STANOWISKO

NADZÓR AUDYTU WEWNĘTRZNEGO NAD WYKONYWANIEM USŁUG ZLECANYCH NA ZEWNĄTRZ

USPRAWNIANIE ŁADU POPRZEZ AUDYT WEWNĘTRZNY

Instytut Audytorów Wewnętrznych IIA Polska

2

O ECIIA

Europejska Konfederacja Instytutów Audytorów Wewnętrznych (ECIIA) jest profesjonalnym przedstawicielstwem 35 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

[1] Technologia finansowa (FinTech lub fintech) to nowa branża wykorzystująca technologię do usprawniania działań w zakresie finansów. Wykorzystanie smartfonów do bankowości mobilnej, internetowe usługi inwestycyjne i krypto-waluty to przykłady technologii, które mają na celu uczynienie usług finansowych bardziej dostępnymi dla ogółu społeczeństwa. Firmy z branży technologii finansowej to zarówno startupy, jak i uznane firmy finansowe i technologiczne, które mają na celu zastąpienie lub ulepszenie korzystania z usług finansowych świadczonych przez tradycyjne firmy finansowe.

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

Funkcja audytu wewnętrznego ma do odegrania ważną rolę w zapewnieniu skuteczności i bezpieczeństwa kluczowych procesów zlecanych przez banki podmiotom zewnętrznym. Zasadniczą sprawą jest, aby kluczowi interesariusze, w tym kierownictwo, radę i organy nadzoru banku, mogły polegać na pracy audytu wewnętrznego odnośnie zarządzania ryzykiem zewnętrznych dostawców usług, przy jednoczesnym wypełnianiu przez audyt wewnętrzny zadań wynikających z jego funkcji odnośnie danego obszaru.
Niniejszy dokument przedstawia stanowisko Komisji Bankowości ECIIA w sprawie najlepszych praktyk, które mogą być wdrażane w ramach funkcji audytu wewnętrznego w odniesieniu do audytowania usług zlecanych na zewnątrz.
W niniejszym dokumencie nie rozważa się:

- zlecania na zewnątrz funkcji audytu wewnętrznego
- insourcing* (od jednego podmiotu prawnego do drugiego w ramach tej samej grupy), chociaż wiele takich samych koncepcji mogłoby mieć zastosowanie, z uwzględnieniem specyfiki danego podmiotu, kraju lub wymogów nadzorczych.

Kontekst

Na organizacji ciąży nieprzerwana odpowiedzialność za zapewnienie, aby procesy zlecane przez nią na zewnątrz były skutecznie kontrolowane i aby nie dochodziło do przeoczenia ryzyk. Co więcej, sam outsourcing istotnych działań może zwiększyć ryzyko operacyjne, na które narażony jest bank.

Zlecanie działań operacyjnych podmiotom zewnętrznym przez instytucje finansowe nie jest zjawiskiem nowym. Jednak w ostatnich latach złożoność procesów zlecanych na zewnątrz stale rośnie, podobnie jak nieodłączne ryzyko związane z przesyłaniem, w szczególności, danych klienta poza organizację. W konsekwencji wzrasta znaczenie silnych struktur zarządzania doborem zewnętrznych wykonawców w ramach pierwszej linii obrony, podobnie jak potrzeba zapewnienia adekwatnego monitorowania i nadzoru z drugiej i trzeciej linii.

W niniejszym dokumencie przeanalizowano następujące podstawowe aspekty roli funkcji audytu wewnętrznego w odniesieniu do zarządzania ryzykiem zewnętrznych dostawców usług:

1. Umiejscowienie czynności zlecanych na zewnątrz w ramach „uniwersum audytu" i oceny ryzyka
2. Kluczowe obszary zainteresowania audytu wewnętrznego
   a. proces wyboru usługodawców zewnętrznych
   b. struktura zarządzania usługodawcami zewnętrznymi (dostawcami)
   c. audyty kompleksowe
3. Testowanie, a następnie opieranie się na pracy innych
   a. funkcje pierwszej lub drugiej linii zapewnienia
   b. praca komórki audytu wewnętrznego usługodawcy zewnętrznego
   c. praca zewnętrznych dostawców zapewnienia
4. Specjalne wymagania dotyczące outsourcingu do „FinTechs"

[1] Chief Audit Executives from DZ Bank AG, Crédit Agricole SA, ABN AMRO, Grupo Santander, UniCredit S.p.A., KBL European Private Bankers, Nordea, National Bank of Greece
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

4

PODSTAWY

1 Umiejscowienie czynności zlecanych na zewnątrz w ramach „uniwersum audytu" i oceny ryzyka

Międzynarodowe ramowe zasady praktyki zawodowej Instytutu Audytorów Wewnętrznych określają w ramach standardu „2010 – Planowanie" potrzebę, aby Zarządzający audytem wewnętrznym opracował wynikający z analizy ryzyka plan audytu, oparty na udokumentowanej ocenie ryzyka. Plan powinien być dostosowany do zachodzących zmian w organizacji dotyczących jej działalności, ryzyka, operacji, programów, systemów i mechanizmów kontroli.

W praktyce audyt wewnętrzny zwykle osiąga to poprzez reprezentowanie działań banku w ramach określonego „uniwersum audytu", który następnie podlega ocenie ryzyka w celu ustalenia odpowiednich priorytetów planu audytu. Działania zlecane na zewnątrz powinny w całości zintegrowane w „uniwersum audytu" i podlegać tym samym nieodłącznym procesom oceny ryzyka, co operacje przeprowadzane „wewnętrznie" bezpośrednio przez bank.

Ocena ryzyka powinna również odnosić się do tego, czy ryzyko związane z daną działalnością zwiększyło się, czy zmniejszyło w wyniku jej zlecenia na zewnątrz.

Przy ustalaniu ryzyka rezydualnego (pozostałego po uwzględnieniu działań podjętych w wyniku wprowadzonych kontroli), funkcja audytu wewnętrznego może uwzględniać wyniki testów pierwszej lub drugiej linii zapewnienia (w przypadku, gdy zostały one sprawdzone przez audyt wewnętrzny i ustalono, że działają prawidłowo) oraz wyniki pracy zewnętrznych wykonawców usług (w tym ich funkcji audytu wewnętrznego), zgodnie z postanowieniami zawartymi w punkcie 3 poniżej.

Właściwa reakcja audytu powinna być następnie określona na podstawie wyników oceny ryzyka w odniesieniu do stwierdzonego ryzyka, związanego ze wszystkimi innymi działaniami w banku (tj. zgodnie ze zwykłym cyklem planowania opartym na ryzyku).

Funkcjonujące w banku procesy zarządzania doborem zewnętrznych wykonawców powinny gwarantować prawidłowość wykonywania usług zlecanych na zewnątrz, a dodatkowo powinny mieć swoje miejsce w „uniwersum audytu" i podlegać ocenie ryzyka oraz regularnym audytom opartym o analizę ryzyka.

2 Kluczowe obszary zainteresowania audytu wewnętrznego

Obowiązkiem kierownictwa jest ustalenie odpowiednich ram zarządzania ryzykiem zewnętrznych wykonawców usług (ryzykiem dostawcy), a rolą funkcji audytu wewnętrznego jest ocena efektywności ram zarządzania ryzykiem dostawców banku. Tam, gdzie potwierdzono skuteczność w/w ram zarządzania, funkcja audytu wewnętrznego może rzadziej przeprowadzać kompleksowy audytna miejscu u zewnętrznego wykonawcy. W przypadkach braku skutecznych ram zarządzania ryzykiem dostawcy, funkcja audytu wewnętrznego powinna rozważyć potrzebę zastosowania alternatywnych rozwiązań.

a. Proces wyboru usługodawców zewnętrznych

Funkcja audytu wewnętrznego nie powinna odgrywać bezpośredniej roli w zatwierdzaniu outsourcingu określonych procesów, ponieważ mogłoby to podważać jej niezależność. Rola audytu wewnętrznego polega raczej na sprawdzeniu, czy istnieją odpowiednie ramy wyboru dostawców (w tym badania due diligence w zakresie należytej staranności dostawcy) i zapewnieniu, że zarządzanie procesem decyzyjnym obejmuje wszystkie istotne zagadnienia i odpowiednie oceny ryzyk potencjalnych działań outsourcingowych. Niezależnie od powyższego audyt wewnętrzny powinien dokonać przeglądu standardów umownych organizacji, dotyczących ustaleń odnośnie współpracy z podmiotami zewnętrznymi, aby zapewnić, że warunki uzgodnione ze wszystkimi wykonawcami istotnych usług zawierają „prawo do audytu".

b. Zarządzanie usługodawcami zewnętrznymi (dostawcami)

Audyt wewnętrzny powinien dokonać przeglądu i oceny adekwatności struktury zarządzania dostawcami banku, aby ustalić czy zapewnia ona właściwe zarządzanie i nadzór nad kluczowymi czynnościami zleconymi podmiotom zewnętrznym. W praktyce proces zarządzania dostawcami w banku może obejmować wiele różnych elementów. Audyt wewnętrzny powinien brać pod uwagę zróżnicowanie ich znaczenia i określić odpowiednie podejście audytu, stosowne do specyficznych warunków funkcjonowania instytucji.

Jako minimum, funkcja audytu wewnętrznego powinna przejrzeć wszystkie obszary procesu zarządzania dostawcami, w których może zachodzić skłonność do bazowania na własnej ocenie ryzyka, czyli „w zamian" podjęcia bezpośredniego „badania kompleksowego" u dostawcy. Przykładowo mogą obejmować (a) proces oceny ryzyka dostawcy (który zazwyczaj określa znaczenie dostawcy, a w konsekwencji poziom nadzoru za pośrednictwem procesu zarządzania dostawcami) oraz (b) działanie pierwszej lub drugiej linii funkcji zapewnienia dostawcy.

W przypadku (a) funkcja audytu wewnętrznego powinna upewnić się, że wszelkie procedury oceny ryzyka dokładnie oceniają znaczenie procesów podejmowanych przez dostawcę, szczególnie jeżeli funkcja audytu wewnętrznego zamierza wykorzystać tę możliwość w celu uzupełnienia własnej oceny ryzyka dostawcy. W przypadku (b) funkcja audytu wewnętrznego powinna ocenić adekwatność zakresu i jakości pracy wykonywanej przez każdą, pierwszą lub drugą linię zapewnienia dostawcy. w tym w uzasadnionych przypadkach za pomocą testów powtórnych.

c. Audyty kompleksowe

Na podstawie własnej oceny ryzyka audyt wewnętrzny może zdecydować o przeprowadzeniu bezpośrednich „audytów kompleksowych" na miejscu u zewnętrznego usługodawcy. Zazwyczaj będzie to obejmować szczegółowe badanie wykonywania przez usługodawcę kontroli operacyjnych przeprowadzanych procesów, a także analizę ogólnej organizacji zarządzania dostawcy w kontekście skutecznego zarządzania kluczowymi ryzykami, na które narażony jest proces zlecony na zewnątrz.

Oprócz audytu kompleksowego, audytowanie wyników procesów dostawcy może czasem także dostarczać zapewnienia – bez potrzeby faktycznego audytu dostawcy. Na przykład, jeśli dostawca dostarcza aplikację, funkcja audytu wewnętrznego może audytować zabezpieczenia systemu.

Przed rozpoczęciem audytu kompleksowego, audyt wewnętrzny powinien również wziąć pod uwagę praktyczne aspekty takiego przedsięwzięcia, w tym potencjalne ograniczenia w zakresie prywatności danych, w szczególności gdy dostawca obsługuje dane dla wielu klientów, które mogą wpłynąć na możliwość skutecznego wykonania audytu.

3 Testowanie oraz opieranie się na pracy innych

a. Funkcje pierwszej i drugiej linii zapewnienia

Audyt wewnętrzny może korzystać z pracy niezależnej pierwszej lub drugiej linii zapewnienia dla formułowania własnych ocen ryzyka dotyczących środowiska kontroli u dostawców, tam gdzie skuteczność tych funkcji została odpowiednio sprawdzona. W rezultacie audyt wewnętrzny może zrezygnować z przeprowadzania kompleksowych audytów u dostawców, u których zostały już wykonane odpowiednie testy przez inną funkcję zapewnienia banku, a funkcja audytu wewnętrznego upewniła się co do skuteczności tej funkcji.

b. Dział audytu wewnętrznego usługodawcy

W przypadku, gdy audyt wewnętrzny banku zamierza polegać na pracy audytu wewnętrznego usługodawcy, powinien on przeprowadzić odpowiednie testy działania funkcji audytu wewnętrznego dostawcy, w tym wykonanie testów powtórnych, w celu określenia skuteczności działania tej funkcji. Audyt wewnętrzny banku może również badać, czy dział audytu wewnętrznego usługodawcy został poddany zewnętrznej ocenie jakości zgodnie z zaleceniami standardu IPPF[2].

c. Zewnętrzni dostawcy zapewnienia

W szczególnych przypadkach usługodawca może zlecić stronie trzeciej przeprowadzenie niezależnej oceny kontroli – ma tu zastosowanie Międzynarodowy Standard Usług Atestacyjnych (ISAE) 3402[3] „Raport Kontroli Organizacji Usług" (Typ II). Oceniając wykorzystanie ocen kontroli, takich jak ISAE 3402, audyt wewnętrzny powinien starannie przeanalizować, czy zakres oceny jest wystarczający w stosunku do zakresu ryzyka usługodawcy. W wielu przypadkach konieczne jest uzupełnienie zakresu ISAE 3402 o dodatkowe procesy zarządzania ryzykiem.

---

[2] Standard IPPF (The International Professional Practices Framework) – Miedzynarodowe Ramowe Zasady Praktyki Zawodowej IIA

[3] MSUA 3402 (ang. ISAE 3402) to międzynarodowy standard, który umożliwia organizacji świadczącej usługi typu B2B przedstawienie realizowanych procesów oraz wdrożonych mechanizmów kontrolnych. W praktyce certyfikacja w oparciu o ten standard jest wykorzystywana przez organizacje usługowe (w szczególności biura rachunkowe lub centra usług wspólnych tj. shared service centres) do przedstawienia zarówno swoim klientom, jak i ich audytorom realizowanych usług w jednolitym i spójnym formacie.
System kontroli przedstawiony przez organizację podlega weryfikacji przez niezależnego audytora, w zakresie zgodności opisu oraz rzeczywistej efektywności opisanych mechanizmów kontrolnych. Niezależny audytor przedstawia ocenę systemu w dołączonym do raportu sprawozdaniu atestacyjnym.
Organizacje usługowe poddają się certyfikacji ISAE 3402, aby wykazać transparentność, jakość i bezpieczeństwo mechanizmów kontrolnych w procesach biznesowych, z pomocą których realizują obsługę swoich klientów.
Źródło: http://www.audytfinansowy.org/oferta/certyfikacja-msua-3402

We wszystkich powyższych przypadkach audyt wewnętrzny powinien, w ramach programu stałego monitorowania, nadzorować rozwiązywanie problemów podnoszonych przez innych dostawców zapewnienia, ponadto działanie to powinno być uzupełnieniem własnych ocen ryzyka przeprowadzanych przez funkcję audytu wewnętrznego.

4 Specjalne wymagania dotyczące outsourcingu do „FinTechs”

Pod wieloma względami, outsourcing do FinTechs nie różni się od outsourcingu od innych dostawców i powinny mieć tu zastosowanie podobne mechanizmy kontrolne. Kluczową kwestią związaną z partnerstwem w zakresie FinTech jest bezpieczeństwo danych klienta, które są przekazywane do FinTech. Wszędzie tam, gdzie to możliwe, banki powinny stosować silną ochronę kryptograficzną, aby chronić dane przechowywane i przesyłane przez systemy dostawców (takie jak chmura), a także zachowywać kontrolę nad kluczami kryptograficznymi. To pozwala bankowi na uzyskanie silnego zapewnienia, że dane są odpowiednio chronione, przy minimalnym zaangażowaniu w sprawdzanie mechanizmów kontroli działających u dostawcy usług. Funkcja audytu wewnętrznego może wówczas skupić się na badaniu określonych procesów, takich jak zarządzanie kluczami kryptograficznymi.

Audyt wewnętrzny musi również dokładnie ocenić, czy w banku panuje zdolność do zrozumienia i zarządzania ryzykiem związanym z FinTechs. Na przykład, czy bank dysponuje wystarczającą wiedzą do oceny bezpieczeństwa procesów kryptograficznych używanych w FinTechs? Jeśli nie, to ryzyko związane z używaniem FinTechs i ich technologii może nie zostać dostatecznie zrozumiane i efektywnie zarządzane. Funkcja audytu wewnętrznego musi również dokładnie ocenić własną zdolność do audytowania FinTechs.

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

Michał Fruba, CGAP, LA 9001, LA 27001, LA 20000, Prince 2 Practitioner, MSP, MoR, ITIL, ACE, Agile PM
Sebastian Burgemejster, CISA, CISM, CRISC, CGAP, CCSA, CRMA, CSXF, COSO, ACE

Skład DTP

Marcin Boguś