

PROJEKT

Komisja Nadzoru Finansowego

Rekomendacja H

dotycząca systemu kontroli wewnętrznej w bankach

Warszawa, 2016 r.

WSTĘP

Niniejsza Rekomendacja jest wydana na podstawie art. 137 ust. 1 pkt 5 ustawy z dnia 29 sierpnia 1997 r. – *Prawo bankowe* (Dz. U. z 2015 r. poz. 128, z późn. zm.) i art. 11 ust. 1 oraz art. 67 ust. 2 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2016 r. poz. 174 i 615) i stanowi nowelizację Rekomendacji H Komisji Nadzoru Finansowego (dalej: KNF) *dotyczącej systemu kontroli wewnętrznej w bankach*, wydanej w 2011 r. (dalej: Rekomendacja)¹.

Aktualna nowelizacja Rekomendacji ma na celu zapewnienie spójności oczekiwań KNF, w odniesieniu do dobrych praktyk w zakresie systemu kontroli wewnętrznej w bankach, ze zmienionymi przepisami prawa (z których część wejdzie w życie 1 stycznia 2016 r.) oraz obowiązującymi standardami rynkowymi.

Niniejsza Rekomendacja stanowi zbiór dobrych praktyk w zakresie systemu kontroli wewnętrznej, które przedstawiają oczekiwania KNF wobec banków w zakresie postępowania zgodnego z przepisami dotyczącymi znowelizowanych zasad funkcjonowania systemu kontroli wewnętrznej w banku, określonych w ustawie z dnia 29 sierpnia 1997 r. – *Prawo bankowe* i ustawie z dnia 7 grudnia 2000 r. *o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających* (Dz. U. z 2014 r. poz. 109 oraz z 2015 r. poz. 1166). Rekomendacja bierze także pod uwagę planowane zmiany legislacyjne zmierzające do zastąpienia (obowiązującej nie dłużej niż do końca kwietnia 2017 r.) uchwały Nr 258/2011 KNF², rozporządzeniem ministra właściwego do spraw instytucji finansowych, które zostanie wydane na podstawie art. 9f ust. 1 ustawy z dnia 29 sierpnia 1997 r. – *Prawo bankowe*, *określającym szczegółowy sposób funkcjonowania w bankach systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, w tym tryb anonimowego zgłaszania wskazanemu członkowi zarządu lub rady nadzorczej naruszeń prawa oraz obowiązujących w banku procedur i standardów etycznych, mając na względzie potrzebę zapewnienia skutecznego funkcjonowania organów statutowych banku i należytego podejścia do podejmowanego ryzyka w zakresie prowadzonej działalności, a także zapewnienie skutecznego działania mechanizmów wykrywania naruszeń*.

W Rekomendacji uwzględniono również krajowe standardy odnoszące się do zagadnień związanych z systemem kontroli wewnętrznej, w tym m.in. *Zasady Ładu Korporacyjnego dla instytucji nadzorowanych*, wydane przez KNF w dniu 22 lipca 2014 r. oraz opracowany przez

¹ Pierwsza Rekomendacja H *dotycząca kontroli wewnętrznej w banku* została opracowana w 1999 r. i zaktualizowana w 2002 r. przez Generalny Inspektorat Nadzoru Bankowego.

² Uchwała z dnia 4 października 2011 r. w sprawie szczegółowych warunków szacowania przez banki kapitału wewnętrznego i dokonywania przeglądów procesu szacowania i utrzymywania kapitału wewnętrznego oraz zasad ustalania polityki zmiennych składników wynagrodzeń osób zajmujących stanowiska kierownicze w banku.

KNF projekt Rekomendacji Z *dotyczącej zasadładu wewnętrznego w bankach*, jak również standardy wydawane przez inne instytucje (nadzorcze i branżowe), w tym:

- Wytyczne Europejskiego Urzędu Nadzoru Bankowego (European Banking Authority; EBA) z dnia 27 września 2011 r., w *sprawie zarządzania wewnętrznego (Guidelines on Internal Governance, GL44)*;
- Wytyczne Bazylejskiego Komitetu ds. Nadzoru Bankowego (Basel Committee on Banking Supervision; BCBS): (a) *Corporate governance principles for banks* z lipca 2015 r., (b) *The internal audit function in banks* z 2012 r., (c) *Compliance and the compliance function in banks* z kwietnia 2005 r.;
- *Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego* wydane przez Instytut Audytorów Wewnętrznych (The Institute of Internal Auditors; IIA) z 2012 r. oraz projekt ich zmian z 2016 r.;
- *Dobre Praktyki Spółek Notowanych na GPW 2016*, przyjęte dnia 13 października 2015 r. przez Giełdę Papierów Wartościowych w Warszawie;
- Wytyczne Komitetu Organizacji Sponsorujących Komisję Treadway (The Committee of Sponsoring Organizations of the Treadway Commission; COSO) *Internal Control — Integrated Framework* z 2013 r.

Uwzględniając istotne zmiany, jakie nastąpiły w otoczeniu regulacyjnym w ciągu pięciu lat od dokonania ostatniej nowelizacji Rekomendacji w 2011 r. (tj. wskazane powyżej zmiany polskich przepisów prawa i rekomendowanych standardów, jak i rozwiązań światowych, w tym zwłaszcza europejskich), znowelizowana Rekomendacja bazuje na następujących założeniach:

1. Oparcie systemu kontroli wewnętrznej na anglosaskiej koncepcji *internal control system*, tj. zbiorze mechanizmów kontrolnych zapewniających osiągnięcie ustawowo określonych celów (tj. skuteczności i efektywności działania banku, wiarygodności sprawozdawczości finansowej, przestrzegania zasad zarządzania ryzykiem w banku, zgodności działania banku z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi).
2. Traktowanie systemu kontroli wewnętrznej jako odrębnego systemu względem systemu zarządzania ryzykiem poprzez rozróżnienie tych dwóch systemów (zgodnie z ustawą z dnia 29 sierpnia 1997 r. – *Prawo bankowe*), z odrębnymi mechanizmami kontroli wewnętrznej (mechanizmami kontrolnymi) i mechanizmami kontroli ryzyka.
3. Umieszczenie komórki do spraw zgodności w systemie kontroli wewnętrznej oraz traktowanie jej jako kluczowego (obok funkcji kontroli) elementu zapewniania zgodności w banku (tj. zapewniania przestrzegania przez banki przepisów, regulacji wewnętrznych i standardów rynkowych), a tym samym wzmocnienie pozycji komórki do spraw zgodności, wychodząc naprzeciw potrzebom ograniczania rosnącego ryzyka braku zgodności z uwzględnieniem najlepszych praktyk w tym zakresie.

4. Usytuowanie w ramach systemu kontroli wewnętrznej komórki audytu wewnętrznego, mającej za zadanie prowadzenie niezależnej i obiektywnej działalności doradczej i zapewniającej, w szczególności poprzez badanie i ocenę adekwatności i skuteczności systemu zarządzania ryzykiem i systemu kontroli wewnętrznej.
5. Ujęcie systemu kontroli wewnętrznej w ramach tzw. modelu trzech linii (poziomów) obrony, poprzez wyodrębnienie trzech linii obrony (pierwsza linia obrony – operacyjne zarządzanie ryzykiem w banku, druga linia obrony – co najmniej niezależne zarządzanie ryzykiem oraz komórka do spraw zgodności, trzecia linia obrony – komórka audytu wewnętrznego) oraz przypisanie odpowiednich mechanizmów kontrolnych i niezależnego monitorowania przestrzegania tych mechanizmów do wszystkich tych linii obrony.

Zapisy niniejszej Rekomendacji mają pierwszeństwo w stosowaniu względem zapisów w zakresie kontroli wewnętrznej uwzględnionych w innych rekomendacjach i wytycznych KNF, w tym w szczególności w odniesieniu do zapisów:

- rozdziału 8 *Zasad Ładu Korporacyjnego dla instytucji nadzorowanych*, wydanych przez KNF w lipcu 2014 r.,
- rekomendacji 14 Rekomendacji M KNF *dotyczącej zarządzania ryzykiem operacyjnym w bankach*, wydanej przez KNF w styczniu 2013 r.,
- dotyczących oceny ryzyka nieosiągnięcia celów systemu kontroli wewnętrznej, wynikających z rekomendacji 17.2 Rekomendacji P *dotyczącej zarządzania ryzykiem płynności finansowej banków*, wydanej przez KNF w marcu 2015 r. i rekomendacji 21.2 Rekomendacji U *dotyczącej dobrych praktyk w zakresie bancassurance*, wydanej przez KNF w czerwcu 2014 r.,
- *Rekomendacji dotyczących funkcjonowania Komitetu Audytu*, wydanych przez KNF w listopadzie 2010 r., w zakresie dotyczącym monitorowania skuteczności systemów kontroli wewnętrznej i audytu wewnętrznego.

Zapisy Rekomendacji powinny być stosowane z uwzględnieniem zasady proporcjonalności, zwłaszcza w przypadku banków spółdzielczych. Oczekiwaniem nadzoru jest też, że w przypadku banków spółdzielczych będących uczestnikami systemu ochrony, o którym mowa w art. 22b ust. 1 ustawy z dnia 7 grudnia 2000 r. *o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających* kontrola wewnętrzna, o której mowa w art. 9c ust. 2 pkt 3 i art. 9d ust. 2 ustawy z dnia 29 sierpnia 1997 r. – *Prawo bankowe*, wykonywana w tych bankach na zasadach określonych w umowie systemu ochrony, będzie zgodna z niniejszą Rekomendacją.

Komisja Nadzoru Finansowego oczekuje, że niniejsza Rekomendacja zostanie wprowadzona w bankach nie później niż do dnia 30 czerwca 2017 r.

Słowniczek stosowanych pojęć

- 1) **Apetyt na ryzyko** – pojęcie to należy rozumieć zgodnie z Rekomendacją Z KNF *dotyczącą zasad ładu wewnętrznego w bankach*.
- 2) **Audyt wewnętrzny** – wyodrębniona w ramach systemu kontroli wewnętrznej banku, niezależna i obiektywna działalność doradcza i zapewniająca komórki audytu wewnętrznego, mająca na celu przysporzenie wartości i usprawnienie procesów w banku oraz dokonywanie oceny adekwatności i skuteczności systemu zarządzania, w tym w szczególności systemu zarządzania ryzykiem i systemu kontroli wewnętrznej.
- 3) **Audytór wewnętrzny** – pracownik komórki audytu wewnętrznego.
- 4) **Badanie audytowe** – przeprowadzane przez komórkę audytu wewnętrznego badanie i ocena wybranego lub wybranych obiektów audytowych, z uwzględnieniem oceny skuteczności i adekwatności systemu zarządzania ryzykiem i systemu kontroli wewnętrznej.
- 5) **Cele systemu kontroli wewnętrznej** – cztery ogólne cele, których osiągnięcie powinno być zapewniane przez system kontroli wewnętrznej, zgodnie z obowiązującymi przepisami prawa (art. 9c ust. 1 ustawy z dnia 29 sierpnia 1997 r. – *Prawo bankowe*) oraz wyodrębnione w ich ramach cele szczegółowe.
- 6) **Działalność doradcza audytu wewnętrznego** – prowadzona przez komórkę audytu wewnętrznego działalność, mająca na celu przysparzanie wartości oraz usprawnienie procesów w banku, niebędąca działalnością zapewniającą.
- 7) **Działalność zapewniająca audytu wewnętrznego** – prowadzona przez komórkę audytu wewnętrznego działalność, mająca na celu dokonywanie oceny adekwatności i skuteczności systemu zarządzania, w tym w szczególności systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, poprzez prowadzone w banku badania audytowe obejmujące całą działalność banku.
- 8) **Jednostka audytowana** – jednostka organizacyjna, komórka organizacyjna lub stanowisko organizacyjne banku, które jest objęte badaniem audytowym.
- 9) **Jednostka organizacyjna, komórka organizacyjna, stanowisko organizacyjne** – pojęcia te należy rozumieć zgodnie z Rekomendacją Z KNF *dotyczącą zasad ładu wewnętrznego w bankach*.
- 10) **Karta audytu** – regulamin funkcjonowania komórki audytu wewnętrznego.
- 11) **Kluczowy mechanizm kontrolny** – mechanizm kontrolny o kluczowym znaczeniu dla osiągnięcia danego celu ogólnego lub szczegółowego systemu kontroli wewnętrznej w danym procesie, bez przestrzegania / stosowania którego może zaistnieć nieakceptowalne przez bank ryzyko, że taki cel nie zostanie osiągnięty.

- 12) **Mechanizm kontrolny** – wyróżnione w ramach funkcji kontroli, wszelkie działanie lub rozwiązanie wykonywane i stosowane w ramach wszystkich trzech linii obrony, w tym zwłaszcza w ramach pierwszej linii obrony, mające za zadanie zapewnienie osiągnięcia celów ogólnych lub szczegółowych systemu kontroli wewnętrznej.
- 13) **Mechanizm kontroli ryzyka** – wyróżnione w ramach systemu zarządzania ryzykiem, wszelkie działanie i rozwiązanie wykonywane i stosowane w ramach pierwszej i drugiej linii obrony, mające za zadanie ograniczanie ryzyka występującego w banku poprzez zapewnienie, że zidentyfikowane i ocenione przez bank ryzyko nie przekroczy określonego poziomu (np. limity dopuszczalnej wielkości udzielanych kredytów, zasady oceny zdolności kredytowej, zabezpieczenie spłaty kredytu). Działanie mechanizmu kontroli ryzyka jest zapewniane poprzez stosowanie odpowiednio zaprojektowanych mechanizmów kontrolnych (np. rejestrowanie przekroczeń danego limitu, podział zadań w procesie oceny zdolności kredytowej, dokumentacja zabezpieczenia spłaty kredytu).
- 14) **Monitorowanie pionowe** – niezależne monitorowanie przez drugą linię obrony (weryfikacja bieżąca lub testowanie) przestrzegania mechanizmów kontrolnych w ramach pierwszej linii obrony.
- 15) **Monitorowanie poziome** – niezależne monitorowanie w ramach danej linii obrony (weryfikacja bieżąca lub testowanie) przestrzegania mechanizmów kontrolnych.
- 16) **Obiekt audytowy** – jednostki, komórki oraz stanowiska organizacyjne, a także procesy funkcjonujące w banku oraz w jego podmiotach zależnych, stanowiące potencjalny przedmiot badania audytowego.
- 17) **Plany audytu** – strategiczne (długoterminowe) i operacyjne (roczne) plany badań audytowych.
- 18) **Podmiot dominujący, podmiot zależny** – pojęcia te należy rozumieć zgodnie z ustawą z dnia 29 sierpnia 1997 r. – *Prawo bankowe*.
- 19) **Proces** – zbiór wszelkich wzajemnie powiązanych ze sobą czynności wykonywanych przez jednostki, komórki, stanowiska organizacyjne banku oraz jego podmioty zależne, których realizacja jest niezbędna do uzyskania określonego rezultatu (np. udzielenie kredytu, sprzedaż wierzytelności, zaksięgowanie transakcji określonego rodzaju, sporządzenie sprawozdania finansowego). W ramach procesów wykonywane są operacje, transakcje oraz inne czynności niezbędne do uzyskania określonego rezultatu.
- 20) **Proces zarządzania ryzykiem braku zgodności** – realizowany przez komórkę do spraw zgodności (przy ewentualnym wsparciu innych komórek pierwszej lub drugiej linii obrony), proces identyfikacji, oceny, kontroli i monitorowania ryzyka braku zgodności działalności banku z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi oraz przedstawianie raportów w tym zakresie.

- 21) **Proces audytowy** – sformalizowany proces obejmujący przygotowanie planów audytu, przygotowanie badania audytowego, przeprowadzenie badania audytowego oraz monitorowanie efektywności realizacji zaleceń poaudytowych.
- 22) **Raport z badania audytowego** – dokument lub dokumenty kończące badania audytowe, obejmujące co najmniej:
- opis badania audytowego, w tym jego cel, termin i zakres,
 - ustalenia badania audytowego wraz z wykrytymi nieprawidłowościami i ich kategoryzacją,
 - ocenę adekwatności i skuteczności systemu zarządzania ryzykiem i systemu kontroli wewnętrznej,
 - zalecenia poaudytowe wraz ze wskazanymi adresatami oraz terminami realizacji zaleceń.
- 23) **Ryzyko braku zgodności** – ryzyko zaistnienia negatywnych skutków nieprzestrzegania przepisów prawa, regulacji wewnętrznych oraz standardów rynkowych w procesach funkcjonujących w banku.
- 24) **System zarządzania, system kontroli wewnętrznej i system zarządzania ryzykiem** – pojęcia te należy rozumieć zgodnie z ustawą z dnia 29 sierpnia 1997 r. – *Prawo bankowe*.
- 25) **Testowanie** – porównywanie na wybranej próbie testowej stanu faktycznego ze stanem wymaganym, dokonywane w celu oceny co najmniej przestrzegania mechanizmów kontrolnych w odniesieniu do zakończonych czynności wykonywanych w ramach procesów funkcjonujących w banku. Testowanie, jako element niezależnego monitorowania w ramach funkcji kontroli, może być monitorowaniem poziomym (testowanie poziome w ramach danej linii obrony) lub monitorowaniem pionowym (testowanie pionowe pierwszej linii obrony przez drugą linię obrony).
- 26) **Trzy linie (poziomy) obrony** – system zarządzania ryzykiem i system kontroli wewnętrznej zorganizowany w banku na trzech, niezależnych i wzajemnie uzupełniających się liniach (poziomach), gdzie:
- na pierwszą linię obrony składa się operacyjne zarządzanie ryzykiem, powstałym w związku z działalnością prowadzoną przez bank,
 - na drugą linię obrony składa się co najmniej zarządzanie ryzykiem przez pracowników na specjalnie powoływanych do tego stanowiskach lub w komórkach organizacyjnych, niezależnie od operacyjnego zarządzania ryzykiem na pierwszym poziomie oraz działalność komórki do spraw zgodności,
 - na trzecią linię obrony składa się działalność komórki audytu wewnętrznego.

Na wszystkich trzech liniach obrony bank stosuje odpowiednio mechanizmy kontrolne oraz niezależnie monitoruje ich przestrzeganie.

- 27) **Uniwersum audytu** – zbiór obiektów audytowych obejmujący całą działalność banku oraz jego podmiotów zależnych.
- 28) **Ustawa o funkcjonowaniu banków spółdzielczych** – ustawa z dnia 7 grudnia 2000 r. *o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających* (Dz. U. z 2014 r. poz. 109 oraz z 2015 r. poz. 1166).
- 29) **Ustawa – Prawo bankowe** – ustawa z dnia 29 sierpnia 1997 r. – *Prawo bankowe* (Dz. U. z 2015 r. poz. 128 z późn. zm.).
- 30) **Weryfikacja bieżąca** – porównywanie stanu faktycznego ze stanem wymaganym, dokonywane w celu oceny co najmniej przestrzegania mechanizmów kontrolnych, przed rozpoczęciem lub w trakcie trwających czynności wykonywanych w ramach procesów funkcjonujących w banku. Weryfikacja bieżąca, jako element niezależnego monitorowania w ramach funkcji kontroli, może być monitorowaniem poziomym (weryfikacja bieżąca pozioma w ramach danej linii obrony) lub monitorowaniem pionowym (weryfikacja bieżąca pionowa pierwszej linii obrony przez drugą linię obrony).
- 31) **Zapewnianie zgodności** – zapewnianie przestrzegania przepisów prawa, regulacji wewnętrznych oraz standardów rynkowych, odpowiednio poprzez funkcję kontroli oraz zarządzanie ryzykiem braku zgodności.

LISTA REKOMENDACJI

A. ORGANIZACJA SYSTEMU KONTROLI WEWNĘTRZNEJ W BANKU

Rekomendacja 1

W ramach trzech linii obrony bank powinien projektować, wprowadzać oraz zapewniać funkcjonowanie adekwatnego i skutecznego systemu kontroli wewnętrznej, ustanowić kryteria adekwatności i skuteczności tego systemu, określić zadania zarządu banku i rady nadzorczej oraz ogłosić, w sposób ogólnie dostępny, opis systemu kontroli wewnętrznej.

Rekomendacja 2

W ramach celów ogólnych systemu kontroli wewnętrznej bank powinien wyodrębnić cele szczegółowe oraz powiązać je z procesami funkcjonującymi w banku.

Rekomendacja 3

Zarząd banku powinien opracować zasady kategoryzacji, dokumentowania i raportowania o nieprawidłowościach wykrytych przez system kontroli wewnętrznej.

B. FUNKCJA KONTROLI

Rekomendacja 4

Zarząd banku odpowiada za projektowanie, wprowadzanie i zapewnianie działania funkcji kontroli, a rada nadzorcza za nadzór i coroczną ocenę funkcji kontroli.

Rekomendacja 5

Bank powinien określić kryteria, jakie są uwzględniane przy projektowaniu mechanizmów kontrolnych oraz dokumentować ich projektowanie, wprowadzanie i stosowanie.

Rekomendacja 6

Bank powinien zapewniać niezależne monitorowanie przestrzegania mechanizmów kontrolnych, obejmujące weryfikację bieżącą oraz testowanie.

Rekomendacja 7

Weryfikacja bieżąca powinna być dokonywana w sposób ciągły w ramach procesów funkcjonujących w banku.

Rekomendacja 8

Testowanie powinno obejmować ocenę co najmniej przestrzegania mechanizmów kontrolnych i być dokonywane w przypadku zakończonych czynności wykonywanych

w ramach procesów funkcjonujących w banku.

Rekomendacja 9

Bank powinien ustanowić matrycę funkcji kontroli oraz określić zakres zadań odnośnie zapewniania funkcjonowania matrycy.

Rekomendacja 10

Bank powinien określić zasady raportowania co najmniej o kluczowych mechanizmach kontrolnych oraz wynikach testowania pionowego.

C. ZAPEWNIANIE ZGODNOŚCI

Rekomendacja 11

Bank powinien wyodrębnić zapewnianie zgodności jako jeden z czterech ogólnych celów systemu kontroli wewnętrznej. Bank powinien zapewniać zgodność poprzez funkcję kontroli oraz zarządzanie ryzykiem braku zgodności.

Rekomendacja 12

Bank powinien wyodrębnić komórkę do spraw zgodności, zapewnić jej odpowiednie usytuowanie w strukturze organizacyjnej banku, określić w sposób formalny jej uprawnienia i obowiązki, jak również zapewniać niezależność oraz odpowiedni status kierującemu komórką do spraw zgodności i jej pracownikom.

Rekomendacja 13

Zapewnianie zgodności, w ramach funkcji kontroli, powinno obejmować stosowanie mechanizmów kontrolnych, niezależne monitorowanie ich przestrzegania oraz raportowanie.

Rekomendacja 14

Proces zarządzania ryzykiem braku zgodności powinien obejmować identyfikację, ocenę, kontrolę, monitorowanie oraz raportowanie o ryzyku braku zgodności przez komórkę do spraw zgodności. Bank powinien zdefiniować ryzyko braku zgodności oraz opracować odpowiednie procedury i metodyki.

Rekomendacja 15

W ramach procesu zarządzania ryzykiem braku zgodności bank powinien identyfikować ryzyko braku zgodności. Bank powinien szczegółowo określić zakres informacji wykorzystywanych do identyfikacji ryzyka braku zgodności.

Rekomendacja 16

W ramach zarządzania ryzykiem braku zgodności, bank powinien oceniać zidentyfikowane ryzyko braku zgodności poprzez pomiar ilościowy lub szacowanie jakościowe.

Rekomendacja 17

W ramach procesu zarządzania ryzykiem braku zgodności, bank powinien projektować i wprowadzać mechanizmy kontroli ryzyka braku zgodności w celu utrzymania ryzyka braku zgodności na określonym poziomie.

Rekomendacja 18

W ramach procesu zarządzania ryzykiem braku zgodności, bank powinien monitorować wielkość i profil ryzyka braku zgodności. Bank powinien określić przy tym zakres testowania sposobu wdrożenia i przestrzegania mechanizmów kontroli ryzyka braku zgodności.

Rekomendacja 19

W ramach zarządzania ryzykiem braku zgodności, bank powinien, co kwartał, jednocześnie raportować do zarządu banku i rady nadzorczej lub komitetu audytu, jeżeli został powołany, o wynikach identyfikacji, oceny, kontroli i monitorowania wielkości i profilu ryzyka braku zgodności.

Rekomendacja 20

Bank powinien opracować zasady współpracy komórki do spraw zgodności banku z analogicznymi komórkami podmiotu dominującego i podmiotów zależnych, jak również określić zakres dopuszczalnego korzystania z usług doradczych podmiotów zewnętrznych.

Rekomendacja 21

Bank powinien opracować zasady raportowania przez komórkę do spraw zgodności, odnośnie realizacji jej zadań, do zarządu banku i rady nadzorczej.

D. AUDYT WEWNĘTRZNY

Rekomendacja 22

Bank powinien wyodrębnić niezależną komórkę audytu wewnętrznego i przypisać jej zadania wykonywane w ramach działalności zapewniającej oraz działalności doradczej.

Rekomendacja 23

Bank powinien zapewnić odpowiednie usytuowanie komórki audytu wewnętrznego w strukturze organizacyjnej banku, określić w sposób formalny jej uprawnienia i obowiązki, jak również zapewniać niezależność, obiektywizm oraz odpowiedni status kierującemu komórką audytu wewnętrznego i audytorom wewnętrznym.

Rekomendacja 24

Bank powinien szczegółowo określić prawa i obowiązki kierującego komórką audytu wewnętrznego, kierującego badaniem audytowym oraz audytorów wewnętrznych, zwłaszcza w odniesieniu do procesu audytowego, a także opracować szczegółowe procedury i metodyki badania audytowego.

Rekomendacja 25

W ramach procesu audytowego bank powinien stosować plany audytu, których przygotowywanie i zatwierdzanie powinno być poprzedzone analizą poziomu ryzyka wynikającego z działalności prowadzonej przez bank.

Rekomendacja 26

W ramach procesu audytowego audytorzy wewnętrzni powinni z należytą starannością przygotować się do badania audytowego. Kierujący badaniem audytowym powinien opracować program badania audytowego.

Rekomendacja 27

W ramach procesu audytowego audytorzy wewnętrzni powinni w sposób niezależny i obiektywny przeprowadzić badanie audytowe, które powinno być zakończone raportem z badania audytowego.

Rekomendacja 28

W ramach procesu audytowego komórka audytu wewnętrznego powinna monitorować efektywność realizacji zaleceń poaudytowych.

Rekomendacja 29

Bank powinien opracować zasady współpracy komórki audytu wewnętrznego banku z analogicznymi komórkami podmiotu dominującego i podmiotów zależnych oraz z biegłym rewidentem.

Rekomendacja 30

Bank powinien opracować program zapewniania jakości działalności doradczej i zapewniającej, wykonywanej przez komórkę audytu wewnętrznego.

Rekomendacja 31

Bank powinien opracować zasady raportowania przez komórkę audytu wewnętrznego do zarządu banku i rady nadzorczej lub komitetu audytu, jeżeli został powołany.

REKOMENDACJE

A. ORGANIZACJA SYSTEMU KONTROLI WEWNĘTRZNEJ

Rekomendacja 1

W ramach trzech linii obrony bank powinien projektować, wprowadzać oraz zapewniać funkcjonowanie adekwatnego i skutecznego systemu kontroli wewnętrznej, ustanowić kryteria adekwatności i skuteczności tego systemu, określić zadania zarządu banku i rady nadzorczej oraz ogłosić, w sposób ogólnie dostępny, opis systemu kontroli wewnętrznej.

- 1.1 Zarząd banku powinien projektować, wprowadzać oraz zapewniać w odniesieniu do wszystkich jednostek, komórek, stanowisk organizacyjnych oraz podmiotów zależnych, funkcjonowanie adekwatnego i skutecznego systemu kontroli wewnętrznej, który obejmuje funkcję kontroli, komórkę do spraw zgodności i komórkę audytu wewnętrznego oraz powinien zapewniać niezależność tym komórkom, jednostkom i stanowiskom, środki finansowe niezbędne do skutecznego wykonywania zadań oraz systematycznego podnoszenia kwalifikacji i zdobywania doświadczenia oraz umiejętności przez pracowników tych jednostek, komórek i stanowisk.
- 1.2 Zarząd banku powinien podejmować działania mające na celu zapewnienie ciągłości działania systemu kontroli wewnętrznej, w tym właściwej współpracy wszystkich pracowników banku w ramach funkcji kontroli oraz z komórką do spraw zgodności i komórką audytu wewnętrznego. Bank powinien również zapewnić dostęp pracowników tych komórek do niezbędnych dokumentów źródłowych, w tym zawierających informacje poufne, w związku z wykonywaniem przez nich obowiązków służbowych.
- 1.3 Zarząd banku, projektując, wprowadzając i zapewniając funkcjonowanie adekwatnego i skutecznego systemu kontroli wewnętrznej powinien uwzględniać:
 - a) stopień skomplikowania procesów funkcjonujących w banku i w podmiotach zależnych,
 - b) zasoby, którymi dysponuje bank,
 - c) ryzyko zaistnienia nieprawidłowości w zakresie poszczególnych procesów, w tym w szczególności w zakresie procesów istotnych,
 - d) ocenę dotychczasowej adekwatności i skuteczności pierwszej, drugiej i trzeciej linii obrony.
- 1.4 Zarząd banku powinien ustanowić kryteria adekwatności i skuteczności systemu kontroli wewnętrznej, a rada nadzorcza powinna je zatwierdzić. Kryteria te powinny być odpowiednio stosowane w ramach wszystkich trzech linii obrony oraz podlegać

okresowej aktualizacji. Zarząd banku powinien określić rodzaje działań podejmowanych w celu usunięcia nieprawidłowości wykrytych przez system kontroli wewnętrznej, w tym środki naprawcze i dyscyplinujące. Do środków naprawczych powinno należeć w szczególności, projektowanie nowych i aktualizacja dotychczasowych mechanizmów kontrolnych (np. zmiana procedury, modyfikacja poszczególnych procesów, szkolenia).

- 1.5 W przypadku, gdy bank wprowadza system kontroli wewnętrznej uwzględniający rozwiązania funkcjonujące w jego podmiocie dominującym, zarząd banku powinien zapewnić zgodność tego systemu z przepisami prawa krajowego i niniejszą Rekomendacją, w tym dokonać udokumentowanej analizy potwierdzającej tę zgodność (np. dokonać mapowania przyjętego systemu na poszczególne rekomendacje niniejszej Rekomendacji).
- 1.6 Zarząd banku powinien, nie rzadziej niż raz w roku, informować radę nadzorczą o sposobie wypełnienia zadań, o których mowa w rekomendacjach 1.1-1.4, ze szczególnym uwzględnieniem:
 - a) adekwatności i skuteczności systemu kontroli wewnętrznej w zapewnianiu osiągnięcia każdego z celów systemu kontroli wewnętrznej,
 - b) skali i charakterze nieprawidłowości znaczących i krytycznych oraz najważniejszych działaniach zmierzających do usunięcia tych nieprawidłowości, w tym o podjętych środkach naprawczych i dyscyplinujących,
 - c) zapewniania niezależności komórce do spraw zgodności i komórce audytu wewnętrznego,
 - d) zapewniania środków finansowych niezbędnych do skutecznego wykonywania zadań przez pracowników komórki do spraw zgodności i komórki audytu wewnętrznego oraz do systematycznego podnoszenia kwalifikacji oraz zdobywania doświadczenia i umiejętności przez pracowników tych komórek.
- 1.7 Rada nadzorcza powinna sprawować nadzór nad projektowaniem, wprowadzeniem i zapewnianiem funkcjonowania adekwatnego i skutecznego systemu kontroli wewnętrznej, w szczególności w oparciu o informacje otrzymywane od zarządu banku oraz komórki do spraw zgodności i komórki audytu wewnętrznego. W ramach nadzoru nad systemem kontroli wewnętrznej, rada nadzorcza może zlecić bieżące monitorowanie systemu kontroli wewnętrznej komitetowi audytu. Bez względu na zlecenie bieżącego monitorowania systemu kontroli wewnętrznej komitetowi audytu, rada nadzorcza powinna odpowiadać za nadzór i coroczną ocenę adekwatności i skuteczności systemu kontroli wewnętrznej.
- 1.8 Rada nadzorcza powinna dokonać corocznej oceny adekwatności i skuteczności systemu kontroli wewnętrznej, w tym adekwatności i skuteczności funkcji kontroli,

komórki do spraw zgodności oraz komórki audytu wewnętrznego. W ramach dokonywanej oceny rada nadzorcza powinna w szczególności uwzględnić:

- a) opinię komitetu audytu, jeżeli taki komitet został powołany,
- b) informację zarządu banku, o której mowa w rekomendacji 1.6,
- c) okresowe raporty komórki do spraw zgodności i komórki audytu wewnętrznego,
- d) istotne, z punktu widzenia adekwatności i skuteczności systemu kontroli wewnętrznej, informacje uzyskane od podmiotu dominującego, podmiotów zależnych lub instytucjonalnego systemu ochrony,
- e) ustalenia dokonane przez biegłego rewidenta,
- f) ustalenia wynikające z czynności nadzorczych wykonywanych przez uprawnione do tego instytucje (np. KNF, Urząd Ochrony Konkurencji i Konsumentów),
- g) istotne z punktu widzenia adekwatności i skuteczności systemu kontroli wewnętrznej, oceny i opinie dokonywane przez podmioty zewnętrzne, jeżeli były wydawane.

1.9 Bank powinien ogłosić w sposób ogólnie dostępny, w tym na stronie internetowej (jeżeli ją prowadzi), opis systemu kontroli wewnętrznej, uwzględniający:

- a) cele systemu kontroli wewnętrznej,
- b) rolę zarządu banku, rady nadzorczej i komitetu audytu, jeżeli został powołany,
- c) przyjęty schemat organizacji trzech linii obrony w ramach struktury organizacyjnej banku,
- d) funkcję kontroli, w tym najczęściej stosowane rodzaje mechanizmów kontrolnych i sposób ich niezależnego monitorowania,
- e) umiejscowienie, zakres zadań, niezależność komórki do spraw zgodności i komórki audytu wewnętrznego,
- f) przyjęte kryteria adekwatności i skuteczności systemu kontroli wewnętrznej oraz zasady kategoryzacji nieprawidłowości,
- g) zasady corocznej oceny skuteczności i adekwatności systemu kontroli wewnętrznej, dokonywanej przez radę nadzorczą.

Rekomendacja 2

W ramach celów ogólnych systemu kontroli wewnętrznej bank powinien wyodrębnić cele szczegółowe oraz powiązać je z procesami funkcjonującymi w banku.

2.1 Zarząd banku, wyodrębniając cele szczegółowe systemu kontroli wewnętrznej, powinien uwzględnić co najmniej takie aspekty, jak:

- a) zakres i stopień złożoności działalności banku,
- b) zakres stosowania określonych przepisów prawa, standardów rynkowych oraz obowiązujących w banku regulacji wewnętrznych do których przestrzegania zobowiązany jest bank,

- c) stopień osiągania planów operacyjnych i biznesowych przyjętych w banku,
 - d) kompletność, prawidłowość i kompleksowość procedur księgowych;
 - e) jakość (dokładność i niezawodność) systemów: księgowego, sprawozdawczego i operacyjnego,
 - f) adekwatność, funkcjonalność i bezpieczeństwo środowiska teleinformatycznego,
 - g) struktura organizacyjna banku, podział kompetencji i zasady koordynacji działań pomiędzy poszczególnymi jednostkami, komórkami, stanowiskami organizacyjnymi, a także system tworzenia i obiegu dokumentów i informacji,
 - h) zakres czynności powierzonych przez bank do wykonania podmiotom zewnętrznym.
- 2.2 Zarząd banku powinien zatwierdzać kryteria wyboru danego procesu za istotny, uwzględniając strategię zarządzania bankiem i jego model biznesowy, wpływ danego procesu na wynik finansowy i adekwatność kapitałową banku, strategię zarządzania ryzykiem, apetyt na ryzyko oraz krytyczne i kluczowe procesy określone przez bank zgodnie z Rekomendacją M KNF *dotyczącą zarządzania ryzykiem operacyjnym w bankach*.
- 2.3 Przy wyborze istotnych procesów bank powinien również uwzględniać rolę podmiotów zależnych, jeżeli mają one wpływ na zapewnianie osiągnięcia celów ogólnych systemu kontroli wewnętrznej.
- 2.4 Zarząd banku powinien zatwierdzać wyniki wyboru istotnych procesów oraz dokonywać powiązania każdego z celów ogólnych i szczegółowych z procesami istotnymi funkcjonującymi w banku. Zarząd banku powinien dokonywać regularnego przeglądu wszystkich procesów funkcjonujących w banku pod kątem ich istotności.

Rekomendacja 3

Zarząd banku powinien opracować zasady kategoryzacji, dokumentowania i raportowania o nieprawidłowościach wykrytych przez system kontroli wewnętrznej.

- 3.1 Zarząd banku powinien opracować zasady kategoryzacji nieprawidłowości wykrytych przez system kontroli wewnętrznej, obejmujących co najmniej nieprawidłowości znaczące i krytyczne, biorąc pod uwagę ich negatywny wpływ na zapewnianie osiągnięcia określonych celów systemu kontroli wewnętrznej.
- 3.2 Zarząd banku, określając kategorie nieprawidłowości, powinien ustanowić procedury, zgodnie z którymi:
- a) w przypadku wykrycia nieprawidłowości znaczących i krytycznych w ramach pierwszej linii obrony, powinny one być niezwłocznie raportowane do komórki organizacyjnej drugiej linii obrony, odpowiedzialnej za niezależne monitorowanie procesu, w ramach którego zaistniała dana nieprawidłowość krytyczna, oraz do

komórki audytu wewnętrznego, a w przypadku nieprawidłowości krytycznych, również do zarządu banku,

- b) w przypadku wykrycia nieprawidłowości znaczących i krytycznych w ramach drugiej linii obrony, powinny one być niezwłocznie raportowane do komórki audytu wewnętrznego, a w przypadku nieprawidłowości krytycznych, również do zarządu banku i rady nadzorczej lub komitetu audytu, jeżeli został powołany.

3.3 Wszelkie wykryte nieprawidłowości powinny być, w miarę możliwości, niezwłoczne korygowane. Bank powinien prowadzić rejestr wszystkich nieprawidłowości znaczących i krytycznych.

B. FUNKCJA KONTROLI

Rekomendacja 4

Zarząd banku odpowiada za projektowanie, wprowadzanie i zapewnianie działania funkcji kontroli, a rada nadzorcza za nadzór i coroczną ocenę funkcji kontroli.

- 4.1. Zarząd banku powinien ustanowić odpowiednie zasady projektowania, zatwierdzania i wdrażania mechanizmów kontrolnych we wszystkich procesach funkcjonujących w banku, w tym określić rolę komórek odpowiedzialnych za opracowanie projektu mechanizmu kontrolnego, jego zatwierdzenie oraz wdrożenie. Zarząd banku odpowiada za zapewnienie adekwatności i skuteczności mechanizmów kontrolnych w procesach funkcjonujących w banku.
- 4.2. Zarząd banku powinien ustanowić odpowiedni zakres i kryteria niezależnego monitorowania przestrzegania mechanizmów kontrolnych, obejmujący weryfikację bieżącą i testowanie.
- 4.3. Zarząd banku powinien zapewnić funkcjonowanie w banku matrycy funkcji kontroli oraz przypisać odpowiednie zadania związane z prowadzeniem tej matrycy.
- 4.4. Zarząd banku powinien ustanowić zasady raportowania co najmniej o efektywności kluczowych mechanizmów kontrolnych oraz o wynikach ich testowania pionowego.
- 4.5. Rada nadzorcza, dokonując corocznej oceny funkcji kontroli, powinna brać pod uwagę także wypełnianie przez zarząd banku obowiązków, o których mowa w części B niniejszej Rekomendacji.

Rekomendacja 5

Bank powinien określić kryteria, jakie są uwzględniane przy projektowaniu mechanizmów kontrolnych oraz dokumentować ich projektowanie, wprowadzanie i stosowanie.

- 5.1. Bank powinien określić kryteria, jakie są uwzględniane przy projektowaniu mechanizmów kontrolnych, które powinny obejmować co najmniej:
 - a) adekwatność danego rodzaju mechanizmu kontrolnego w odniesieniu do poszczególnych procesów,
 - b) skuteczność danego rodzaju mechanizmu kontrolnego w przeszłości,
 - c) możliwość niezależnego monitorowania danego mechanizmu kontrolnego.
- 5.2. Bank powinien określić kryteria wyboru kluczowych mechanizmów kontrolnych dostosowanych do specyfiki banku, jak również zapewniać, że mechanizmy te odgrywają podstawową rolę w zapewnianiu osiągnięcia celów systemu kontroli

wewnętrznej. Bank powinien przypisać kluczowe mechanizmy kontrolne co najmniej procesom istotnym. Bank powinien zapewnić dokonywanie z odpowiednią częstotliwością niezależnego monitorowania oraz badania w ramach trzeciej linii obrony, przestrzegania kluczowych mechanizmów kontrolnych.

- 5.3. Mechanizmy kontrolne powinny być odpowiednio stosowane w zakresie wszystkich trzech linii obrony, we wszystkich procesach funkcjonujących w banku, spełniając rolę:
- a) prewencyjną – poprzez zapobieganie nieprawidłowościom (np. poprzez ustalenie ścieżki autoryzacji w procesie odstępstw, wprowadzenie zasad kontroli dostępu),
 - b) detekcyjną – poprzez wykrywanie nieprawidłowości (np. poprzez weryfikację dokumentacji),
 - c) korekcyjną – poprzez korektę nieprawidłowości (np. poprzez zapewnienie automatycznego korygowania błędów w systemach informatycznych, w odniesieniu do określonych pól wypełnianych przez pracowników banku).
- 5.4. W zależności od określonych celów ogólnych i szczegółowych systemu kontroli wewnętrznej, stopnia złożoności procesów, ryzyka zaistnienia nieprawidłowości oraz z uwzględnieniem dostępnych zasobów, bank powinien stosować zróżnicowane mechanizmy kontrolne, w tym: automatyczne (wbudowane w systemy informatyczne), półautomatyczne i manualne. Bank powinien unikać stosowania wyłącznie manualnych mechanizmów kontrolnych w danym procesie.
- 5.5. Do głównych rodzajów mechanizmów kontrolnych funkcjonujących w banku powinny należeć co najmniej:
- a) procedury – rozumiane jako zdefiniowany sposób określonego postępowania przez pracowników poszczególnych komórek organizacyjnych,
 - b) podział obowiązków – rozumiany jako podział zadań i uprawnień przypisanych pracownikom na poszczególnych stanowiskach w ramach danego procesu, mający na celu zapobieganie sytuacjom, w których pracownik kontroluje samego siebie lub istnieje potencjalny konflikt interesów między pracownikami mającymi powiązania personalne (np. poprzez oddzielenie etapu zawierania transakcji od etapów jej rejestrowania i weryfikowania jej prawidłowości albo tzw. kontrolę dwóch par oczu),
 - c) autoryzacja, w tym zwłaszcza autoryzacja operacji finansowych i gospodarczych – rozumiana jako system zatwierdzania decyzji i czynności wykonywanych przez pracowników na poszczególnych stanowiskach w ramach danego procesu (np. poprzez wprowadzenie obowiązku autoryzacji w systemie informatycznym w procesie zawierania transakcji przekraczających określony poziom limitów obowiązujących w banku),

- d) kontrola dostępu – rozumiana jako zestaw uprawnień dostępu do określonego obszaru, systemu, procesu,
 - e) kontrola fizyczna – rozumiana jako zestaw uprawnień dostępu do określonego, fizycznie wydzielonego obszaru w banku (np. poprzez zapewnienie autoryzowanego wstępu (z zastosowaniem karty / kodu), na teren niektórych jednostek lub komórek organizacyjnych banku),
 - f) ewidencjonowanie systemów: księgowego, sprawozdawczego i operacyjnego oraz operacji finansowych i gospodarczych – rozumiane jako system rejestrowania i przechowywania określonych rodzajowo danych wprowadzonych i generowanych w danym systemie,
 - g) weryfikacja, w tym inwentaryzacja – rozumiana jako porównywanie stanu faktycznego ze stanem wymaganym,
 - h) nadzór przełożonego – rozumiany jako sprawowanie przez przełożonego w toku nadzoru służbowego określonych czynności sprawdzających w stosunku do podległego pracownika,
 - i) rejestr odstępstw – rozumiany jako wykaz zarejestrowanych wyjątków w ramach wykonywania określonych czynności wynikających z ustalonych przez bank zasad (procedur) postępowania,
 - j) wskaźniki wydajności – rozumiane jako wskaźniki prezentujące stopień wykonania danego celu w określonym czasie,
 - k) organizacja szkoleń dla pracowników banku.
- 5.6. W przypadku mechanizmów kontroli ryzyka (np. limit), mechanizmy kontrolne (np. nadzór przełożonego odnośnie przestrzegania limitu), powinny zapewniać, że mechanizmy kontroli ryzyka są przestrzegane.
- 5.7. Bank powinien dokumentować proces projektowania, zatwierdzania i wprowadzania mechanizmów kontrolnych w sposób umożliwiający zidentyfikowanie komórki odpowiedzialnej za opracowanie projektu mechanizmu kontrolnego, jego zatwierdzenie oraz wdrożenie. Bank powinien dokumentować stosowanie mechanizmów kontrolnych³ w sposób umożliwiający niezależne monitorowanie przestrzegania poszczególnych mechanizmów kontrolnych, badanie i ocenę ich adekwatności i skuteczności przez komórkę audytu wewnętrznego, przeprowadzanie badań przez biegłych rewidentów oraz dokonywanie czynności nadzorczych przez uprawnione do tego instytucje. Do podstawowych sposobów dokumentowania powinny należeć w szczególności:
- a) podpisy na dokumentach,
 - b) rejestrowanie każdej operacji, transakcji, produktu i usługi,

³ W praktyce często można się spotkać z nazwą „dowody kontroli”.

- c) przechowywanie w systemie informatycznym potwierdzenia stosowania poszczególnych mechanizmów kontrolnych,
- d) raporty, w tym generowane przez system informatyczny.

Rekomendacja 6

Bank powinien zapewniać niezależne monitorowanie przestrzegania mechanizmów kontrolnych, obejmujące weryfikację bieżącą oraz testowanie.

- 6.1. Niezależne monitorowanie przestrzegania mechanizmów kontrolnych powinno być wpisane we wszystkie procesy funkcjonujące w banku oraz stosowane odpowiednio:
 - a) jako monitorowanie poziome w ramach pierwszej linii obrony oraz monitorowanie pionowe pierwszej linii obrony przez drugą linię obrony,
 - b) jako monitorowanie poziome w ramach drugiej linii obrony,
 - c) jako monitorowanie poziome w ramach trzeciej linii obrony, poprzez wykonywanie czynności w ramach programu zapewniania jakości, o którym mowa w rekomendacji 30.
- 6.2. Niezależne monitorowanie przestrzegania mechanizmów kontrolnych powinno obejmować weryfikację bieżącą i testowanie. Bank powinien przyjąć odpowiednie proporcje pomiędzy weryfikacją bieżącą i testowaniem, w ramach monitorowania pionowego i poziomego, biorąc pod uwagę cele systemu kontroli wewnętrznej, stopień złożoności procesów, w tym zwłaszcza procesów istotnych, liczbę, rodzaj i stopień złożoności mechanizmów kontrolnych, ryzyko zaistnienia nieprawidłowości, a także zasoby poszczególnych linii obrony, w tym kwalifikacje, doświadczenie i umiejętności pracowników tych linii.
- 6.3. Bank powinien w sposób jednoznaczny przypisać komórkom organizacyjnym odpowiedzialność za wykonywanie zadań związanych z monitorowaniem pionowym lub poziomym. Pracownicy komórek organizacyjnych odpowiedzialni za wykonywanie zadań związanych z monitorowaniem pionowym i poziomym, powinni posiadać odpowiednie kwalifikacje, doświadczenie i umiejętności w zakresie związanym z wykonywaniem tych zadań.
- 6.4. Bank powinien zapewniać niezależność monitorowania pionowego poprzez jednoznaczne wyodrębnienie linii obrony oraz niezależność monitorowania poziomego poprzez jednoznaczne rozdzielenie zadań dotyczących stosowania danego mechanizmu kontrolnego i niezależnego monitorowania jego przestrzegania w ramach danej linii. Poza przypadkami bieżącej weryfikacji w ramach monitorowania poziomego, o której mowa w rekomendacji 7.2a, ta sama osoba nie powinna jednocześnie odpowiadać za

stosowanie danego mechanizmu kontrolnego oraz niezależne monitorowanie jego przestrzegania.

Rekomendacja 7

Weryfikacja bieżąca powinna być dokonywana w sposób ciągły w ramach procesów funkcjonujących w banku.

- 7.1. Weryfikacja bieżąca powinna być stosowana przed rozpoczęciem lub w trakcie czynności wykonywanych w ramach procesów funkcjonujących w banku. Bank powinien określić, co w danym procesie jest mechanizmem kontrolnym, a co jego weryfikacją bieżącą.
- 7.2. Weryfikacja bieżąca powinna być podstawowym elementem monitorowania poziomego, w szczególności w ramach pierwszej linii obrony i może być realizowana przez⁴:
 - a) pracownika w toku wykonywania przez niego czynności operacyjnych (np. weryfikacja poprawności dokumentacji kredytowej lub danych wprowadzonych w odpowiednich polach w systemie informatycznym),
 - b) przełożonego w ramach wykonywania nadzoru służbowego,
 - c) innego pracownika tej samej komórki w ramach podziału obowiązków (tzw. weryfikacja na drugą rękę).
- 7.3. Weryfikacja bieżąca jako element monitorowania pionowego powinna być dokumentowana w sposób analogiczny do wskazanego w rekomendacji 5.7.

Rekomendacja 8

Testowanie powinno obejmować ocenę co najmniej przestrzegania mechanizmów kontrolnych i być dokonywane w przypadku zakończonych czynności wykonywanych w ramach procesów funkcjonujących w banku.

- 8.1. Testowanie powinno być stosowane w przypadku zakończonych czynności wykonywanych w ramach procesów funkcjonujących w banku, w tym na wybranej próbie testowej.
- 8.2. W ramach monitorowania poziomego, komórka organizacyjna powinna testować (testowanie poziome⁵) co najmniej przestrzeganie mechanizmów kontrolnych w ramach tej samej linii obrony, co komórka organizacyjna przeprowadzająca testy.

⁴ Można się spotkać z określeniem „kontrola funkcjonalna wstępna i bieżąca”.

⁵ Można się spotkać z określeniem „kontrola funkcjonalna następna”.

W ramach monitorowania pionowego, komórka organizacyjna usytuowana w drugiej linii obrony powinna testować (testowanie pionowe)⁶, co najmniej przestrzeganie mechanizmów kontrolnych. W przypadku procesów istotnych, podstawową rolę powinno odgrywać testowanie pionowe pierwszej linii obrony przez drugą linię obrony.

- 8.3. Bank powinien określić komórki organizacyjne odpowiedzialne za testowanie, w tym zwłaszcza testowanie kluczowych mechanizmów kontrolnych zapewniających osiągnięcie każdego z celów ogólnych systemu kontroli wewnętrznej, w tym:
- a) określić rolę komórki do spraw zgodności w testowaniu pionowym przestrzegania kluczowych mechanizmów kontrolnych, zapewniających osiąganie zgodności działania banku z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi,
 - b) określić rolę komórki (komórek) organizacyjnej odpowiedzialnej za zarządzanie ryzykiem w testowaniu pionowym przestrzegania mechanizmów kontrolnych zapewniających działanie mechanizmów kontroli ryzyka (np. testowanie rejestrowania przekroczeń danego limitu, testowanie przestrzegania podziału zadań przy procesie oceny zdolności kredytowej, testowanie sposobu sporządzania dokumentacji zabezpieczenia spłaty kredytu).
- 8.4. W przypadku, gdy komórki odpowiedzialne za zarządzanie ryzykiem nie dysponują odpowiednimi zasobami do realizacji zadań w zakresie testowania, bank powinien odpowiednio zwiększyć zasoby tych komórek lub przypisać te zadania, zwłaszcza w zakresie testowania pionowego, innej komórce organizacyjnej⁷ lub komórkom organizacyjnym w ramach drugiej linii obrony.
- 8.5. Bank powinien opracować i wdrożyć regulacje wewnętrzne dotyczące testowania, z odpowiednim uwzględnieniem zasad, o których mowa w rekomendacji 27 i 28, w tym w szczególności zasad dotyczących:
- a) planowania testowania oraz oceny ich wyników,
 - b) wskazywania komórek organizacyjnych odpowiedzialnych za przeprowadzenie testu, wraz z przypisanymi im uprawnieniami i obowiązkami,
 - c) zakresu testowania,
 - d) częstotliwości testowania, uzależnionej od częstotliwości badań audytowych w danym okresie, stopnia złożoności procesów funkcjonujących w banku, rodzaju kluczowych mechanizmów kontrolnych,
 - e) zasad doboru próby do testowania,

⁶ Można się spotkać z określeniem „komórka kontroli wewnętrznej” lub „komórka kontroli instytucjonalnej”.

⁷ Przykładowo wspomnianej wcześniej „komórce kontroli wewnętrznej” albo innej komórce dedykowanej do testowania pionowego.

- f) sposobu przeprowadzenia testowania,
- g) zasad sporządzania projektu raportu z wynikami testowania, jego omawiania, zatwierdzania oraz przekazywania,
- h) wymaganej dokumentacji testowania.

Rekomendacja 9

Bank powinien ustanowić matrycę funkcji kontroli oraz określić zakres zadań odnośnie zapewniania funkcjonowania matrycy.

- 9.1. W ramach matrycy funkcji kontroli bank powinien opisać powiązanie celów ogólnych systemu kontroli wewnętrznej z procesami istotnymi wraz z wpisanymi w te procesy kluczowymi mechanizmami kontrolnymi i niezależnym monitorowaniem tych mechanizmów.
- 9.2. Za dokumentowanie matrycy funkcji kontroli, w tym pozyskiwanie niezbędnych informacji o celach ogólnych systemu kontroli wewnętrznej i procesach istotnych oraz za aktualizację informacji w matrycy, powinna być odpowiedzialna wskazana komórka organizacyjna funkcjonująca w ramach drugiej linii obrony.
- 9.3. Bank powinien wskazać, w ramach komórek organizacyjnych, osoby, które są odpowiedzialne za niezwłoczne dostarczanie komórce dokumentującej matrycę funkcji kontroli, informacji dotyczących:
 - a) ustanowienia lub zmiany kluczowych mechanizmów kontrolnych,
 - b) przypisania obowiązku niezależnego monitorowania przestrzegania kluczowych mechanizmów kontrolnych lub zmiany zakresu tego obowiązku,
 - c) ustanowienia lub zmiany procesów istotnych.
- 9.4. Bank powinien uzupełniać matrycę funkcji kontroli o dodatkowe elementy wynikające z systemu kontroli wewnętrznej jego podmiotów zależnych, jeżeli mają one wpływ na zapewnianie osiągnięcia celów ogólnych systemu kontroli wewnętrznej w procesach istotnych.

Rekomendacja 10

Bank powinien określić zasady raportowania co najmniej o kluczowych mechanizmach kontrolnych oraz wynikach testowania pionowego.

- 10.1. Bank powinien ustanowić zasady okresowego, nie rzadziej niż półrocznego, raportowania co najmniej o statusie realizacji planowanych do wdrożenia kluczowych mechanizmów kontrolnych oraz o wynikach testowania pionowego przestrzegania kluczowych mechanizmów kontrolnych, obejmujące co najmniej zestawienie wykrytych nieprawidłowości znaczących i krytycznych.

10.2. Bank powinien wskazać odbiorców raportów o kluczowych mechanizmach kontrolnych i wynikach testowania pionowego, obejmującego co najmniej komórkę audytu wewnętrznego, zarząd banku i radę nadzorczą lub komitet audytu, jeżeli został powołany.

C. ZAPEWNIANIE ZGODNOŚCI

Rekomendacja 11

Bank powinien wyodrębnić zapewnianie zgodności jako jeden z czterech ogólnych celów systemu kontroli wewnętrznej. Bank powinien zapewniać zgodność poprzez funkcję kontroli oraz zarządzanie ryzykiem braku zgodności.

- 11.1. W ramach celu ogólnego systemu kontroli wewnętrznej, jakim jest zapewnianie zgodności, bank powinien odpowiednio wyodrębnić cele szczegółowe dotyczące zapewniania zgodności.
- 11.2. W ramach zapewniania zgodności, zarząd banku powinien opracować i zapewniać przestrzeganie polityki zgodności, zawierającej co najmniej:
- a) podstawowe zasady zapewniania zgodności w ramach funkcji kontroli przez wszystkich pracowników banku,
 - b) podstawowe zasady efektywnego zarządzania ryzykiem braku zgodności przez komórkę do spraw zgodności,
 - c) rodzaje działań podejmowanych w przypadku wykrycia nieprawidłowości w stosowaniu polityki zgodności, w tym środki naprawcze i dyscyplinujące,
 - d) zakres i częstotliwość informacji, o których mowa w rekomendacji 1.6a, dotyczących sposobu wypełnienia zadań odnośnie zapewniania zgodności, w tym raportów w sprawie zarządzania ryzykiem braku zgodności.
- 11.3. W ramach zapewniania zgodności, rada nadzorcza powinna:
- a) zatwierdzać politykę zgodności,
 - b) nadzorować wykonywanie obowiązków przez zarząd banku, dotyczących zapewniania zgodności zarówno w ramach funkcji kontroli, jak i zarządzania ryzykiem braku zgodności,
 - c) co najmniej raz w roku oceniać efektywność zarządzania ryzykiem braku zgodności przez bank, w oparciu o okresowe i roczne raporty komórki do spraw zgodności oraz informacje od zarządu banku.

Rekomendacja 12

Bank powinien wyodrębnić komórkę do spraw zgodności, zapewnić jej odpowiednie usytuowanie w strukturze organizacyjnej banku, określić w sposób formalny jej uprawnienia i obowiązki, jak również zapewnić niezależność oraz odpowiedni status kierującemu komórką do spraw zgodności i jej pracownikom.

- 12.1. Opracowany przez kierującego komórką do spraw zgodności oraz zatwierdzony przez zarząd banku i radę nadzorczą, regulamin funkcjonowania komórki do spraw zgodności, powinien określać co najmniej:

- a) cel i szczegółowe zasady działania komórki do spraw zgodności,
- b) usytuowanie komórki do spraw zgodności w strukturze organizacyjnej banku,
- c) ogólny zakres zadań komórki do spraw zgodności, wykonywanych w ramach funkcji kontroli,
- d) ogólny zakres zadań komórki do spraw zgodności, wykonywanych na każdym etapie zarządzania ryzykiem braku zgodności,
- e) ogólne wymogi dotyczące kwalifikacji, doświadczenia i umiejętności oraz rękopisami należytego wykonywania obowiązków przez kierującego komórką do spraw zgodności i jej pracowników, w tym znajomości języka polskiego,
- f) podstawowe prawa i obowiązki kierującego komórką do spraw zgodności oraz jej pracowników,
- g) funkcjonujące w banku mechanizmy zapewniające niezależność komórce do spraw zgodności, w szczególności w zakresie wymogów przewidzianych w przepisach prawa,
- h) sposób zapewniania środków finansowych niezbędnych do skutecznego wykonywania zadań oraz systematycznego podnoszenia kwalifikacji, zdobywania doświadczenia i umiejętności przez pracowników komórki do spraw zgodności,
- i) zasady opracowywania i zatwierdzania procedur i metodyk niezależnego monitorowania przez komórkę do spraw zgodności, w ramach funkcji kontroli,
- j) zasady opracowywania i zatwierdzania procedur i metodyk określających tryb i zasady zarządzania ryzykiem braku zgodności,
- k) zasady odpowiedniego dokumentowania czynności wykonywanych w ramach funkcji kontroli oraz zarządzania ryzykiem braku zgodności,
- l) zasady współpracy komórki do spraw zgodności z komórką (stanowiskiem) organizacyjnym do spraw prawnych, komórką (komórkami) odpowiedzialną za zarządzanie ryzykiem oraz komórką audytu wewnętrznego,
- m) zasady współpracy komórki do spraw zgodności z analogicznymi komórkami w podmiocie dominującym i podmiotach zależnych,
- n) relacje komórki do spraw zgodności z zarządem banku i radą nadzorczą oraz z komitetami zarządu banku i rady nadzorczej,
- o) zasady okresowego raportowania do zarządu banku i rady nadzorczej lub komitetu audytu, jeżeli został powołany.

12.2. Usytuowanie komórki do spraw zgodności w strukturze organizacyjnej powinno gwarantować niezależność tej komórce, a fakt ten powinien wynikać ze statutu banku. Komórka do spraw zgodności powinna podlegać bezpośrednio prezesowi banku.

12.3. Zarząd banku odpowiada za funkcjonujące w banku mechanizmy zapewniające niezależność komórce do spraw zgodności, w szczególności w zakresie wymogów przewidzianych w przepisach prawa.

- 12.4. Zarząd banku powinien zapewnić komórce do spraw zgodności środki finansowe niezbędne do skutecznego wykonywania zadań oraz systematycznego podnoszenia kwalifikacji, zdobywania doświadczenia i umiejętności przez pracowników tej komórki.
- 12.5. Zarząd banku powinien zapewnić odpowiedni status kierującemu komórką do spraw zgodności poprzez szczegółowe określenie obowiązków i uprawnień kierującego tą komórką, jak również trybu jego powoływania i odwoływania, a także wysokości wynagrodzenia. Wysokość wynagrodzenia (w tym premii) kierującego komórką do spraw zgodności, spełniająca wymogi przewidziane w przepisach prawa dotyczących polityki wynagrodzeń, powinna być zatwierdzana przez radę nadzorczą lub komitet audytu, jeżeli został powołany i nie powinna odbiegać od wynagrodzenia osób pełniących kluczowe funkcje w banku.
- 12.6. Zarząd banku powinien zapewnić kierującemu komórką do spraw zgodności oraz pracownikom tej komórki odpowiedni zakres uprawnień, obejmujący co najmniej:
- a) prawo dostępu do wszelkich niezbędnych informacji i danych (w tym poufnych i wrażliwych) oraz do pomieszczeń w zakresie koniecznym do wykonywania zadań w obecności osób odpowiedzialnych za te pomieszczenia oraz prawo dostępu do systemów informatycznych (bez możliwości ingerencji w zasoby systemu), uwzględniających informacje i dane niezbędne do wykonywania zadań,
 - b) prawo do żądania informacji i danych oraz otrzymywania niezwłocznych odpowiedzi od pracowników i komórek organizacyjnych posiadających te informacje i dane,
 - c) prawo do wglądu do wszelkich akt i dokumentów oraz sporządzania kopii, odpisów lub wyciągów oraz do dokonywania oględzin, przeliczeń, pomiarów w zakresie koniecznym do wykonywania zadań,
 - d) prawo do żądania pisemnych oraz ustnych wyjaśnień i oświadczeń oraz otrzymywania niezwłocznych odpowiedzi (bez zbędnych opóźnień) od pracowników banku, w związku z wykonywanymi zadaniami komórki do spraw zgodności,
 - e) prawo do uzyskiwania pomocy od pracowników odpowiednich komórek organizacyjnych banku w zakresie koniecznym do wykonywania zadań,
 - f) możliwość stosowania narzędzi informatycznych wspomagających realizację zadań komórki do spraw zgodności.
- 12.7. Do obowiązków kierującego komórką do spraw zgodności powinno należeć w szczególności:
- a) opracowanie regulaminu funkcjonowania komórki do spraw zgodności,
 - b) opracowanie rocznego planu zadań komórki do spraw zgodności,

- c) zatwierdzanie procedur i metodyk wykorzystywanych w procesie niezależnego monitorowania, w ramach funkcji kontroli oraz zarządzania ryzykiem braku zgodności,
 - d) zatwierdzenie wyników identyfikacji, oceny, kontroli oraz monitorowania ryzyka braku zgodności, realizowanych przez komórkę do spraw zgodności oraz przekazywanie raportów zawierających te wyniki,
 - e) opracowanie zasad okresowego raportowania do zarządu banku i rady nadzorczej lub komitetu audytu, jeżeli został powołany, zgodnie z rekomendacją 21.
- 12.8. Do obowiązków pracownika komórki do spraw zgodności powinno należeć w szczególności:
- a) przestrzeganie zasad etyki zawodowej,
 - b) przestrzeganie zasad poufności w odniesieniu do informacji pozyskiwanych w związku z wykonywaniem zadań,
 - c) wykonywanie czynności z zachowaniem niezbędnej niezależności i obiektywizmu,
 - d) odpowiednie zabezpieczanie materiałów i dokumentów uzyskanych podczas wykonywania czynności, w tym zabezpieczanie ich przed dostępem dla niepowołanych osób,
 - e) odpowiednie dokumentowanie wykonywanych czynności, umożliwiających weryfikację bieżącej realizacji zadań komórki do spraw zgodności oraz przestrzeganie zasad ich archiwizacji,
 - f) niezwłoczne informowanie przełożonych o krytycznym poziomie ryzyka braku zgodności.

Rekomendacja 13

Zapewnianie zgodności, w ramach funkcji kontroli, powinno obejmować stosowanie mechanizmów kontrolnych, niezależne monitorowanie ich przestrzegania oraz raportowanie.

- 13.1. W ramach funkcji kontroli bank powinien zapewniać zgodność, z uwzględnieniem rekomendacji, o których mowa w części B niniejszej Rekomendacji.
- 13.2. W ramach przestrzegania obowiązujących przepisów prawa, regulacji wewnętrznych i standardów rynkowych każdy z pracowników banku powinien stosować mechanizmy kontrolne i dokonywać niezależnego monitorowania przestrzegania mechanizmów kontrolnych, zgodnie z przypisanymi mu obowiązkami służbowymi.
- 13.3. Bank powinien unikać sytuacji, w której odpowiedzialność za całkowite zapewnianie zgodności ponosi jedynie komórka do spraw zgodności, tj. z pominięciem pozostałych jednostek, komórek, stanowisk organizacyjnych banku oraz pracowników banku.

W ramach funkcji kontroli komórka do spraw zgodności powinna zapewniać zgodność poprzez:

- a) weryfikację bieżącą pionową, w szczególności z uwzględnieniem rekomendacji 7, chyba że weryfikacja ta została przypisana innym komórkom, zgodnie z rekomendacją 13.5,
- b) testowanie pionowe, w sposób wskazany w rekomendacji 8.

13.4. Zakres weryfikacji bieżącej pionowej oraz testowanie pionowe, dokonywane przez komórkę do spraw zgodności, powinny być odpowiednio dostosowane do specyfiki działalności banku. Zakres weryfikacji bieżącej pionowej może obejmować w szczególności weryfikację przestrzegania mechanizmów kontrolnych (np. procedur), przez pierwszą linię obrony w takich obszarach jak:

- a) ochrona konsumentów, w tym zwłaszcza stosowania wzorów umów, pod kątem potencjalnego występowania klauzul umownych uznanych za niedozwolone,
- b) przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu oraz przestrzeganie sankcji międzynarodowych,
- c) działalność konkurencyjna pracowników banku,
- d) konflikty interesów,
- e) skargi i reklamacje,
- f) działalność banku podlegająca wymogom wynikającym z przepisów regulujących funkcjonowanie rynków instrumentów finansowych (np. wymóg klasyfikacji klientów, testów odpowiedniości i adekwatności, wymogi odnośnie odpowiedniego doradztwa inwestycyjnego),
- g) przeciwdziałanie manipulacjom rynkowym,
- h) obowiązki informacyjne względem klientów banków.

13.5. W przypadku, gdy komórce do spraw zgodności nie przypisano weryfikacji bieżącej pionowej w zakresie, o którym mowa w rekomendacji 13.4, bank powinien zapewnić, że zadania te będą realizowane przez innych pracowników lub komórki organizacyjne w ramach drugiej linii obrony.

13.6. W przypadku, gdy komórce do spraw zgodności przypisano określone zadania w ramach danych procesów funkcjonujących w banku, niebędących weryfikacją bieżącą lub testowaniem, pracownicy tej komórki mogą je wykonywać, o ile nie naruszy to ich niezależności i skuteczności odnośnie weryfikacji bieżącej lub testowania.

Rekomendacja 14

Proces zarządzania ryzykiem braku zgodności powinien obejmować identyfikację, ocenę, kontrolę, monitorowanie oraz raportowanie o ryzyku braku zgodności przez

komórkę do spraw zgodności. Bank powinien zdefiniować ryzyko braku zgodności oraz opracować odpowiednie procedury i metodyki.

- 14.1. Komórka do spraw zgodności powinna być odpowiedzialna za realizację procesu zarządzania ryzykiem braku zgodności w procesach funkcjonujących w banku. W przypadku, gdy część zadań odnośnie identyfikacji i oceny ryzyka została powierzona innym komórkom organizacyjnym banku w ramach pierwszej lub drugiej linii obrony, komórka do spraw zgodności powinna dokonywać weryfikacji identyfikacji i oceny ryzyka braku zgodności przez te komórki oraz ponosić ostateczną odpowiedzialność za realizację procesu zarządzania ryzykiem braku zgodności.
- 14.2. Bank powinien określić rodzaje negatywnych skutków, jakie może powodować nieprzestrzeganie przepisów prawa, regulacji wewnętrznych oraz standardów rynkowych, w zakresie dotyczącym działalności banku, uwzględniając zarówno potencjalne skutki finansowe, jak i niefinansowe, jakie mogą się zmaterializować w odniesieniu do tego ryzyka.
- 14.3. Zarządzanie ryzykiem braku zgodności powinno być prowadzone w oparciu o roczny plan zadań komórki do spraw zgodności oraz procedury i metodyki zarządzania tym ryzykiem. Kierujący komórką do spraw zgodności powinien opracować roczny plan zadań komórki do spraw zgodności oraz przekazywać go do opiniowania zarządowi banku oraz przedstawić do zatwierdzenia radzie nadzorczej.

Rekomendacja 15

W ramach procesu zarządzania ryzykiem braku zgodności, bank powinien identyfikować ryzyko braku zgodności. Bank powinien szczegółowo określić zakres informacji wykorzystywanych do identyfikacji ryzyka braku zgodności.

- 15.1. Komórka do spraw zgodności powinna być odpowiedzialna za identyfikację ryzyka braku zgodności, w tym powinna projektować, wprowadzać i stosować procedury i metodyki identyfikacji ryzyka braku zgodności, określając zakres i rodzaj informacji, które są niezbędne do identyfikacji tego ryzyka.
- 15.2. Do podstawowych informacji wykorzystywanych w ramach identyfikacji ryzyka, powinny należeć co najmniej:
- a) zmiany przepisów prawa, regulacji wewnętrznych i standardów rynkowych,
 - b) prowadzone w banku rejestry i dokumentacje (np. rejestr strat ryzyka operacyjnego),
 - c) informacje uzyskiwane od innych komórek organizacyjnych, w ramach wykonywania przypisanych im obowiązków, w tym zwłaszcza w ramach niezależnego monitorowania przez te komórki,

- d) ustalenia dokonane przez komórkę do spraw zgodności, w związku z bieżącą weryfikacją oraz testowaniem, wykonywanymi przez tę komórkę,
- e) wyniki wewnętrznych postępowań wyjaśniających przeprowadzanych przez komórkę do spraw zgodności lub inne komórki organizacyjne banku,
- f) nieprawidłowości zidentyfikowane przez bank w ramach wszystkich trzech linii obrony,
- g) informacje otrzymywane w ramach anonimowego kanału powiadamiania o nadużyciach oraz informacje uzyskiwane w ramach sygnałów wczesnego ostrzegania,
- h) ustalenia wynikające z czynności nadzorczych wykonywanych przez uprawnione instytucje (np. KNF) oraz czynności realizowanych przez inne upoważnione instytucje (np. Urząd Ochrony Konkurencji i Konsumentów).

Rekomendacja 16

W ramach zarządzania ryzykiem braku zgodności, bank powinien oceniać zidentyfikowane ryzyko braku zgodności poprzez pomiar ilościowy lub szacowanie jakościowe.

- 16.1. Bank powinien dokonywać zarówno całościowej oceny ryzyka braku zgodności, jak i oceny ryzyka braku zgodności dla procesów funkcjonujących w banku, w szczególności w zakresie procesów istotnych.
- 16.2. Bank powinien dokonywać oceny ryzyka braku zgodności, poprzez pomiar ilościowy lub szacowanie jakościowe. Bank powinien dokumentować ocenę ryzyka braku zgodności w formie mapy ryzyka W ramach podstawowych procedur i metod oceny ryzyka, bank powinien uwzględniać m.in.:
 - a) samoocenę ryzyka,
 - b) analizy scenariuszowe,
 - c) analizy luk regulacyjnych,
 - d) wskaźniki ryzyka braku zgodności.
- 16.3. Dokonując oceny ryzyka braku zgodności, bank powinien dokonywać co najmniej oceny prawdopodobieństwa wystąpienia poszczególnych niezgodności oraz oceniać ich potencjalne skutki, w tym finansowe i niefinansowe.
- 16.4. W ramach odpowiedzialności za ocenę ryzyka braku zgodności, komórka do spraw zgodności powinna ustalić, wprowadzić i stosować procedury i metody oceny ryzyka braku zgodności.

Rekomendacja 17

W ramach procesu zarządzania ryzykiem braku zgodności, bank powinien projektować i wprowadzać mechanizmy kontroli ryzyka braku zgodności w celu utrzymania ryzyka braku zgodności na określonym poziomie.

- 17.1. W ramach odpowiedzialności za kontrolę ryzyka braku zgodności, komórka do spraw zgodności powinna:
- a) określić rodzaje mechanizmów kontroli ryzyka braku zgodności stosowanych w banku,
 - b) wskazywać komórki organizacyjne odpowiedzialne za zaprojektowanie i wdrożenie poszczególnych rodzajów mechanizmów kontroli ryzyka braku zgodności w procesach, w których uczestniczą.
- 17.2. Komórka do spraw zgodności odpowiada za stosowanie wybranych rodzajów mechanizmów kontroli ryzyka braku zgodności, do których należą:
- a) analiza nowych produktów i usług wprowadzanych do oferty banku lub ich modyfikacja, pod kątem zgodności z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi,
 - b) wydawanie szczegółowych wytycznych przez komórkę do spraw zgodności, dotyczących określonego postępowania,
 - c) informowanie o najbardziej istotnych zmianach w przepisach prawa, regulacjach wewnętrznych i standardach rynkowych,
 - d) uczestnictwo w projektach wdrożeniowych, w kontekście zapewniania zgodności z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi (o ile nie narusza to niezależności komórki do spraw zgodności w procesie testowania),
 - e) przeprowadzanie lub zlecanie szkoleń w zakresie wskazanym przez komórkę do spraw zgodności,
 - f) określenie wskaźników ryzyka braku zgodności lub sygnałów ostrzegawczych.

Rekomendacja 18

W ramach procesu zarządzania ryzykiem braku zgodności, bank powinien monitorować wielkość i profil ryzyka braku zgodności. Bank powinien określić przy tym zakres testowania sposobu wdrożenia i przestrzegania mechanizmów kontroli ryzyka braku zgodności.

- 18.1. Bank powinien monitorować wielkość i profil ryzyka braku zgodności, uwzględniając w szczególności zmiany wielkości i profilu tego ryzyka, wynikające z zastosowanych mechanizmów kontroli ryzyka braku zgodności (np. w związku z wdrożeniem szczegółowych zaleceń komórki do spraw zgodności).
- 18.2. W ramach odpowiedzialności za monitorowanie wielkości i profilu ryzyka braku zgodności komórka do spraw zgodności powinna zaprojektować, wprowadzić

i stosować procedury i metodyki monitorowania ryzyka braku zgodności, w tym w szczególności testować sposób wdrożenia i przestrzegania mechanizmów kontroli ryzyka braku zgodności (np. testować wdrożenie szczegółowych wytycznych komórki do spraw zgodności).

- 18.3. W ramach monitorowania wielkości i profilu ryzyka braku zgodności, bank powinien wykorzystać co najmniej:
- a) informacje pozyskane w trakcie weryfikacji bieżącej pionowej oraz testowania pionowego, o których mowa w rekomendacji 13.3,
 - b) informacje pozyskane ze źródeł służących do identyfikacji ryzyka, o których mowa w rekomendacji 15.2.
- 18.4. Bank może połączyć testowanie sposobu wdrożenia i przestrzegania mechanizmów kontroli ryzyka braku zgodności z testowaniem pionowym, o którym mowa w rekomendacji 13.3b.
- 18.5. W przypadku, gdy wyniki monitorowania wielkości i profilu ryzyka braku zgodności wskazują, że sposób wdrożenia i przestrzegania mechanizmów kontroli ryzyka braku zgodności jest w ocenie komórki do spraw zgodności niewystarczający, bank powinien dokonać odpowiedniej korekty wielkości i profilu ryzyka braku zgodności.

Rekomendacja 19

W ramach zarządzania ryzykiem braku zgodności, bank powinien, co kwartał, jednocześnie raportować do zarządu banku i rady nadzorczej lub komitetu audytu, jeżeli został powołany, o wynikach identyfikacji, oceny, kontroli i monitorowania wielkości i profilu ryzyka braku zgodności.

- 19.1. Komórka do spraw zgodności powinna być odpowiedzialna za kompleksowe raportowanie wyników dotyczących:
- a) identyfikacji ryzyka braku zgodności, w tym obejmujących kluczowe zmiany w przepisach prawa, regulacjach wewnętrznych i standardach rynkowych,
 - b) oceny ryzyka braku zgodności, w tym obejmujących zestawienie ocen ryzyka braku zgodności wskazujących na wielkość i profil ryzyka braku zgodności na poziomie wysokim,
 - c) kontroli ryzyka braku zgodności, w tym obejmujących zestawienie najważniejszych rodzajów mechanizmów kontroli ryzyka braku zgodności,
 - d) monitorowania wielkości i profilu ryzyka braku zgodności, w tym obejmujących zestawienie statusów wdrożenia mechanizmów kontroli ryzyka braku zgodności oraz przypadki korekty oceny ryzyka braku zgodności oraz testowania pionowego, w przypadkach o których mowa w rekomendacji 18.4

- 19.2. Raporty powinny być przekazywane z częstotliwością kwartalną, przez kierującego komórką do spraw zgodności, zarówno zarządowi banku, jak i radzie nadzorczej lub komitetowi audytu, jeżeli został powołany. Jednocześnie, w przypadku gdy zidentyfikowana wielkość ryzyka braku zgodności jest wysoka lub krytyczna, niezbędne informacje w tym zakresie powinny być przekazywane przez komórkę do spraw zgodności niezwłocznie do zarządu banku i rady nadzorczej oraz do komórki audytu wewnętrznego.

Rekomendacja 20

Bank powinien opracować zasady współpracy komórki do spraw zgodności banku z analogicznymi komórkami podmiotu dominującego i podmiotów zależnych, jak również określić zakres dopuszczalnego korzystania z usług doradczych podmiotów zewnętrznych.

- 20.1. Zasady współpracy komórki do spraw zgodności banku, będącego podmiotem zależnym, z analogiczną komórką podmiotu dominującego powinny być określone w sformalizowanej polityce, opracowanej przez zarząd banku i zatwierdzonej przez radę nadzorczą banku, będącego podmiotem zależnym. Komórka do spraw zgodności banku, będącego podmiotem zależnym, może współpracować z analogiczną komórką podmiotu dominującego, o ile nie narusza to obowiązujących bank przepisów prawa oraz regulacji ostrożnościowych i niezależności komórki do spraw zgodności banku, będącego podmiotem zależnym, oraz jest uzasadnione interesem tego banku.
- 20.2. Zakres współpracy komórki do spraw zgodności banku, będącego podmiotem zależnym, z analogiczną komórką podmiotu dominującego powinien być wyraźnie określony i obejmować wymianę wiedzy, doświadczenia, stosowania procedur i metodyk oraz ewentualne wsparcie eksperckie. W ramach zarządzania ryzykiem braku zgodności analogiczna komórka podmiotu dominującego nie może narzucać oceny ryzyka braku zgodności, rodzajów mechanizmów kontroli ryzyka braku zgodności oraz korekty ryzyka braku zgodności, dokonywanej w ramach monitorowania ryzyka braku zgodności.
- 20.3. Zasady współpracy komórki do spraw zgodności banku z analogiczną komórką podmiotu zależnego powinny być określone w sformalizowanej polityce opracowanej przez zarząd banku i zatwierdzonej przez radę nadzorczą.
- 20.4. Bank może, w uzasadnionych przypadkach korzystać z określonych usług doradczych w ramach zarządzania ryzykiem braku zgodności, o ile ostateczna odpowiedzialność za zarządzanie ryzykiem spoczywa na komórce do spraw zgodności. W ramach

zarządzania ryzykiem braku zgodności, bank może korzystać w szczególności z takich usług doradczych, jak:

- a) dostarczanie analiz na potrzeby identyfikacji ryzyka braku zgodności,
- b) wsparcie w zakresie opracowywania procedur i metodyk dotyczących zarządzania ryzykiem braku zgodności,
- c) wsparcie w zakresie niektórych mechanizmów kontroli ryzyka braku zgodności (np. organizacja szkoleń lub przygotowywanie opinii prawnych przez wyspecjalizowane podmioty zewnętrzne).

Rekomendacja 21

Bank powinien opracować zasady raportowania przez komórkę do spraw zgodności, odnośnie realizacji jej zadań, do zarządu banku i rady nadzorczej.

21.1. Kierujący komórką do spraw zgodności powinien opracować, a zarząd banku i rada nadzorcza powinny zatwierdzić zasady rocznego i jednoczesnego raportowania przez komórkę do spraw zgodności do zarządu banku i rady nadzorczej lub komitetu audytu, jeżeli został powołany, odnośnie realizacji zadań tej komórki, obejmującego co najmniej:

- a) sprawozdanie z realizacji zadań komórki do spraw zgodności,
- b) zestawienie wyników testowania przestrzegania kluczowych mechanizmów kontrolnych, w oparciu o informacje, o których mowa w rekomendacji 10.1,
- c) wyniki identyfikacji, oceny, monitorowania i kontroli ryzyka braku zgodności, w oparciu o informacje, o których mowa w rekomendacji 19.1,
- d) sposób zapewnienia niezależności komórce do spraw zgodności i jej pracownikom,
- e) informacje o zapewnieniu środków finansowych niezbędnych do skutecznego wykonywania zadań przez komórkę do spraw zgodności,
- f) zakres współpracy komórki do spraw zgodności banku z analogiczną komórką podmiotu dominującego i podmiotów zależnych.

D. AUDYT WEWNĘTRZNY

Rekomendacja 22

Bank powinien wyodrębnić niezależną komórkę audytu wewnętrznego i przypisać jej zadania wykonywane w ramach działalności zapewniającej oraz działalności doradczej.

- 22.1. W ramach działalności zapewniającej komórka audytu wewnętrznego powinna być odpowiedzialna za dokonanie oceny adekwatności i skuteczności systemu zarządzania, w tym w szczególności systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, poprzez przeprowadzanie badań audytowych ujętych w ramach zdefiniowanego przez bank procesu audytowego. Na proces audytowy składać się powinny co najmniej:
- a) plany audytu,
 - b) przygotowanie badania audytowego,
 - c) przeprowadzenie badania audytowego, z uwzględnieniem raportowania jego wyników,
 - d) monitorowanie efektywności realizacji zaleceń poaudytowych.
- 22.2. W odniesieniu do systemu zarządzania ryzykiem, proces audytowy powinien obejmować ocenę adekwatności i skuteczności systemu zarządzania ryzykiem, odpowiednio na pierwszej i drugiej linii obrony, z uwzględnieniem adekwatności i skuteczności mechanizmów kontroli ryzyka stosowanych w ramach tych linii. W odniesieniu do systemu kontroli wewnętrznej, proces audytowy powinien obejmować ocenę adekwatności i skuteczności systemu kontroli wewnętrznej, odpowiednio na pierwszej i drugiej linii obrony, z uwzględnieniem adekwatności i skuteczności mechanizmów kontrolnych i niezależnego monitorowania ich przestrzegania w ramach tych linii.
- 22.3. Komórka audytu wewnętrznego powinna dostosować zakres badań audytowych systemu kontroli wewnętrznej do wyników, skuteczności i adekwatności weryfikacji bieżącej i testowania przestrzegania mechanizmów kontrolnych przez komórki organizacyjne w ramach pierwszej i drugiej linii obrony.
- 22.4. W ramach działalności doradczej komórka audytu wewnętrznego może przysparzać wartości i usprawnień w odniesieniu do działalności banku, o ile działalność taka nie zagraża niezależności, efektywności i obiektywizmowi działalności zapewniającej oraz:
- a) podejmowana jest na wniosek zarządu banku, rady nadzorczej, komitetu audytu lub komitetu do spraw ryzyka,
 - b) podejmowana jest w odniesieniu do kluczowych, z punktu widzenia banku, rozwiązań o charakterze systemowym,

- c) nie obejmuje projektowania, opiniowania i zatwierdzania procedur i metodyk stosowanych w banku,
 - d) skutkuje jedynie niewiążącymi rekomendacjami wydawanymi przez komórkę audytu wewnętrznego,
 - e) podejmowana jest z uwzględnieniem zasobów mieszczących się w limitach działalności doradczej, określonych przez bank dla komórki audytu, zgodnie z którymi działalność doradcza powinna mieć charakter działalności wyjątkowej.
- 22.5. W przypadku, gdy pracownik komórki audytu wewnętrznego wykonywał działalność doradczą odnośnie danego rozwiązania, co najmniej przez rok nie powinien on wykonywać działalności zapewniającej w zakresie, który był przedmiotem jego działalności doradczej.

Rekomendacja 23

Bank powinien zapewnić odpowiednie usytuowanie komórki audytu wewnętrznego w strukturze organizacyjnej banku, określić w sposób formalny jej uprawnienia i obowiązki, jak również zapewnić niezależność, obiektywizm oraz odpowiedni status kierującemu komórką audytu wewnętrznego i audytorom wewnętrznym.

- 23.1. Opracowana przez kierującego komórką audytu wewnętrznego i zatwierdzona przez zarząd banku oraz radę nadzorczą karta audytu powinna określać co najmniej:
- a) misję i cele komórki audytu wewnętrznego oraz zasady opracowywania strategii działalności komórki audytu wewnętrznego,
 - b) usytuowanie komórki audytu wewnętrznego w strukturze organizacyjnej banku,
 - c) zakres zadań komórki audytu wewnętrznego, wykonywanych w ramach działalności zapewniającej oraz działalności doradczej,
 - d) ogólne wymogi dotyczące kwalifikacji, doświadczenia i umiejętności oraz rękojmi należytego wykonywania obowiązków przez kierującego komórką audytu wewnętrznego i audytorów wewnętrznych, w tym znajomości języka polskiego,
 - e) podstawowe prawa i obowiązki kierującego komórką audytu wewnętrznego, kierującego badaniem audytowym oraz audytorów wewnętrznych,
 - f) funkcjonujące w banku mechanizmy zapewniające niezależność komórce audytu wewnętrznego, w szczególności w zakresie wymogów przewidzianych w przepisach prawa,
 - g) sposób zapewniania środków finansowych niezbędnych do skutecznego wykonywania zadań oraz systematycznego podnoszenia kwalifikacji, zdobywania doświadczenia i umiejętności przez audytorów wewnętrznych,

- h) minimalną liczbę audytorów wewnętrznych posiadających stosowne certyfikaty zawodowe, w relacji do wszystkich pracowników komórki audytu wewnętrznego (np. *Certified Internal Auditor* – certyfikat audytora wewnętrznego),
- i) minimalną relację liczby pracowników zatrudnionych (etatów) w komórce audytu wewnętrznego do liczby wszystkich pracowników banku,
- j) zasady opracowywania i zatwierdzania planów audytu, raportów z badania audytowego oraz procedur i metodyk badania audytowego,
- k) opis wszystkich etapów procesu audytowego,
- l) zasady przeprowadzania badań audytowych nieprzewidzianych w planach audytu (tj. audytów doraźnych),
- m) zasady współpracy komórki audytu wewnętrznego z komórką (stanowiskiem) organizacyjnym do spraw prawnych oraz komórką do spraw zgodności i komórką (komórkami) odpowiedzialną za zarządzanie ryzykiem,
- n) zasady współpracy komórki audytu wewnętrznego z analogiczną komórką podmiotu dominującego i podmiotów zależnych oraz z biegłym rewidentem,
- o) relacje komórki audytu wewnętrznego z zarządem banku i radą nadzorczą oraz z komitetami zarządu banku i rady nadzorczej,
- p) zasady etyki zawodowej,
- q) zasady zapewniania jakości działalności zapewniającej i doradczej komórki audytu wewnętrznego,
- r) zasady okresowego i jednoczesnego raportowania do zarządu banku i rady nadzorczej lub komitetu audytu, jeżeli został powołany.

23.2. Działalność komórki audytu wewnętrznego powinna wynikać z, opracowanej przez kierującego tą komórką, długofalowej strategii jej działalności, obejmującej co najmniej wizję funkcjonowania komórki w określonym przedziale czasowym, jej model organizacyjny (struktura organizacyjna uwzględniająca strukturę organizacyjną banku, odpowiednia liczba audytorów), program rozwoju pracowników, planowane do wdrożenia narzędzia informatyczne oraz relacje banku z analogicznymi komórkami podmiotu dominującego i podmiotów zależnych oraz z biegłym rewidentem. Strategia działalności komórki audytu wewnętrznego powinna być opiniowana przez zarząd banku i zatwierdzana przez radę nadzorczą.

23.3. Usytuowanie komórki audytu wewnętrznego w strukturze organizacyjnej powinno gwarantować niezależność komórki audytu wewnętrznego, a fakt ten powinien wynikać ze statutu banku. Komórka audytu wewnętrznego powinna podlegać organizacyjnie prezesowi zarządu banku. Stanowisko kierującego komórką audytu wewnętrznego powinno być usytuowane na poziomie bezpośrednio poniżej poziomu zarządu banku (np. poziom dyrektora zarządzającego w banku, o ile takie stanowisko zostało ustanowione).

- 23.4. Zarząd banku odpowiada za funkcjonujące w banku mechanizmy zapewniające niezależność komórce audytu, w szczególności w zakresie wymogów przewidzianych w przepisach prawa. Pracownicy komórki audytu wewnętrznego nie powinni wykonywać żadnych innych czynności w banku poza tymi, które wynikają z działalności zapewniającej lub doradczej, w tym zwłaszcza nie powinni wykonywać żadnych czynności operacyjnych.
- 23.5. Zarząd banku odpowiada za zapewnianie warunków do obiektywnego wykonywania zadań przez kierującego komórką audytu wewnętrznego, kierującego badaniem audytowym oraz audytorów wewnętrznych, w szczególności poprzez:
- a) określenie zasad wyłączania kierującego badaniem audytowym i audytorów wewnętrznych z wykonywania zadań, w przypadku konfliktu interesów, w tym zwłaszcza w przypadku występowania powiązań o charakterze personalnym, z pracownikami jednostek audytowanych,
 - b) określenie zasad ponownej realizacji badania audytowego w przypadku uznania, że w toku procesu audytowego kierujący badaniem audytowym lub audytor wewnętrzny nie zachował niezależności i nie kierował się zasadami bezstronności,
 - c) określenie minimalnego okresu, w którym kierujący badaniem audytowym lub audytor wewnętrzny nie może wykonywać badania audytowego, w związku z realizacją przez niego – w czasie, gdy był wcześniej zatrudniony w jednostce audytowanej – zadań podlegających badaniu audytowemu.
- 23.6. Audytorzy wewnętrzni, wykonując przypisane im zadania, powinni zachowywać niezależność i kierować się bezstronnością, poprzez stosowanie zasad należytej staranności i sceptycznego osądu. W szczególności nie powinni się zgadzać na stosowanie rozwiązań i kompromisów, które mogłyby mieć negatywny wpływ na jakość ich pracy, jak również powinni wyłączać się z wykonywania zadań w przypadku występowania powiązań personalnych z pracownikami jednostek audytowych.
- 23.7. Zarząd banku powinien zapewniać odpowiedni status kierującemu komórką audytu wewnętrznego poprzez szczegółowe określenie obowiązków i uprawnień kierującego tą komórką, jak również trybu jego powoływania i odwoływania, a także wysokości wynagrodzenia. Wysokość wynagrodzenia (w tym premii) kierującego komórką audytu wewnętrznego, spełniająca wymogi przewidziane w przepisach prawa dotyczących polityki wynagrodzeń, powinna być zatwierdzana przez radę nadzorczą lub komitet audytu, jeżeli został powołany i nie powinna odbiegać od wynagrodzenia osób pełniących kluczowe funkcje w banku.
- 23.8. Zarząd banku powinien zapewniać odpowiedni status audytorom wewnętrznym, poprzez określenie:

- a) zasad transferu pracowników z innych komórek organizacyjnych banku do komórki audytu wewnętrznego,
- b) zasad doskonalenia kwalifikacji, zdobywania doświadczenia i umiejętności zawodowych przez audytorów wewnętrznych, w tym poprzez ustalanie indywidualnych programów rozwoju oraz określanie wymaganej, minimalnej liczby audytorów wewnętrznych posiadających stosowne certyfikaty zawodowe, w relacji do wszystkich pracowników komórki audytu wewnętrznego (np. *Certified Internal Auditor* – certyfikat audytora wewnętrznego),
- c) zasad okresowej oceny pracy audytorów wewnętrznych, na której wynik nie powinni mieć wpływu pracownicy jednostek audytowanych.

23.9. Zarząd banku powinien zapewniać komórce audytu wewnętrznego środki finansowe niezbędne do skutecznego wykonywania zadań, jak również systematycznego podnoszenia kwalifikacji oraz zdobywania doświadczenia i umiejętności przez audytorów wewnętrznych. Zarząd banku powinien określić co najmniej:

- a) minimalną relację liczby pracowników zatrudnionych (etatów) w komórce audytu wewnętrznego do liczby wszystkich pracowników banku,
- b) wysokość przeciętnego wynagrodzenia audytorów wewnętrznych, umożliwiającego zatrudnianie wysoko wykwalifikowanych specjalistów oraz zasady i kryteria przyznawania im premii, która nie powinna być uzależniona od wyników finansowych uzyskiwanych w jednostkach przez nich audytowanych.

Rekomendacja 24

Bank powinien szczegółowo określić prawa i obowiązki kierującego komórką audytu wewnętrznego, kierującego badaniem audytowym oraz audytorów wewnętrznych, zwłaszcza w odniesieniu do procesu audytowego, a także opracować szczegółowe procedury i metodyki badania audytowego.

24.1. Zarząd banku powinien zapewnić kierującemu komórką audytu wewnętrznego, kierującemu badaniem audytowym oraz audytorom wewnętrznym, odpowiedni zakres uprawnień, obejmujący co najmniej:

- a) prawo do uczestnictwa w, wybranych przez kierującego komórką audytu wewnętrznego, posiedzeniach komitetów powołanych przez zarząd banku,
- b) prawo dostępu do wszelkich niezbędnych informacji i danych (w tym poufnych i wrażliwych) oraz do pomieszczeń, w zakresie koniecznym do wykonywania zadań w obecności osób odpowiedzialnych za te pomieszczenia oraz prawo dostępu do systemów informatycznych (bez możliwości ingerencji w zasoby systemu), uwzględniających informacje i dane niezbędne do wykonywania zadań,

- c) prawo do przeprowadzania obserwacji oraz asystowania przy wszelkich czynnościach wykonywanych w jednostce audytowanej,
- d) prawo do żądania informacji i danych oraz otrzymywania niezwłocznych odpowiedzi od pracowników i komórek organizacyjnych posiadających te informacje,
- e) prawo do wglądu do wszelkich akt i dokumentów oraz sporządzania kopii, odpisów lub wyciągów oraz dokonywania oględzin, przeliczeń i pomiarów w zakresie koniecznym do wykonywania zadań,
- f) prawo do żądania pisemnych oraz ustnych wyjaśnień i oświadczeń oraz otrzymywania niezwłocznych odpowiedzi od pracowników jednostek audytowanych,
- g) prawo do uzyskiwania pomocy od pracowników jednostek audytowanych, w zakresie koniecznym do wykonywania zadań,
- h) możliwość stosowania narzędzi informatycznych, dostosowanych do specyfiki działalności banku, stopnia złożoności procesów funkcjonujących w banku oraz potrzeb badań audytowych,
- i) prawo do uzyskiwania pomocy od ekspertów zewnętrznych, zgodnie z regulacją wewnętrzną opracowaną w banku.

24.2. Do obowiązków kierującego komórką audytu wewnętrznego, powinno należeć w szczególności:

- a) przygotowanie strategii działalności komórki audytu,
- b) opracowanie karty audytu,
- c) przygotowywanie planów audytu,
- d) opracowywanie zasad corocznej aktualizacji uniwersum audytu oraz mapy ryzyka,
- e) zatwierdzanie wyników analizy ryzyka o której mowa w rekomendacji 25.2,
- f) zatwierdzanie programu, w tym harmonogramu badania audytowego oraz istotnych odstępstw od wykonania programu lub harmonogramu badania audytowego,
- g) zatwierdzanie przypisania audytorów wewnętrznych do poszczególnych badań audytowych, weryfikacja ich niezależności i obiektywizmu oraz – w zależności od wyników tej weryfikacji – podejmowanie decyzji o ewentualnym wyłączeniu audytora wewnętrznego z badania audytowego,
- h) pisemnie informowanie kierującego jednostką audytowaną o zamiarze przeprowadzenia badania audytowego, zgodnie z rekomendacją 27.1,
- i) podejmowanie decyzji w sprawie wydłużenia terminu badania audytowego,
- j) zatwierdzanie raportu z badania audytowego, zgodnie z rekomendacją 27.9,
- k) zatwierdzanie nowego terminu realizacji zaleceń poaudytowych, zgodnie z rekomendacją 28.5,

- l) zapewnianie jakości funkcjonowania komórki audytu wewnętrznego,
 - m) opracowywanie zasad okresowego i jednoczesnego raportowania do zarządu banku i rady nadzorczej lub komitetu audytu, jeżeli został powołany zgodnie z rekomendacją 31.
- 24.3. Do obowiązków kierującego badaniem audytowym. powinno należeć w szczególności:
- a) opracowywanie programu badania audytowego, w tym harmonogramu badania audytowego,
 - b) sprawowanie nadzoru nad wykonywaniem zadań przez audytorów wewnętrznych w ramach badania audytowego,
 - c) przygotowywanie projektu raportu z badania audytowego.
- 24.4. Do obowiązków audytora wewnętrznego uczestniczącego w badaniu powinno należeć w szczególności:
- b) przestrzeganie zasad etyki obowiązujących audytorów wewnętrznych (np. kodeksu etyki wydane go przez Instytut Audytorów Wewnętrznych),
 - c) przestrzeganie zasad poufności, w odniesieniu do informacji pozyskiwanych w związku z wykonywaniem zadań,
 - d) przeprowadzenie badania audytowego z zachowaniem niezbędnej niezależności i obiektywizmu,
 - e) odpowiednie zabezpieczanie materiałów i dokumentów uzyskanych podczas badania audytowego, w tym zabezpieczanie ich przed dostępem ze strony osób niepowołanych,
 - f) odpowiednie dokumentowanie badania audytowego, w tym sporządzanie dokumentacji roboczej, umożliwiającej weryfikację bieżącą realizacji badań przez audytora oraz przestrzeganie zasad ich archiwizacji,
 - g) niezwłoczne informowanie przełożonych o nieprawidłowościach krytycznych oraz występujących trudnościach podczas badania audytowego, mogących mieć wpływ na terminowość lub jakość badania.
- 24.5. Bank powinien opracować szczegółowe procedury i metodyki badania audytowego, dostosowane do konkretnych zadań, które ma wykonywać komórka audytu wewnętrznego i zasobów, jakimi ona dysponuje. Procedury i metodyki badania audytowego powinny obejmować co najmniej:
- a) szczegółowy sposób postępowania na każdym etapie procesu badania audytowego,
 - b) sposób i zakres badania wybranych obiektów audytowych (np. metodyka badania procesu sprawozdawczości finansowej, metodyka badania obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego),
 - c) metody i techniki audytowe (np. metody doboru próby),
 - d) sposób wykorzystania technologii i narzędzi informatycznych w ramach badania audytowego,

- e) sposób uwzględniania w badaniu matrycy funkcji kontroli,
- f) sposób wyznaczania zespołu audytorów wewnętrznych,
- g) wzory formularzy, dokumentacji roboczej oraz wzór raportu z badania audytowego.
- h) zasady sporządzania, archiwizacji i wglądu do raportów oraz dokumentacji roboczej.

Rekomendacja 25

W ramach procesu audytowego bank powinien stosować plany audytu, których przygotowywanie i zatwierdzanie powinno być poprzedzone analizą poziomu ryzyka wynikającego z działalności prowadzonej przez bank.

- 25.1. Zakres i częstotliwość badań audytowych w danym okresie, powinna wynikać ze strategicznego (długoterminowego) oraz opartego na nim operacyjnego (rocznego) planu badań audytowych. Kierujący audytem wewnętrznym powinien opracować plany audytu w oparciu o uniwersum audytu oraz mapę ryzyka. Uniwersum audytu oraz mapa ryzyka powinny podlegać corocznej aktualizacji.
- 25.2. Komórka audytu wewnętrznego powinna dokonywać analizy (identyfikacji i oceny) poziomu ryzyka zaistnienia nieprawidłowości we wszystkich obszarach działalności banku. Analiza poziomu ryzyka, w tym zidentyfikowane obszary ryzyka i poziom ich istotności, powinna być zatwierdzana przez kierującego komórką audytu wewnętrznego i dokumentowana w formie mapy ryzyka. Identyfikacja i ocena poziomu ryzyka na potrzeby planów działalności zapewniającej powinna obejmować co najmniej:
- a) przyjętą przez bank strategię działalności oraz strategię zarządzania ryzykiem, jak również wynikający z tych strategii model biznesowy banku oraz apetyt na ryzyko,
 - b) obowiązujące przepisy prawa i standardy rynkowe oraz zidentyfikowane zmiany w tym zakresie, które są planowane do wdrożenia w najbliższym czasie,
 - c) informacje uzyskane w trakcie badań audytowych, w tym nieprawidłowości znaczące i krytyczne zidentyfikowane podczas wcześniejszych badań audytowych,
 - d) stopień i terminowość realizacji zaleceń poaudytowych przez jednostki audytowane,
 - e) wielkość i profil poszczególnych rodzajów ryzyka w banku, w tym zwłaszcza ryzyka operacyjnego,
 - f) informacje uzyskane przez komórkę audytu wewnętrznego w ramach uczestnictwa w komitetach banku powołanych przez zarząd,
 - g) wprowadzenie lub planowane wprowadzenie zmian w strukturze organizacyjnej, nowych procesów w działalności banku, w tym zwłaszcza procesów istotnych lub znacznej modyfikacji dotychczas funkcjonujących procesów,

- h) wprowadzenie lub planowane wprowadzenie nowych produktów lub usług do oferty banku lub ich znacznej modyfikacji, w szczególności w odniesieniu do produktów lub usług istotnych z punktu widzenia jego działalności i wyników finansowych,
- i) sygnały ostrzegawcze i anonimowe powiadomienia o nadużyciach,
- j) informacje przekazywane przez jednostki, komórki, stanowiska organizacyjne banku usytuowane w ramach pierwszej i drugiej linii obrony, zgodnie z rekomendacją 3.2,
- k) informacje wynikające z regularnych przeglądów szacowania kapitału wewnętrznego i zarządzania kapitałowego,
- l) informacje uzyskiwane od podmiotu dominującego lub podmiotów zależnych,
- m) ustalenia wynikające z badań przeprowadzanych przez audytora zewnętrznego, w tym zwłaszcza biegłego rewidenta,
- n) ustalenia wynikające z czynności wykonywanych w ramach nadzoru sprawowanego przez upoważnione do tego podmioty (np. wyniki inspekcji lub procesu badania i oceny nadzorczej przeprowadzanych przez KNF),
- o) zmiany w otoczeniu gospodarczym banku.

25.3. Opracowując strategiczny (długoterminowy) i operacyjny (roczny) plan badań audytowych oraz dokonując zmiany tych planów, kierujący komórką audytu wewnętrznego powinien ponadto uwzględnić co najmniej:

- a) misję, strategię i cele komórki audytu wewnętrznego,
- b) sugestie i wskazania zarządu banku (lub jego członków), rady nadzorczej, komitetu audytu, jeżeli został powołany oraz komitetu do spraw ryzyka,
- c) zalecenia instytucji wykonujących czynności nadzorcze (np. KNF),
- d) zasoby kadrowe komórki audytu wewnętrznego oraz rezerwy czasowe na wykonanie zadań dotyczących monitorowania efektywności realizacji zaleceń poaudytowych,
- e) dostępne narzędzia informatyczne, dostosowane do specyfiki działalności banku, stopnia złożoności procesów funkcjonujących w banku oraz potrzeb badań audytowych,
- f) istotne zmiany elementów wchodzących w skład uniwersum audytu lub matrycy funkcji kontroli.

25.4. W ramach strategicznego (długoterminowego) planu badań audytowych kierujący komórką audytu wewnętrznego powinien wskazać minimalną częstotliwość obejmowania badaniem audytowym wszystkich obiektów audytowych z uniwersum audytu.

- 25.5. W przypadku pojawienia się nowych, istotnych okoliczności, w tym zwłaszcza istotnych zmian w uniwersum audytu lub mapie ryzyka, plany audytu powinny być odpowiednio aktualizowane.
- 25.6. Strategiczny (długoterminowy) i operacyjny (roczny) plan badań audytowych oraz ich zmiany, powinny być przekazywane do opiniowania zarządowi banku oraz przedstawiane do zatwierdzenia radzie nadzorczej.
- 25.7. Kierujący komórką audytu wewnętrznego powinien regularnie, nie rzadziej niż raz na pół roku, informować zarząd banku i radę nadzorczą lub komitet audytu, jeżeli został powołany o statusie realizacji operacyjnego (rocznego) planu badań audytowych.

Rekomendacja 26

W ramach procesu audytowego audytorzy wewnętrzni powinni z należytą starannością przygotować się do badania audytowego. Kierujący badaniem audytowym powinien opracować program badania audytowego.

- 26.1. Przed rozpoczęciem badania audytowego, kierujący tym badaniem powinien przygotować program badania audytowego, który powinien być zatwierdzony przez kierującego komórką audytu wewnętrznego. Program badania audytowego powinien obejmować co najmniej:
- a) opis celu, zakresu i okresu objętego badaniem audytowym, w tym szczegółową listę zagadnień do badania,
 - b) dostępne zasoby, w tym skład zespołu audytorów wewnętrznych, mających przeprowadzić badanie, wraz z przypisanymi im zadaniami, zapewniający odpowiednią wydajność pracy oraz jakość badania audytowego,
 - c) podstawowe informacje i dokumenty, które mają być wykorzystane w badaniu audytowym,
 - d) opis badanych obiektów audytowych, w tym informacje znajdujące się w matrycy funkcji kontroli,
 - e) wstępną analizę ryzyka zaistnienia nieprawidłowości w danym obiekcie audytowym,
 - f) syntetyczny opis systemów informatycznych wykorzystywanych w ramach procesów realizowanych w obiekcie audytowym,
 - g) harmonogram badania audytowego, określający sekwencję i ramy czasowe zadań realizowanych w toku badania audytowego,
 - h) wskazanie szczegółowych procedur i metodyk badania audytowego, w tym zwłaszcza metod i techniki badania audytowego, planowanych do zastosowania w ramach badania audytowego.

- 26.2. Audytorzy wewnętrzni powinni mieć zapewniony odpowiedni czas na przygotowanie się do badania audytowego, w tym na analizę informacji odnośnie jednostek audytowanych.

Rekomendacja 27

W ramach procesu audytowego audytorzy wewnętrzni powinni w sposób niezależny i obiektywny przeprowadzić badanie audytowe, które powinno być zakończone sporządzeniem raportu.

- 27.1. Przed rozpoczęciem badania audytowego, kierujący komórką audytu wewnętrznego powinien odpowiednio wcześniej i zgodnie z kartą audytu, pisemnie poinformować kierującego daną jednostką audytowaną o zamiarze przeprowadzenia badania, wskazując planowany termin oraz zakres badania audytowego. W wyjątkowych przypadkach, określonych przez bank, komórka audytu wewnętrznego może odstąpić od pisemnego informowania kierującego daną jednostką audytowaną o zamiarze przeprowadzenia badania.
- 27.2. Badanie audytowe powinno zostać przeprowadzone w jednostce audytowanej, w godzinach pracy oraz powinno być zrealizowane w terminie nie dłuższym niż 3 miesiące od momentu pisemnego poinformowania o zamiarze przeprowadzenia badania audytowego do momentu zatwierdzenia raportu z badania audytowego. W uzasadnionych przypadkach, godziny i termin badania mogą zostać wydłużone przez kierującego komórką audytu wewnętrznego.
- 27.3. Badanie audytowe powinno zostać przeprowadzone na podstawie karty audytu, strategicznego (długoterminowego) i operacyjnego (rocznego) planu badania audytowego, programu i harmonogramu badania audytowego oraz procedur i metodyk audytu wewnętrznego. Wszelkie istotne zmiany i odstępstwa od wykonania programu i harmonogramu badania audytowego powinny być zatwierdzane przez kierującego komórką audytu wewnętrznego.
- 27.4. Kierujący jednostką audytowaną powinien zapewnić audytorom wewnętrznym odpowiednie warunki do przeprowadzenia badania oraz udzielać niezbędnej pomocy technicznej i organizacyjnej.
- 27.5. Rozbieżności dotyczące faktów stwierdzonych w trakcie przeprowadzania badania, powinny być na bieżąco omawiane z pracownikami jednostki audytowanej. Audytorzy wewnętrzni powinni na bieżąco informować kierującego komórką audytu wewnętrznego o wykrytych nieprawidłowościach, w tym w szczególności o nieprawidłowościach znaczących i krytycznych z punktu widzenia bezpieczeństwa i stabilności działania banku. Kierujący komórką audytu wewnętrznego powinien

niezwłocznie analizować pozyskane informacje, a w przypadku nieprawidłowości krytycznych, poinformować o tym zarząd banku i radę nadzorczą lub komitet audytu, jeżeli został powołany.

- 27.6. Każde z badań audytowych powinno być dokumentowane zgodnie ze szczegółowymi zasadami dokumentacji roboczej, opracowanymi przez bank.
- 27.7. Każde z badań audytowych powinno być dokumentowane w formie pisemnego raportu z badania audytowego. Bank powinien określić szczegółowy sposób opracowywania raportu (w tym jego zawartość i formę), termin przygotowania i przekazania raportu oraz jego odbiorców, jak również określić wykaz dokumentacji załączanej do raportu. Raport z badania audytowego powinien zawierać co najmniej:
- a) opis badania audytowego, w tym jego cel, termin i zakres,
 - b) ocenę adekwatności i skuteczności systemu zarządzania ryzykiem i systemu kontroli wewnętrznej,
 - c) ustalenia badania audytowego, wraz z wykrytymi nieprawidłowościami i ich kategoryzacją,
 - d) zalecenia poaudytowe wraz ze wskazanymi adresatami oraz terminami realizacji zaleceń.
- 27.8. Treść i termin realizacji zaleceń poaudytowych powinny być dostosowane do skali i charakteru ustaleń z badania audytowego, kategoryzacji wykrytych nieprawidłowości oraz oceny adekwatności oraz skuteczności systemu zarządzania ryzykiem i systemu kontroli wewnętrznej. Zalecenia poaudytowe powinny wskazywać co najmniej:
- a) szczegółowy opis planowanych działań naprawczych lub dyscyplinujących,
 - b) jednostki, komórki lub stanowiska organizacyjne banku, które mają być zaangażowane w realizację zaleceń, w tym komórkę wiodącą/ koordynującą, jeżeli zalecenie dotyczy jednocześnie kilku komórek lub jednostek,
 - c) członka zarządu banku nadzorującego obszar działalności banku, którego dotyczy zalecenie,
 - d) termin realizacji zaleceń poaudytowych.
- 27.9. Przygotowany przez kierującego badaniem audytowym, projekt raportu z badania audytowego, powinien zostać omówiony z kierującymi jednostkami audytowanymi, a w przypadkach zidentyfikowania nieprawidłowości znaczących i krytycznych, również z członkami zarządu banku nadzorującymi obszar działalności banku, którego dotyczy badanie audytowe, a następnie zatwierdzony przez kierującego komórką audytu wewnętrznego. Bank powinien posiadać procedury uzgadniania treści raportu z badania audytowego. Przedmiotem uzgadniania treści raportu z badania audytowego nie powinna być kategoryzacja nieprawidłowości oraz ocena adekwatności i skuteczności systemu zarządzania ryzykiem i systemu kontroli wewnętrznej w jednostce audytowanej. W przypadku rozbieżności, co do treści raportu z badania

audytowego, kierujący badaniem audytowym sporządza protokół rozbieżności, i załącza go do raportu z badania audytowego (protokół rozbieżności zawiera stanowiska komórki audytu wewnętrznego i kierujących jednostkami audytowanymi). Ostateczna decyzja co do treści raportu jest podejmowana przez kierującego komórką audytu wewnętrznego, a rozbieżności co do treści raportu z badania audytowego, nie powinny wstrzymywać możliwości zatwierdzenia raportu przez kierującego komórką audytu wewnętrznego.

27.10. Zatwierdzony raport z badania audytowego powinien zostać niezwłocznie przekazany do wszystkich niezbędnych odbiorców, z uwzględnieniem co najmniej kierujących jednostkami audytowanymi, prezesa zarządu banku, członków zarządu banku nadzorujących obszar działalności banku, którego dotyczy zalecenie poaudytowe, rady nadzorczej lub komitetu audytu, jeżeli został powołany.

Rekomendacja 28

W ramach procesu audytowego komórka audytu wewnętrznego powinna monitorować efektywność realizacji zaleceń poaudytowych.

28.1. Komórka audytu wewnętrznego powinna regularnie monitorować efektywność realizacji zaleceń poaudytowych, które może być prowadzone w formie:

- a) weryfikacji realizacji zaleceń poaudytowych, bez przeprowadzania dedykowanego badania audytowego,
- b) przeprowadzania dedykowanego badania audytowego mającego na celu weryfikację realizacji zaleceń poaudytowych,
- c) weryfikacji realizacji zaleceń poaudytowych w trakcie kolejnego badania audytowego.

28.2. Dobór formy monitorowania efektywności realizacji zaleceń poaudytowych powinien zależeć od kategoryzacji nieprawidłowości, będących podstawą wydanych zaleceń oraz zakresu i złożoności działań niezbędnych do wykonania, mających za zadanie realizację tych zaleceń.

28.3. Realizacja zaleceń poaudytowych powinna być regularnie raportowana do komórki audytu wewnętrznego.

28.4. Komórka audytu wewnętrznego powinna regularnie (nie rzadziej niż raz na kwartał) przekazywać informacje o efektywności realizacji zaleceń poaudytowych do prezesa zarządu banku, członka zarządu banku nadzorującego obszar działalności banku, którego dotyczy zalecenie, rady nadzorczej lub komitetu audytu, jeżeli został powołany.

28.5. W przypadku przekroczenia ustalonego terminu realizacji zalecenia poaudytowego, kierujący jednostką audytowaną proponuje nowy termin realizacji zalecenia poaudytowego, który jest akceptowany przez członka zarządu banku nadzorującego obszar działalności banku, którego dotyczy zalecenie oraz zatwierdzany przez kierującego komórką audytu wewnętrznego. O wyznaczeniu nowego terminu, kierujący komórką audytu wewnętrznego powinien poinformować prezesa zarządu banku i radę nadzorczą lub komitet audytu, jeżeli został powołany.

Rekomendacja 29

Bank powinien opracować zasady współpracy komórki audytu wewnętrznego banku z analogicznymi komórkami podmiotu dominującego i podmiotów zależnych oraz z biegłym rewidentem.

29.1. Zasady współpracy komórki audytu wewnętrznego z biegłym rewidentem, powinny być określone w sformalizowanej polityce opracowanej przez zarząd banku i zatwierdzonej przez radę nadzorczą. Zasady współpracy powinny określać zakres i charakter współpracy w toku procesu badania sprawozdania finansowego lub badania skonsolidowanego sprawozdania finansowego, w szczególności poprzez:

- a) omówienie z biegłym rewidentem, na odpowiednio wczesnym etapie badania, systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, w tym w szczególności roli funkcji kontroli na pierwszej i drugiej linii obrony, w zapewnianiu wiarygodności sprawozdawczości finansowej, w sposób umożliwiający biegłemu rewidentowi poznanie systemu kontroli wewnętrznej badanej jednostki (np. zgodnie z Międzynarodowym Standardem Rewizji Finansowej 315),
- b) omówienie z biegłym rewidentem, na odpowiednio wczesnym etapie badania, roli komórki audytu wewnętrznego jako trzeciej linii obrony, w sposób umożliwiający biegłemu rewidentowi korzystanie z wyników pracy komórki audytu wewnętrznego (np. zgodnie z Międzynarodowym Standardem Rewizji Finansowej 610),
- c) omówienie przez biegłego rewidenta istotnych ustaleń wykrytych w trakcie badania, w tym nieprawidłowości znaczących w odniesieniu do procesu sprawozdawczości finansowej oraz wszelkich znaczących słabości systemu kontroli wewnętrznej w zakresie sprawozdawczości finansowej oraz systemu księgowości.

29.2. Zasady współpracy komórki audytu wewnętrznego banku, będącego podmiotem zależnym, z analogiczną komórką podmiotu dominującego, powinny być określone w sformalizowanej polityce opracowanej przez zarząd banku i zatwierdzonej przez

radę nadzorczą banku, będącego podmiotem zależnym. Komórka audytu wewnętrznego może współpracować z analogiczną komórką podmiotu dominującego, o ile nie narusza to obowiązujących bank przepisów prawa oraz regulacji ostrożnościowych i niezależności komórki audytu wewnętrznego banku, będącego podmiotem zależnym oraz jest uzasadnione interesem tego banku.

29.3. Zakres współpracy komórki audytu wewnętrznego banku, będącego podmiotem zależnym, z analogiczną komórką podmiotu dominującego, powinien być wyraźnie określony i może obejmować wymianę wiedzy, doświadczenia, sformalizowanych procedur i metodyk audytowych oraz ewentualny udział w procesie audytowym, o ile:

- a) zarząd banku, będącego podmiotem zależnym i jego rada nadzorcza, lub komitet audytu, jeżeli został powołany, wyrażają jednoznaczną zgodę na każdorazową współpracę w ramach badania audytowego,
- b) w ramach planowania badań audytowych, analogiczna komórka podmiotu dominującego nie narzuca planów, programów, w tym harmonogramów badań audytowych,
- c) udział audytorów wewnętrznych analogicznej komórki podmiotu dominującego w przeprowadzaniu badania audytowego jest dopuszczalny wówczas, gdy komórka audytu wewnętrznego nie posiada wystarczającej liczby ekspertów w danym obszarze, gwarantujących odpowiednią jakość badania audytowego oraz gdy audytorzy wewnętrzni analogicznej komórki podmiotu dominującego spełniają rolę eksperckiego wsparcia zespołu audytowego,

29.4. Zasady współpracy komórki audytu wewnętrznego z analogiczną komórką podmiotu zależnego, powinny być określone w sformalizowanej polityce opracowanej przez zarząd banku i zatwierdzonej przez radę nadzorczą.

Rekomendacja 30

Bank powinien opracować program zapewniania jakości działalności doradczej i zapewniającej, wykonywanej przez komórkę audytu wewnętrznego.

30.1. Program zapewniania jakości powinien obejmować monitorowanie poziome jakości działalności komórki audytu wewnętrznego oraz dokonywanie oceny wewnętrznej i zewnętrznej działalności tej komórki.

30.2. W ramach oceny wewnętrznej kierujący komórką audytu wewnętrznego dokonuje oceny jakości pracy komórki audytu wewnętrznego przez zastosowanie odpowiednich kryteriów, obejmujących co najmniej takie mierniki działania, jak: stopień realizacji planu audytu, terminowość realizacji zadań, w tym realizacji badań audytowych,

rotację w komórce audytu wewnętrznego. Wyniki oceny wewnętrznej powinny być przedstawione i omówione na posiedzeniach zarządu banku i rady nadzorczej.

- 30.3. Działalność zapewniająca i doradcza komórki audytu wewnętrznego powinna podlegać regularnej ocenie zewnętrznej, nie rzadziej jednak, niż co pięć lat. Oceny zewnętrznej nie powinien dokonywać podmiot, który w ciągu trzech ostatnich lat świadczył usługi doradcze na rzecz banku, związane z audytem wewnętrznym banku.

Rekomendacja 31

Bank powinien opracować zasady raportowania przez komórkę audytu wewnętrznego do zarządu banku i rady nadzorczej lub komitetu audytu, jeżeli został powołany.

- 31.1. Kierujący komórką audytu wewnętrznego powinien opracować, a zarząd banku i rada nadzorcza powinny zatwierdzić zasady rocznego i jednoczesnego raportowania przez komórkę audytu wewnętrznego do zarządu banku i rady nadzorczej lub komitetu audytu, jeżeli został powołany, obejmujące co najmniej:

- a) sprawozdanie z realizacji celów, misji i strategii audytu wewnętrznego,
- b) stopień realizacji planów audytu,
- c) zestawienie wyników przeprowadzonych badań audytowych w danym okresie, wraz ze wskazaniem nieprawidłowości znaczących i krytycznych,
- d) status realizacji zaleceń poaudytowych, ze szczególnym uwzględnieniem zmian terminu realizacji zaleceń oraz zaleceń niezrealizowanych w terminie,
- e) ocenę skuteczności systemu kontroli wewnętrznej i systemu zarządzania ryzykiem, w ramach pierwszej i drugiej linii obrony,
- f) sposób zapewnienia niezależności komórce audytu wewnętrznego oraz kierującemu komórką audytu wewnętrznego i audytorom wewnętrznym,
- g) informacje o zapewnieniu środków finansowych niezbędnych do skutecznego wykonywania zadań przez komórkę audytu wewnętrznego,
- h) zakres działalności doradczej komórki audytu wewnętrznego,
- i) zakres współpracy komórki audytu wewnętrznego z analogiczną komórką podmiotu dominującego i podmiotów zależnych oraz z biegłym rewidentem,
- j) sposób zapewnienia jakości audytu wewnętrznego, w tym wyniki oceny wewnętrznej i zewnętrznej, jeżeli została przeprowadzona w danym okresie.

SPIS TREŚCI

LISTA REKOMENDACJI.....	9
REKOMENDACJE	14
A. ORGANIZACJA SYSTEMU KONTROLI WEWNĘTRZNEJ	14
B. FUNKCJA KONTROLI	19
C. ZAPEWNIANIE ZGODNOŚCI.....	27
D. AUDYT WEWNĘTRZNY	38

Opracowano w:

Departamencie Inspekcji Bankowych, Instytucji Płatniczych
i Spółdzielczych Kas Oszczędnościowo-Kredytowych UKNF