroli.

Określenie kryteriów stosowanych w podejściu opartym na analizie ryzyka

Podejście oparte na analizie ryzyka nie powinno być sprzeczne z wymogami dotyczącymi częstotliwości audytu narzuconymi przez miejscowe organy regulacyjne (np. corocznym audytem określonego obszaru). W związku z tym należy wprowadzić regulacje w celu poprawnego odzwierciedlenia tych wymogów (np. poprzez zastąpienie oceny ryzyka).

Kryteria stosowane w podejściu do planowania opartym na analizie ryzyka powinny być zdefiniowane i sformalizowane.
Wyniki mechanizmów kontroli pierwszego i drugiego stopnia, kluczowe wskaźniki ryzyka monitorowane przez drugą linię obrony, istotne zmiany organizacyjne uwzględnione w procesach zatwierdzania/zmiany nowych produktów, bieżące zdarzenia i czynniki makroekonomiczne, a także zmiany przepisów, powinny być w odpowiednim czasie uwzględnione w planie audytu.

Ze względu na to, że ryzyka na jakie napotyka każda organizacja, zależą od rodzaju działalności, lokalizacji, struktury organizacyjnej, produktów, klientów i usługodawców, funkcja audytu wewnętrznego wymaga elastyczności, aby móc odpowiednio wcześnie reagować na zmieniające się czynniki wewnętrzne i zewnętrzne.
Aby ustalić przejrzyste i oparte na analizie ryzyka podejście do planowania audytu wewnętrznego oraz skorzystać z jego zalet, konieczne są wiążące wytyczne dotyczące jego wdrażania i formy.
Wytyczne te należy następnie przedstawić lokalnym/macierzystym organom nadzoru, zabiegać o ich akceptację i w ten sposób inicjować zmiany lokalnych regulacji. Dzięki takim działaniom mogą być uwzględnione także ryzyka zidentyfikowane przez organy nadzorcze.

Zdefiniowanie roli funkcji audytu wewnętrznego, jako trzeciej linii obrony w przewidywaniu nowych pojawiających się ryzyk

Przebieg tworzenia planu audytu wewnętrznego ma kluczowe znaczenie dla ustalenia zadań audytowych, w taki sposób, aby w odpowiednim czasie mogły być zidentyfikowane istotne ryzyka i dzięki temu zapewniona korzyść dla organizacji.
Przy istnieniu szeregu obowiązkowych zadań audytu wynikających z przepisów, funkcja audytu wewnętrznego może dodatkowo usprawnić zarządzanie ryzykami, redukcję kosztów, lepszą ochronę klienta, stabilność dostaw i tym samym wymierną wartości dla organizacji dzięki właściwej identyfikacji potrzeb w zakresie zadań audytowych w hierarchii wartości organizacji.
Pojawiające się zagrożenia mogą być spowodowane wieloma czynnikami: zmianami ekonomicznymi lub demograficznych, zmianami przekroju konkurencji i klientów lub zmianami technologicznymi. Audyt wewnętrzny ma na celu dostarczenie zapewnienia, że organizacja jest świadoma pojawiających się zagrożeń i reaguje na nie.

Na wzrost znaczenia rzetelnego i kompleksowego podejścia do planowania audytu, opartego na analizie ryzyka, wpływa wiele czynników. Zarządzający audytem stoi przed wyzwaniem ze strony Komitetu Audytu i kierownictwa wyższego szczebla, aby dostarczyć zapewnienia, że wszystkie znaczące ryzyka są zidentyfikowane i właściwie zarządzane.

11 IPPF 2050 „W celu zapewnienia odpowiedniego zakresu audytu i minimalizacji powielania wysiłków, zarządzający audytem wewnętrznym powinien wymieniać informacje, koordynować działania i brać pod uwagę możliwość polegania na pracy innych zarówno wewnętrznych, jaki zewnętrznych wykonawców usług zapewniających i doradczych".

Ponadto istnieje zwiększone ryzyko związane z rozszerzaniem działalności na rynkach wschodzących i w krajach rozwijających się, zwiększonymi wymogami regulacyjnymi, a także powszechna koncentracja uwagi na redukcji kosztów.
Funkcja audytu wewnętrznego może usprawnić procesy organizacyjne poprzez prowadzenie audytów w oparciu o wartości i uwzględnianie w zaleceniach szerokiego spojrzenia na przyszłe ryzyka z makroekonomicznego punktu widzenia. Może zagłębić się w strategię organizacji z punktu widzenia zmian i trendów makroekonomicznych oraz dokonać ich odniesienia do istniejących ram zarządzania.

Terminowy przegląd i przedstawienie planu audytu

Ogólna struktura audytu wewnętrznego i oceny ryzyka powinny być odpowiednio komunikowane w ramach organizacji.
Roczny plan audytu należy regularnie aktualizować i odpowiednio komunikować jego korekty, uwzględniając wszelkie istotne zmiany w ogólnym profilu ryzyka, luki/incydenty lub inne pojawiające się informacje na temat ryzyk, które nie były znane w czasie tworzenia pierwotnego planu.

Wszelkie znaczące odchylenia od pierwotnego planu powinny być regularnie i w sposób klarowny zgłaszane Zarządowi i Radzie Nadzorczej/Komitetowi Audytu.

Ponadto, prowadzona na bieżąco dokumentacja dotycząca planu audytu powinna potwierdzać, iż działalność audytu, jako całości w wystarczającym stopniu odpowiada na wymagania wynikające z czynników zewnętrznych, a także wewnętrznej oceny ryzyka.

Zapewnienie bieżącej aktualizacji planu audytu można osiągnąć, wprowadzając odpowiednie reguły w regulacjach dotyczących podejścia opartego na analizie ryzyka.

Kilka przykładów tego, jak uwzględnić ten aspekt (nie jest to wyczerpująca lista):

- można dodać czynnik ryzyka, który rośnie wraz z upływem czasu, tym samym przydzielając wyższą preferencję obiektom audytu, które przez określony czas nie zostały poddane audytowi,
- kryterium „knock-out”[12], które wymusza uwzględnienie obiektu w planie audytu po odpowiednim okresie czasu lub
- obiekty audytu są uwzględniane w procesach planowania w oparciu o czas ich ostatniego audytu (najstarsze pierwsze).

W oparciu o to podejście, wszystkie cele audytu, jako całości są uwzględniane w planowaniu. Plan audytu na następny okres (cały rok) obejmuje cele audytu łącznie z analizą ryzyka, jako elementem procesu planowania.

Należy opracować i udokumentować całościowy proces, który uwzględnia specyfikę podmiotu w odniesieniu do wyżej wymienionych aspektów, a następnie przekłada się na indywidualne podejście oparte na analizie ryzyka, specyficzne dla firmy. Powinien on również obejmować obszerną dokumentację, minimalne wymagania dotyczące regularnych przeglądów oraz uzasadnienia zmian ocen ryzyka.

12 kryterium „knock-out” – kryterium zapadalności dla danego obszaru audytowego w przyjętym interwale czasowym (przyp. redakcji)

NASZA MISJA

Misją ECIIA jest zgodny głos dla profesji audytu wewnętrznego w Europie poprzez współpracę z Unią Europejską, Parlamentem oraz Komisją Europejską, jak również każdą instytucją wpływu. ECIIA reprezentuje i rozwija profesję Audytu Wewnętrznego i dobrego Ładu Organizacyjnego w Europie.

O INSTYTUCIE IIA POLSKA

IIA jest reprezentowany w Polsce przez Instytut Audytorów Wewnętrznych IIA Polska. Instytut Audytorów Wewnętrznych 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 1600 osób z całego kraju. Instytut nie prowadzi działalności gospodarczej i opiera się na aktywności społecznej członków i wolontariuszy realizujących cele Instytutu.

Więcej na stronie: www.iia.org.pl

Tłumaczenie

Andrzej Mataczyno

Redakcja

Sebastian Burgemejster, CISA, CISM, CRISC, CGAP, CCSA, CRMA, CSXF, COSO, ACO
Rafał Urbaniak, CGAP, ACO

Skład DTP

Marcin Boguś

ECIIA

The Institute of Internal Auditors

Instytut Audytorów Wewnętrznych IIA Polska