Komisja
Nadzoru
Finansowego

Łukasz Cichy

Funkcja compliance w bankach

CEDUR

CEDUR

Łukasz Cichy

FUNKCJA COMPLIANCE W BANKACH

Warszawa 2015

Komisja
Nadzoru
Finansowego

Publikacja została wydana nakładem Komisji Nadzoru Finansowego

Pl. Powstańców Warszawy 1
00-030 Warszawa
www.knf.gov.pl

Warszawa 2015
Wydanie I

ISBN 978-83-63380-99-1

Nakład: 1500 szt.

Stan prawny na dzień: 22.05.2015 r.

Przygotowanie do druku i druk:
Omikron sp. z o.o.

SPIS TREŚCI

WSTĘP

Compliance, czyli zgodność działalności prowadzonej przez bank z obowiązującymi przepisami prawa, regulacjami wewnętrznymi oraz przyjętymi przez bank standardami postępowania, to nie tylko podstawowy warunek bezpiecznego, stabilnego i ostrożnego zarządzania bankiem, ale także warunek dopuszczalności wykonywania przez tę instytucję jakichkolwiek usług i czynności. Od blisko dekady funkcja compliance w bankach, również w Polsce, przeżywa swój rozkwit i zaczyna zajmować należyte jej miejsce w systemie zarządzania bankiem. Niniejsze opracowanie ma za zadanie przybliżyć ową funkcję w jej ogólnym zarysie, wskazać podstawowy sposób jej organizacji, podział zadań w strukturze organizacyjnej banku, a także podstawowe wątpliwości, jakie nasuwają się przy analizie tego zagadnienia. Jednocześnie, z racji ogólnego charakteru niniejszego opracowania, jego przedmiotem nie jest funkcja compliance w działalności maklerskiej (uregulowana stosownym rozporządzeniem Ministra Finansów[1]), albowiem ta została poddana szczegółowej analizie w odrębnym piśmie UKNF[2]. Niniejsze opracowanie adresowane jest przede wszystkim do osób zajmujących się zawodowo lub naukowo zagadnieniem compliance w bankowości, w tym zwłaszcza do pracowników komórki compliance, komórki audytu wewnętrznego oraz osób pełniących kierownicze funkcje w banku.

[1] Rozporządzenie Ministra Finansów z dnia 24 września 2012 r. w sprawie określenia szczegółowych warunków technicznych i organizacyjnych dla firm inwestycyjnych, banków, o których mowa w art. 70 ust. 2 ustawy o obrocie instrumentami finansowymi, i banków powierniczych oraz warunków szacowania przez dom maklerski kapitału wewnętrznego (Dz.U. z 2012 r. poz. 1072).

[2] Stanowisko Urzędu Komisji Nadzoru Finansowego z dnia 27 maja 2014 r., dostępne na https://www.knf.gov.pl/Images/list_czynosci_nadzorcze_28052014_tcm75-38064.pdf. Stanowisko UKNF uwzględnia *Wytyczne w sprawie określonych aspektów wymogów dyrektywy MiFID dotyczących komórki ds. nadzoru zgodności z prawem* Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych (EUNGiPW).

COMPLIANCE JAKO ELEMENT SYSTEMU KONTROLI WEWNĘTRZNEJ, CZY ELEMENT ZARZĄDZANIA RYZYKIEM?

Historycznie ujmując nowoczesną funkcję compliance, należy przede wszystkim przywołać amerykański model kontroli wewnętrznej z 1992 r. zwany modelem COSO[3], który obok wiarygodności sprawozdawczości finansowej oraz skuteczności i efektywności działalności operacyjnej, traktował zgodność (compliance) z przepisami ustaw i rozporządzeń jako **cel** systemu kontroli wewnętrznej. Ten przełomowy dokument, który kontrolę wewnętrzną rozumie nie, jako porównywanie stanu faktycznego z wymaganym i formułowaniem wniosków, ale jako system zapewniania celów systemu kontroli wewnętrznej – nakazywał, aby każdemu z owych 3 celów zapewniać realizację poprzez 5 komponentów systemu, takich jak: środowisko kontroli, szacowanie ryzyka nieosiągnięcia celów, mechanizmy/czynności kontrolne, monitorowanie oraz informację i komunikację. Zgodność (compliance) stała się więc jednym z głównych celów systemu kontroli wewnętrznej, traktowanym na równi ze sprawozdawczością finansową i działalnością operacyjną.

Popularność modelu COSO, a w konsekwencji takiego pojmowania compliance, sprawiła, iż koncepcja ta, z pewnymi modyfikacjami, została przyjęta nie tylko przez Bazylejski Komitet Nadzoru Bankowego[4], ale także przez prawodawcę unijnego, który zarówno w art. 22 tzw. dyrektywy CRD, jak i w art. 74 oraz 88 ust. 1b ostatniej dyrektywy CRD IV[5] przyjął ów model jako własny. Także obecny Europejski Urząd Nadzoru Bankowego – EUNB (EBA – *European Banking Authority*), jak i jego poprzednik – CEBS, w swoich wytycznych[6], wprost traktowali compliance, jako element systemu kontroli wewnętrznej, obok funkcji audytu wewnętrznego i funkcji kontroli ryzyka. Mając powyższe na uwadze, polski ustawodawca, implementując w 2006 r. ówczesną dyrektywę CRD do ustawy – Prawo bankowe, wprost ustanowił, iż:

---

[3] COSO, *Internal Control – Integrated Framework*, 1992 r.

[4] Basel Committee on Banking Supervision, *Framework for Internal Control Systems in Banking Organizations*, 1998 r.

[5] Odpowiednio Dyrektywa 2006/48/WE Parlamentu Europejskiego i Rady z dnia 14 czerwca 2006 r. w sprawie podejmowania i prowadzenia działalności przez instytucje kredytowe (wersja przeredagowana); Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (*Capital Requirements Directive IV, CRD IV*).

[6] EBA, *Internal Governance*, 2011 r.; CEBS, *The Application of the Supervisory Review Process under Pillar 2*, 2006 r.

Art. 9c. *1. Celem systemu kontroli wewnętrznej jest wspomaganie procesów decyzyjnych przyczyniających się do zapewnienia:*
1) skuteczności i efektywności działania banku;
2) wiarygodności sprawozdawczości finansowej;
3) ***zgodności działania banku z przepisami prawa i regulacjami wewnętrznymi****.*
2. System kontroli wewnętrznej obejmuje:
1) mechanizmy kontroli ryzyka;
2) ***badanie zgodności działania banku z przepisami prawa i regulacjami wewnętrznymi****;*
3) audyt wewnętrzny.

Przyjęcie koncepcji, jakoby funkcja compliance należała do systemu kontroli wewnętrznej, oznacza, po pierwsze, że na banku ciąży obowiązek zapewniania zgodności, po drugie, że bank powinien stosować odpowiednie mechanizmy kontrolne, aby ową zgodność zapewnić, oraz, co najważniejsze, po trzecie, że nie należy łączyć zgodności jako funkcji kontrolnej z innymi funkcjami operacyjnymi i że należy ustalić jej relację z zarządzaniem ryzykiem.

Drugą koncepcją ujmowania funkcji compliance jest niezwykle popularne zarówno w bankach na świecie, jak i w Polsce, traktowanie jej jako elementu zarządzania ryzykiem. Opiera się ono na sporządzonym przez Bazylejski Komitet Nadzoru Bankowego w 2005 r. dokumencie *Zgodność i funkcja zapewnienia zgodności w bankach*, wedle którego funkcja compliance rozumiana jest w kontekście procesu, na który składa się identyfikacja, pomiar, ocena, monitorowanie, testowanie i sprawozdawczość odnośnie **zarządzania ryzykiem braku zgodności**. Ryzyko definiowane jest jako ryzyko sankcji prawnych, bądź regulaminowych, materialnych strat finansowych lub utraty dobrej reputacji, na jakie narażony jest bank w wyniku niestosowania się do ustaw, rozporządzeń, przepisów czy przyjętych przez siebie odpowiednich standardów i kodeksów postępowania mających zastosowanie w jego działalności. Dokument skupia się na obowiązkach rady nadzorczej, zarządu oraz komórki ds. zgodności, abstrahując od roli funkcji compliance w systemie kontroli wewnętrznej, a podkreślając obowiązek współpracy zwłaszcza z ryzykiem operacyjnym. Takie podejście skutkuje przeniesieniem ciężaru z zapewniania zgodności na identyfikowanie i ocenę ryzyka braku owej zgodności, co w konsekwencji powoduje wątpliwości co do charakteru funkcji compliance również wśród osób zawodowo zajmujących się tą kwestią w bankach.

W rzeczywistości zarysowany powyżej problem wydaje się być o wiele bardziej złożony, albowiem dotyka trudnego do rozstrzygnięcia zagadnienia, jakim jest generalnie stosunek systemu kontroli wewnętrznej do zarządzania ryzykiem, i to nie tylko w banku. Na świecie przyjmowane są rozmaite rozwiązania: od amerykańskiej relacji zawierania się systemu kontroli wewnętrznej w zarządzaniu ryzykiem, przez relację odwrotną, wskazywaną przez Bazylejski Komitet Nadzoru Bankowego w dokumencie *Principles for enhancing corporate governance* z 2011 r., poprzez popularną w Wielkiej Brytanii relację tożsamości, aż po wybraną przez unijnego prawodawcę relację rozłączności między systemem kontroli wewnętrznej, a zarządzaniem ryzykiem, na co wskazują nie tylko ww. dyrektywy CRD oraz wytyczne EUNB, ale także dyrektywa 2006/43/EC

oraz dyrektywa 2006/46/EC[7]. Polski ustawodawca również przyjął relację rozłączności, wskazując w art. 9 ust. 3 ustawy – Prawo bankowe, że w ramach systemu zarządzania w banku funkcjonuje co najmniej system zarządzania ryzykiem i system kontroli wewnętrznej.

Podejście będące formą pogodzenia obu koncepcji zostało wprowadzone z uwzględnieniem przepisów ustawy – Prawo bankowe, w uchwale Nr 258/2011 KNF[8] w 2011 r.[9] Z jednej strony, zgodnie z art. 9c ustawy – Prawo bankowe, zarząd, jak stanowi o tym wprost § 11 ww. uchwały, zapewnia zgodność działania banku z obowiązującymi przepisami prawa, co z kolei, choćby wedle art. 22 ust. 1 ustawy – Prawo bankowe czy art. 382 kodeksu spółek handlowych[10], powinno podlegać nadzorowi rady nadzorczej. Z drugiej strony, wedle § 23 tej samej uchwały, zarząd banku odpowiada za efektywne zarządzanie w banku ryzykiem braku zgodności, zaś rada nadzorcza, wedle § 22 ust. 1 ww. uchwały, sprawuje nadzór nad zarządzaniem ryzykiem braku zgodności, rozumianym jako skutki nieprzestrzegania przepisów prawa, regulacji wewnętrznych oraz przyjętych przez bank standardów postępowania. Oznacza to, iż, owszem, funkcja compliance w banku jest rozumiana jako zapewnianie zgodności, co stanowi jeden z trzech ustawowych celów systemu kontroli wewnętrznej, jednakże **w ramach** owego zapewniania, rada nadzorcza ma nadzorować, a zarząd ma zarządzać ryzykiem braku zgodności przy pomocy ustanowienia stałej i efektywnie działającej komórki ds. zarządzania ryzykiem braku zgodności. Przyjmując takie rozwiązanie, które wydaje się najbardziej efektywne, należy również mieć na względzie fakt, iż sama EUNB w ww. wytycznych (EBA, *Internal Governance*), choć, jak wskazano powyżej, zalicza funkcję compliance do systemu kontroli wewnętrznej, to jednocześnie posługuje się pojęciem ryzyka braku zgodności (ryzyka compliance). Z kolei system kontroli wewnętrznej COSO, chociaż traktuje compliance jako cel kontroli wewnętrznej, to w ramach jednego z 5 komponentów nakazuje szacować ryzyko nieosiągnięcia tegoż celu, czyli zgodności. Jednocześnie należy podkreślić, iż funkcja zapewniania zgodności, oprócz zapewniania przestrzegania przepisów, zarządzania ryzykiem braku zgodności, obejmuje także ewentualne doradztwo i raportowanie, które nie mieszczą

[7] Dyrektywa 2006/43/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie ustawowych badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych, zmieniająca dyrektywy Rady 78/660/EWG i 83/349/EWG oraz uchylająca dyrektywę Rady 84/253/EWG; Dyrektywa 2006/46/WE Parlamentu Europejskiego i Rady z dnia 14 czerwca 2006 r. zmieniająca dyrektywy Rady 78/660/EWG w sprawie rocznych sprawozdań finansowych niektórych rodzajów spółek, 83/349/EWG w sprawie skonsolidowanych sprawozdań finansowych, 86/635/EWG w sprawie rocznych i skonsolidowanych sprawozdań finansowych banków i innych instytucji finansowych oraz 91/674/EWG w sprawie rocznych i skonsolidowanych sprawozdań finansowych zakładów ubezpieczeń.

[8] Uchwała Nr 258/2011 Komisji Nadzoru Finansowego z dnia 4 października 2011 r. w sprawie szczegółowych zasad funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz 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, Dz.Urz. KNF z dnia 23 listopada 2011 r. Nr 11 poz. 42.

[9] Należy jednocześnie podkreślić, że wg stanu na dzień 22 maja 2015 r., w Ministerstwie Finansów trwają prace nad projektem nowelizacji ustawy – Prawo bankowe, stanowiącym transpozycję przepisów tzw. pakietu CRD IV/CRR do polskiego porządku prawnego. W związku z powyższym, jak wskazuje ww. projekt – w wersji z dnia 28 kwietnia 2015 r., upoważnienie do wydania uchwały Nr 258/2011 KNF prawdopodobnie zostanie usunięte, a w jego miejsce pojawi się upoważnienie dla „Ministra właściwego do spraw instytucji finansowych", do określenia w drodze rozporządzenia kwestii, które obecnie są regulowane w ww. uchwale KNF (z uwzględnieniem zmian wynikających z dyrektywy CRD IV). Brzmienie tego aktu wykonawczego będzie jednakże uzależnione od decyzji co do ostatecznego sposobu transpozycji pakietu CRD IV/CRR, tj. zakresu, w jakim przepisy te zostaną bezpośrednio transponowane w ustawie, a w jakim będą one przeniesione do aktów niższego rzędu.

[10] Dla uproszczenia wywodu skoncentrowano się na bankach w postaci spółek akcyjnych.

się w zarządzaniu ryzykiem i zapewnianiu przestrzegania przepisów przez pracowników w toku wykonywania obowiązków służbowych.

Jednocześnie należy wskazać na próbę szerokiego ujęcia funkcji compliance w rozdziale 8 *Zasad ładu korporacyjnego dla instytucji nadzorowanych* (dalej: Zasady), wydanych przez KNF w 2014 r.[11] Zasady z racji stosowania do wszystkich podmiotów nadzorowanych przez Komisję Nadzoru Finansowego, a więc nie tylko do banków, ale i do domów maklerskich czy zakładów ubezpieczeń nie przesądzają, czy funkcja compliance ma stanowić element systemu kontroli wewnętrznej, czy zarządzania ryzykiem, czy wręcz stanowić odrębny system, a jedynie opisują w ww. rozdziale 8 „kluczowe systemy i funkcje wewnętrzne", których umiejscowienie zależy do wyboru instytucji nadzorowanych i przepisów regulujących compliance w danym sektorze.

[11] KNF, *Zasady ładu korporacyjnego dla instytucji nadzorowanych*, Warszawa, 22 lipca 2014 r.

PODZIAŁ ZADAŃ W RAMACH FUNKCJI COMPLIANCE

Znając charakter funkcji compliance można wskazać, komu przypisane są obowiązki w ramach owej funkcji na trzech głównych szczeblach w strukturze organizacyjnej banku: szczeblu najwyższych organów banku, czyli rady nadzorczej i zarządu, szczeblu komórki compliance (komórki ds. zgodności) oraz szczeblu najniższym, czyli szczeblu jednostek biznesowych i operacyjnych banku oraz wszystkich szeregowych pracowników banku. Na świecie wyodrębniły się trzy modele odnośnie umiejscowienia funkcji compliance wewnątrz struktury banku.

W tzw. modelu centralnym, zarówno wiedza specjalistyczna, jak i cały proces zapewniania zgodności, bądź zarządzania ryzykiem braku zgodności, skupiają się w komórce ds. zgodności, która ma dostęp do jednostek biznesowych i operacyjnych banku, wszystkich szeregowych pracowników banku oraz bezpośrednio podlega pod zarząd banku – a w szczególności – zwykle prezesa.

W tzw. modelu hybrydowym, wiedza specjalistyczna nadal skupia się w komórce ds. zgodności, jednakże część zadań związanych z zapewnianiem zgodności, czy też zarządzaniem ryzykiem braku zgodności, delegowana jest na jednostki biznesowe i operacyjne banku oraz szeregowych pracowników. Komórka ds. zgodności jest odpowiedzialna za całościowe (systemowe) zapewnianie zgodności i przede wszystkim całościowy proces zarządzania ryzykiem braku zgodności (m.in. monitorując jednostki biznesowe w zakresie działań zgodnych z przepisami), w tym zwłaszcza za koordynację i raportowanie do rady nadzorczej i zarządu, podczas gdy jednostki biznesowe i operacyjne oraz pracownicy mają za zadanie działanie zgodne z przepisami prawa i regulacjami wewnętrznymi oraz częściowe uczestniczenie w procesie zarządzania ryzykiem, poprzez np. identyfikację lub ocenę tego ryzyka.

W tzw. modelu rozproszonym, jak nietrudno się domyśleć, zarówno wiedza specjalistyczna, jak i cały proces zapewniania zgodności, bądź zarządzania ryzykiem braku zgodności delegowany zostaje na jednostki biznesowe i operacyjne banku oraz szeregowych pracowników. Komórka ds. zgodności staje się jedynie formalnym pośrednikiem w przekazywaniu informacji do zarządu lub też staje się wręcz zbędna.

Za najbardziej skuteczny, ale też najbardziej popularny, uznawany jest model hybrydowy, aczkolwiek jego skuteczność uzależniona jest od wielkości banku, czy też tzw. grupy/holdingu, do którego należy bank.

W Polsce, mimo iż nie wyrażono tego wprost, a wynika to z interpretacji obowiązujących przepisów prawa, rekomendacji i przyjmowanych standardów rynkowych, banki powinny stworzyć system hybrydowy. Zgodnie chociażby z rekomendacją 14.1 Rekomendacji M KNF[12] *W przypadku, gdy*

[12] KNF, Rekomendacja M *dotycząca zarządzania ryzykiem operacyjnym w bankach*, 2013.

część zadań odnoszących się do ryzyka braku zgodności jest wykonywana przez jednostkę inną niż komórka ds. zarządzania ryzykiem braku zgodności (np. przez departament prawny) powinien być wyraźnie określony podział obowiązków pomiędzy te jednostki. Oznacza to, iż rekomenduje się ustanowienie skutecznej komórki ds. zgodności (zwanej również komórką ds. zarządzania ryzykiem braku zgodności, czy też komórką compliance) oraz dopuszcza delegowanie części zadań na inne jednostki, a więc m.in. jednostki biznesowe i operacyjne oraz pracowników banku.

Pamiętając o swoistym dualizmie funkcji compliance, która ma za zadanie zapewnianie zgodności jako jeden z celów systemu kontroli wewnętrznej, a jednocześnie w ramach owego zapewniania ma m.in. zarządzać ryzykiem braku zgodności, należy system hybrydowy odnieść do obu tych zadań.

W przypadku zapewniania zgodności na najwyższym szczeblu struktury organizacyjnej banku, zgodnie z uchwałą Nr 258/2011 KNF:

> *§ 11. 1. Zarząd banku zapewnia zgodność działania banku z obowiązującymi przepisami prawa, z uwzględnieniem działania banku na podstawie przepisów prawa innego państwa i powiązań banku z innymi podmiotami, które mogłyby utrudnić skuteczne zarządzanie bankiem.*

Z kolei rada nadzorcza, zgodnie z art. 9a ust. 2 oraz art. 22 ust. 1 ustawy – Prawo bankowe, z racji obowiązku pełnienia funkcji organu nadzoru, nadzoruje także zapewnianie zgodności. Na najniższym szczeblu struktury organizacyjnej banku, zapewnianie zgodności wynika z obowiązków, jakie w ramach systemu kontroli wewnętrznej przypisane są pracownikom. Skoro bowiem zapewnianie zgodności to jeden z celów systemu kontroli wewnętrznej, a zgodnie choćby z Rekomendacją 5 Rekomendacji H[13] *kontrola jest wykonywana na każdym etapie działania banku i wykonywanych zadań i czynności przez pracowników*, to oczywiste jest, iż pracownicy w ramach obowiązków służbowych mają zapewniać zgodność. Jeszcze wyraźniej stanowi o tym § 46 ust. 3 *Zasad ładu korporacyjnego dla instytucji nadzorowanych*, wedle którego *Pracownikom instytucji nadzorowanej w ramach obowiązków służbowych należy przypisać odpowiednie zadania związane z zapewnianiem realizacji celów systemu kontroli wewnętrznej*.

Obowiązek zapewniania zgodności nie został ustanowiony wprost, a jedynie odnośnie komórki ds. zgodności. Wynika on jednak z treści ww. *Zasad ładu korporacyjnego dla instytucji nadzorowanych*, które stanowią, iż:

> *§ 47. 1. Instytucja nadzorowana powinna opracować i wdrożyć efektywną, skuteczną i niezależną funkcję zapewniania zgodności działania instytucji nadzorowanej z przepisami prawa i regulacjami wewnętrznymi oraz z uwzględnieniem rekomendacji nadzorczych.*
> *2. Sposób organizacji funkcji zapewnienia zgodności powinien gwarantować niezależność wykonywania zadań w tym zakresie.*

Sposób zapewniania niezależności wskazanej w § 47 ust. 2 Zasad, o czym będzie mowa poniżej, uregulowany został w § 49 Zasad, które niezależność funkcji zapewniania zgodności postrzegają

[13] KNF, Rekomendacja H *dotycząca systemu kontroli wewnętrznej w bankach*, 2011.

w kontekście uprawnień osoby kierującej **komórką** do spraw zapewnienia zgodności. Oznacza to, że komórka compliance jak najbardziej powinna uczestniczyć w procesie zapewniania zgodności, a jej niezależność jest kluczowym warunkiem skuteczności całej funkcji zapewniania zgodności. Zalecenia Komisji Nadzoru Finansowego nie określają, jakie konkretne zadania powinna w ramach zapewniania zgodności wykonywać komórka ds. zgodności. Wydaje się, że z racji bardziej intensywnego uczestnictwa w zarządzaniu ryzykiem braku zgodności, komórka ta w tym przypadku powinna skupiać się na koordynowaniu całej funkcji, raportowaniu do rady nadzorczej i zarządu oraz doradztwie, jako że większość obowiązków zapewniania zgodności, czyli przestrzegania przepisów, leży po stronie tych, do których te przepisy na co dzień mają zastosowanie, czyli do pracowników oraz do jednostek biznesowych i operacyjnych banku.

Nieco inaczej ciężar obowiązków rozkłada się w przypadku zarządzania ryzykiem braku zgodności. Na najwyższym szczeblu struktury organizacyjnej banku, zgodnie z uchwałą Nr 258/2011 KNF:

§ 22. 1. Rada nadzorcza banku sprawuje nadzór nad zarządzaniem ryzykiem braku zgodności rozumianym jako skutki nieprzestrzegania przepisów prawa, regulacji wewnętrznych oraz przyjętych przez bank standardów postępowania.
2. Rada nadzorcza zatwierdza założenia polityki banku w zakresie ryzyka braku zgodności.
3. Rada nadzorcza co najmniej raz w roku ocenia stopień efektywności zarządzania ryzykiem braku zgodności przez bank.
§ 23. Zarząd banku odpowiada za efektywne zarządzanie w banku ryzykiem braku zgodności.
§ 24. 1. Zarząd banku odpowiada za opracowanie polityki zgodności, zapewnienie jej przestrzegania i składanie sprawozdań radzie nadzorczej w sprawie zarządzania w banku ryzykiem braku zgodności.
2. Polityka zgodności zawiera podstawowe zasady działania pracowników banku i wyjaśnia główne procesy identyfikujące ryzyko braku zgodności i umożliwiające zarządzanie ryzykiem braku zgodności na wszystkich szczeblach organizacji banku.

Podział zadań na najwyższym szczeblu jest więc podobny, jak przy zapewnianiu zgodności. Rada nadzorcza nadzoruje, a zarząd ponosi główną odpowiedzialność za cały proces zarządzania. Jednocześnie na zarządzie ciąży obowiązek ustanowienia tzw. polityki zgodności. Jest to podstawowy i tym samym najważniejszy dokument odnośnie compliance w banku. W wersji minimum, gdy odnosi się jedynie do procesu zarządzania ryzykiem braku zgodności, zarząd powinien ustanawiać i opisywać kwestie związane z zarządzaniem ryzykiem, wynikające wprost z § 23–26 uchwały Nr 258/2011 KNF:

- szczegółowe zadania zarządu, rady nadzorczej odnośnie zarządzania ryzykiem,
- przebieg procesu zarządzania ryzykiem,
- obowiązki komórki ds. zgodności dla procesu zarządzania ryzykiem braku zgodności oraz relację z funkcją compliance na poziomie grupy/holdingu.

W wersji maksimum, gdy polityka zgodności obejmuje nie tylko sam proces zarządzania ryzykiem braku zgodności, ale całą funkcję zapewniania zgodności, dokument ten powinien ustanawiać i opisywać także m.in.:

- proces zapewniania zgodności na wszystkich szczeblach struktury organizacyjnej banku,
- status formalny komórki ds. zgodności, w tym nie tylko jej obowiązki, ale także wymogi organizacyjne, a zwłaszcza mechanizmy zagwarantowania niezależności.

W przypadku zarządzania ryzykiem braku zgodności, kluczową rolę odgrywa środkowy szczebel struktury organizacyjnej banku, czyli komórka ds. zgodności. O ile bowiem, przy zapewnianiu zgodności, to, czy dany przepis ustawy, czy dana regulacja wewnętrzna, jest na co dzień przestrzegana, zależy od zachowania pracowników oraz jednostek biznesowych i operacyjnych, o tyle w przypadku ryzyka braku zgodności, jego identyfikacja, ocena, kontrola i monitorowanie zależą w dużej mierze od know-how pracowników komórki ds. zgodności, których większość obowiązków poświęcona jest właśnie temu zagadnieniu. To na komórce ds. zgodności ciąży bowiem obowiązek opracowania całej metodyki zarządzania ryzykiem braku zgodności i stosowania tej metodyki dla poszczególnych etapów procesu zarządzania ryzykiem. Jednak komórka ds. zgodności nie tylko ocenia całościowe ryzyko braku zgodności, ale także ryzyko braku zgodności w poszczególnych, samodzielnie wybranych obszarach działalności banku, na przykład poprzez prowadzenie testów zgodności, a jednocześnie wykonuje szereg dodatkowych zadań przypisanych wyłącznie tej komórce, o czym będzie mowa poniżej.

W zarządzaniu ryzykiem braku zgodności ważną rolę odgrywa także trzeci szczebel struktury organizacyjnej banku, a więc pracownicy oraz jednostki biznesowe i operacyjne. W modelu hybrydowym, delegowana na nich jest część zadań wykonywanych przez komórkę ds. zgodności, zwłaszcza odnośnie identyfikowania ryzyka, samooceny ryzyka i jego monitorowania. Pracownicy oraz jednostki biznesowe i operacyjne posiadają o wiele więcej kluczowych informacji odnośnie własnej działalności, niż nawet najlepiej przygotowana komórka ds. zgodności, wobec czego informacje te mogą być wykorzystane np. w procesie samooceny ryzyka, która jest następnie weryfikowana i korygowana przez komórkę ds. zgodności. Jednocześnie pracownicy i jednostki biznesowe stanowią podstawowe źródło informacji o ryzyku, w związku z czym, z jednej strony, jako uczestnicy procesu zarządzania ryzykiem dokonują samooceny, a z drugiej stanowią źródło informacji w tym procesie.

Ogólny podział zadań na trzech szczeblach struktury organizacyjnej banku odnośnie zapewniania zgodności oraz zarządzania ryzykiem braku zgodności, rozumianym jako element tego zarządzania, przedstawia poniższa tabela:

Tabela 1. Funkcja compliance – matryca obowiązków (oprac. własne)

Szczeble zarządzania bankiem	Zapewnianie zgodności			
	Zarządzanie ryzykiem braku zgodności	Przestrzeganie przepisów, regulacji wewnętrznych i przyjętych standardów postępowania	Doradztwo	Raportowanie
Zarząd	Tak	Tak	Nie	Tak, do rady nadzorczej
Komórka ds. zgodności	Tak	Tak	Tak	Tak, do rady nadzorczej i zarządu
Pracownicy oraz jednostki biznesowe i operacyjne	Tak	Tak	Nie	Tak, do komórki ds. zgodności

NIEZALEŻNOŚĆ FUNKCJI COMPLIANCE

Kluczowym wymogiem skuteczności funkcji compliance jest wymóg jej niezależności. Dotyczy to zarówno rozumienia funkcji compliance, jako elementu systemu kontroli wewnętrznej spełniającej cel tegoż systemu w postaci zapewnienia zgodności, jak i zarządzania ryzykiem braku zgodności, w tym w szczególności niezależności komórki ds. zgodności i kierującego tą komórką. W przypadku zapewniania zgodności, niezależność funkcji compliance jest wymagana przez ww. wytyczne EUNB (EBA, *Internal Governance*). Zgodnie z 24.6 wytycznych, funkcja kontrolna, a więc również funkcja compliance jest niezależna, jeśli:

a. jej pracownicy nie wykonują żadnych zadań wchodzących w zakres działalności, którą funkcja kontrolna ma monitorować i kontrolować;
b. funkcja kontrolna jest oddzielona organizacyjnie od działalności, którą ma monitorować i kontrolować;
c. kierownik funkcji kontrolnej podlega osobie nieponoszącej odpowiedzialności za zarządzanie działalnością, którą monitoruje i kontroluje funkcja kontrolna. Generalnie kierownik funkcji kontrolnej powinien podlegać bezpośrednio organowi zarządzającemu oraz stosownym komitetom i powinien regularnie uczestniczyć w ich posiedzeniach;
d. wynagrodzenie pracowników funkcji kontrolnej nie powinno być uzależnione od wyników działalności, którą ona monitoruje i kontroluje oraz nie powinno w inny sposób potencjalnie negatywnie wpływać na ich obiektywizm.

Należy jednak pamiętać, że w ramach zapewniania zgodności, funkcja compliance w banku skupia się na wielu rodzajach czynności, w tym również na zapewnianiu, że przepisy ustawy i dane regulacje są przestrzegane. Jak wskazano powyżej, proces ten dotyczy wszystkich pracowników oraz jednostek biznesowych i operacyjnych, które w ramach wykonywania obowiązków służbowych mają zapewniać zgodność. Tym samym trudno uznać, aby wszyscy pracownicy byli niezależni. Trudność w rozumieniu niezależności funkcji compliance, traktowanej jako zapewnianie zgodności, polega na wskazaniu, kiedy jest mowa o funkcji jako całości, kiedy jest mowa o mechanizmie podziału obowiązków w banku w ramach owej funkcji, a kiedy wreszcie jest mowa o komórce ds. zgodności i jej pracownikach. Należy jednocześnie pamiętać, że ww. wytyczne EUNB odnoszą się do wszystkich funkcji kontrolnych, a więc i do tzw. funkcji kontroli ryzyka czy funkcji audytu wewnętrznego. W tych przypadkach wytyczne EUNB odnośnie niezależności również powinny zostać odpowiednio dopasowane do charakteru każdej z funkcji kontrolnej. W polskim tłumaczeniu wytycznych funkcje kontrolne nazywa się „komórkami kontrolnymi". Wydaje się to zbyt daleko idącym uproszczeniem, albowiem, jak wskazano powyżej, w ramach modelu hybrydowego, zadania funkcji (np. compliance) mogą i są realizowane na kilku szczeblach organizacji. Niemniej jednak, odnosząc się do wytycznych EUNB dotyczących niezależności, należy podkreślić, że wytyczne odnośnie wynagrodzenia odnoszą się w oczywisty sposób do pracow-

ników komórki ds. zgodności, zaś wytyczne odnośnie kierującego funkcją compliance odnoszą się w oczywisty sposób do kierującego całą funkcją compliance. Wytyczne EUNB, wskazujące, by nie wykonywać żadnych zadań wchodzących w zakres działalności, którą funkcja kontrolna (compliance) ma monitorować i kontrolować, należy z kolei postrzegać jako klasyczny mechanizm systemu kontroli wewnętrznej w postaci podziału obowiązków (tzw. *segregation of duties*). Oznacza on bowiem, że jeśli w ramach jakiegokolwiek procesu (np. udzielania kredytów), pracownik wykonuje określone zadania, to nie może jednocześnie monitorować i kontrolować wykonywania tych zadań, bo wówczas mamy do czynienia z tzw. problemem kontroli samego siebie. Osadzając to w kontekście funkcji compliance, oznacza to, że za kontrolę i monitoring zgodności udzielania kredytów z określonymi przepisami i regulacjami wewnętrznymi nie może odpowiadać pracownik, który tych kredytów udzielał. W tym właśnie przejawiać się ma niezależność zapewniania zgodności w ramach mechanizmu podziału obowiązków. Jednocześnie nie oznacza to, że za funkcję zapewniania zgodności odpowiada tylko pracownik monitorujący i kontrolujący zgodność udzielania kredytów, albowiem również ten, który kredytów udziela ma obowiązek zapewniania zgodności w ramach wykonywania własnych obowiązków. Innym równie ważnym przypadkiem jest sytuacja, gdy komórka ds. zgodności zajmuje się doradztwem (np. opiniuje daną regulację), czy też stosuje mechanizm kontrolny (np. w postaci wstępnego zatwierdzenia wzorców umownych) i jednocześnie przeprowadza także testy zgodności tychże regulacji czy wzorców. W takim przypadku przeprowadzanie testów zgodności wzorców czy regulacji, o których to zgodności się wcześniej opiniowało, tudzież ową zgodność się zatwierdzało, stanowi klasyczny problem kontroli samego siebie, który powinien być rozstrzygany tak jak w analogicznej sytuacji w przypadkach audytu wewnętrznego – poprzez **zwiększenie zasobów** i wewnętrzny podział zadań między pracowników komórki. Warto jednak dodać, że problem kontroli samego siebie nie będzie jednak występował, gdy ten sam pracownik komórki ds. zgodności najpierw zaopiniuje/zatwierdzi dany wzorzec/regulację, a następnie przeprowadzi testy zgodności odnośnie stosowania owego wzorca/regulacji. Wówczas testy zgodności polegać będą bowiem nie tyle na testowaniu zgodności wzorca/regulacji z danym przepisem prawnym, co na testowaniu zgodności działania danej osoby/komórki z owym wzorcem.

Podobne wątpliwości, jak w przypadku funkcji zapewnienia zgodności, odnoszą się do zarządzania ryzykiem braku zgodności, w którym też część zadań dotyczy całego procesu zarządzania ryzykiem braku zgodności jako niezależnego od innych procesów w banku, część odnosi się do wymogów odnośnie kierującego komórką ds. zgodności, jej statusu i jej pracowników, a część do mechanizmów kontroli wewnętrznej występujących w ramach zarządzania ryzykiem braku zgodności. W tym przypadku dochodzi również dodatkowy problem zakazu łączenia zarządzania ryzykiem z kontrolą wewnętrzną, jednakże należy pamiętać, iż zarządzanie ryzykiem braku zgodności to element systemu kontroli wewnętrznej i w tym przypadku takie łączenie jest wskazane.

Reasumując, w przypadku niezależności funkcji compliance, czy to rozumianej jako zapewnianie zgodności, czy jedynie jako zarządzanie ryzykiem braku zgodności, należy:

- wyodrębnić funkcję compliance jako niezależną od innych funkcji w banku,
- nadać odpowiedni status kierującemu funkcją compliance i zapewnić mu niezależność,
- wyodrębnić niezależną komórkę ds. zgodności (compliance) i osobę nią kierującą,

- ustanowić odpowiednie mechanizmy kontrolne zapewniające niezależność w związku z wykonywaniem obowiązków w ramach poszczególnych procesów, jak np. podział obowiązków, nadzór przełożonego, zatwierdzenia, weryfikacje itd.

Powyższe ogólne wymogi odnośnie niezależności funkcji compliance zostały odzwierciedlone w poszczególnych wytycznych polskiego organu nadzoru.

Niezależność dla wszystkich instytucji nadzorowanych, w tym dla banków, została przewidziana w *Zasadach ładu korporacyjnego dla instytucji nadzorowanych*:

§ 47.
1. Instytucja nadzorowana powinna opracować i wdrożyć efektywną, skuteczną i niezależną funkcję zapewniania zgodności działania instytucji nadzorowanej z przepisami prawa i regulacjami wewnętrznymi oraz z uwzględnieniem rekomendacji nadzorczych.
2. Sposób organizacji funkcji zapewnienia zgodności powinien gwarantować niezależność wykonywania zadań w tym zakresie.

§ 49.
1. Osoba kierująca komórką audytu wewnętrznego oraz osoba kierująca komórką do spraw zapewnienia zgodności mają zapewnioną możliwość bezpośredniego komunikowania się z organem zarządzającym oraz nadzorującym lub komitetem audytu, a także powinny mieć możliwość bezpośredniego i jednoczesnego raportowania do tych organów.
2. Osoba kierująca komórką audytu wewnętrznego oraz osoba kierująca komórką do spraw zapewnienia zgodności uczestniczy w posiedzeniach organu zarządzającego i organu nadzorującego lub komitetu audytu, jeżeli przedmiotem posiedzenia są zagadnienia związane z systemem kontroli wewnętrznej, funkcją audytu wewnętrznego lub funkcją zapewnienia zgodności.
3. W instytucji nadzorowanej powoływanie i odwoływanie osoby kierującej komórką audytu wewnętrznego oraz osoby kierującej komórką do spraw zapewnienia zgodności odbywa się za zgodą organu nadzorującego lub komitetu audytu.
4. W instytucji nadzorowanej, w której nie funkcjonuje komórka audytu lub komórka do spraw zapewnienia zgodności uprawnienia wynikające z ust. 1–3 przysługują osobom odpowiedzialnym za wykonywanie tych funkcji.

W przypadku banków, na niezależność wskazuje wprost rekomendacja 14 Rekomendacji M KNF:

14.2. Funkcjonująca w banku komórka ds. zarządzania ryzykiem braku zgodności powinna być w odpowiednim stopniu niezależna, tj. w szczególności jej kierownik, nie powinien być zaangażowany w działalność, która mogłaby rodzić konflikt interesów z jego obowiązkami w ramach komórki ds. zarządzania ryzykiem braku zgodności.
14.3. Komórka ds. zarządzania ryzykiem braku zgodności musi mieć zapewnione odpowiednie zasoby niezbędne do efektywnego wykonywania jej zadań. W szczególności jej personel powinien posiadać odpowiednie kwalifikacje i doświadczenie, które umożliwią mu właściwe wykonywanie powierzonych obowiązków oraz mieć zapewniony dostęp do informacji niezbędnych do wykonywania swoich obowiązków.

Jak łatwo zauważyć, analizując ww. wytyczne, na szczególną uwagę w kontekście niezależności, zasługuje status osoby kierującej komórką ds. zgodności oraz status samej komórki. Jak to wynika wprost z ww. § 49 *Zasad ładu korporacyjnego dla instytucji nadzorowanych*, status osoby kierującej komórką ds. zgodności został zrównany ze statusem osoby kierującej komórką audytu wewnętrznego. Mają one taki sam dostęp do rady nadzorczej i zarządu i tak samo ich odwołanie wymaga zgody rady nadzorczej lub komitetu audytu. Zasady określają taką komórkę zgodności mianem „komórki do spraw zapewnienia zgodności", co jest zbieżne z przyjętą w Zasadach koncepcją funkcji „zapewniania zgodności" wskazaną w § 47 tego dokumentu. Ponadto, zgodnie z § 49 ust. 4 Zasad *w instytucji nadzorowanej, w której nie funkcjonuje komórka audytu lub komórka do spraw zapewnienia zgodności uprawnienia wynikające z ust. 1–3 przysługują osobom odpowiedzialnym za wykonywanie tych funkcji*. Oznacza to, że w Zasadach przyjęto koncepcję, iż w ramach funkcji zapewniania zgodności (compliance), bez względu na to, czy mamy do czynienia z modelem hybrydowym, czy rozproszonym (jak np. w mniejszych organizacjach niebędących bankami), zawsze należy wyodrębnić osobą odpowiedzialną za zapewnianie zgodności, dysponującą odpowiednią niezależnością. Taką osobę w praktyce nazywa się z jęz. angielskiego *compliance officerem*. Zwykle *compliance officer*, zwany też *chief compliance officerem*, jest osobą jednocześnie odpowiadającą za funkcję zapewniania zgodności oraz kierującą komórką ds. zgodności, więc i procesem zarządzania ryzykiem braku zgodności. Zdarza się jednak tak, że w banku następuje rozdział między osobą odpowiedzialną za całą funkcję zgodności (zwykle jest to osoba na szczeblu zarządu lub osoba podlegająca mu bezpośrednio – *chief compliance officer*), a osobą kierującą samą komórką ds. zgodności (*compliance officer*). Takie rozwiązanie motywowane jest chęcią nadania osobie odpowiedzialnej za całościową funkcję compliance najwyższej rangi w strukturze banku. Z drugiej strony rozwiązanie takie może być niestety również podyktowane chęcią ograniczenia komórki ds. zgodności i jej kierującego poprzez filtrowanie informacji dotyczących compliance przeznaczonych dla rady nadzorczej i zarządu banku. Z tego powodu wydaje się, że takie rozwiązanie można uznać za dopuszczalne, o ile osoba kierująca komórką ds. zgodności nadal będzie posiadała ww. status niezależności, a z kolei większość zadań osoby odpowiadającej za całościową funkcję zapewniania zgodności będzie dotyczyło stricte compliance, a nie, co niedopuszczalne, odpowiedzialności za inne rodzaje ryzyka czy działalność operacyjną. W takim przypadku wybór, kto jest faktycznie *compliance officerem* należy do banku, i w przypadku zachowania niezależności osoby kierującej komórką ds. zgodności, staje się wtórny. Wszak najważniejszy wymóg nadal jest spełniony.

Drugim, obok wymogu niezależności osoby kierującej komórką ds. zgodności, jest wymóg niezależność samej komórki ds. zgodności. Na właściwie zapewnioną niezależność komórki ds. zgodności, składa się:

- wyodrębniony status formalny i działanie na podstawie sformalizowanego dokumentu określającego cel, uprawnienia, zakres zadań i jej odpowiedzialność,
- prawo do swobodnego wyrażania opinii i zajmowania stanowiska bez obawy negatywnych konsekwencji ze strony władz i pracowników banku,
- prawo do prowadzenia wewnętrznych postępowań wyjaśniających incydenty braku zgodności,
- prawo do wnioskowania o zlecenie zewnętrznej opinii prawnej, w przypadku wątpliwości odnośnie aktualnego stanu prawnego,

- swobodny dostęp do kluczowych osób/stanowisk w banku, w tym zwłaszcza do komórki audytu wewnętrznego, departamentu prawnego, komórki ryzyka operacyjnego, koordynatora compliance na poziomie Grupy/holdingu (jeśli taki istnieje), zarządu oraz do rady nadzorczej (komitetu audytu) banku,
- wyposażenie w odpowiednie zasoby ludzkie zarówno pod kątem ilości, jak i wiedzy oraz doświadczenia pracowników umożliwiające realizację funkcji compliance, podział obowiązków oraz wyposażenie w odpowiednie zasoby budżetowe.

Niezwykle istotny dla skuteczności i niezależności komórki ds. zgodności, jest nie tylko ww. dostęp do kluczowych osób/stanowisk w banku, w tym zwłaszcza do komórki audytu wewnętrznego, komórki departamentu prawnego, komórki ryzyka operacyjnego, koordynatora compliance na poziomie Grupy (jeśli taki istnieje), ale także wzajemne relacje z nimi, odzwierciedlone w odpowiednich regulaminach i politykach, o czym stanowi rekomendacja 14.3 Rekomendacji M KNF. Wzajemna wymiana informacji, komunikacja, czerpanie z baz danych, doradztwo i wsparcie, obniża problem asymetrii informacyjnej oraz pozwala na pełniejsze wykorzystanie zasobów. Jednocześnie nie należy zapominać, iż rolą audytu wewnętrznego jest badanie nie tyle zgodności, co przede wszystkim skuteczności systemu zarządzania ryzykiem i systemu kontroli wewnętrznej (zwłaszcza mechanizmów kontrolnych). Kluczową kwestią wydaje się więc po pierwsze, wzajemne ustalenie zakresu przedmiotowego działań audytu wewnętrznego i funkcji compliance, zwłaszcza w kontekście przeprowadzania testów zgodności przez funkcję compliance w taki sposób, aby nie dochodziło do dublowania zadań. Po drugie, należy pamiętać, że z racji przynależności do systemu kontroli wewnętrznej funkcja compliance, w tym także komórka ds. zgodności, powinny być poddawane badaniom audytu wewnętrznego. Mimo iż funkcja compliance, razem z funkcją audytu wewnętrznego, należą do systemu kontroli wewnętrznej, to zgodnie z ww. wytycznymi EUNB, funkcja compliance stanowi tzw. drugą linię obrony, zaś audyt wewnętrzny tzw. trzecią linię obrony, kontrolującą dwie pozostałe.

ZAKRES PRZEDMIOTOWY FUNKCJI COMPLIANCE

Na pytanie o zgodność których działań banku z jaką konkretną regulacją jest przedmiotem funkcji zgodności (compliance) najłatwiej odpowiedzieć wszystkich działań banku ze wszystkimi regulacjami dotyczącymi banków, a konkretnie zgodności działalności banku ze wszystkimi przepisami, regulacjami wewnętrznymi i przyjętymi przez bank standardami postępowania dotyczącymi tejże działalności (czy też bardziej ogólnie – standardami rynkowymi). Wynika to zarówno z art. 9c ust. 1 pkt 3 ustawy – Prawo bankowe stanowiącego, iż zakres przedmiotowy obejmuje zgodność z przepisami prawa i regulacjami wewnętrznymi, jak i z definicji ryzyka braku zgodności, rozumianego wedle § 22 ust. 1 uchwały Nr 258/2011 KNF, jako skutku nieprzestrzegania przepisów prawa, regulacji wewnętrznych oraz przyjętych przez bank standardów postępowania. Nie trudno się domyślić, że tak zarysowany zakres przedmiotowy jest niezwykle szeroki, zwłaszcza, że przepisy prawa zwykle rozumiane są nie tylko jako tzw. *hard law*, ale także jako rozmaite wytyczne i rekomendacje, rozumiane jako tzw. *soft law*. Tym bardziej więc widać, jak użyteczny jest hybrydowy model funkcji compliance, gdzie ogromna część owych przepisów prawa i regulacji wewnętrznych zapewniania jest przez pracowników oraz jednostki biznesowe i operacyjne. Komórka ds. zgodności, w związku ze swoją rolą, co najwyżej prowadzi szkolenia i pełni funkcję doradczą odnośnie stosowania tychże przepisów, koordynuje cały proces zapewniania zgodności, wstępnie opiniuje i zatwierdza wybrane wzorce i regulacje wewnętrzne oraz, co najważniejsze, identyfikuje, ocenia, kontroluje, monitoruje i raportuje o ryzyku braku zgodności z tymi przepisami, regulacjami wewnętrznymi i przyjętymi przez bank standardami postępowania. Jak będzie to widać przy szczegółowej analizie procesu zarządzania ryzykiem, komórka ds. zgodności skupiać się musi z jednej strony na najważniejszych przepisach i regulacjach wewnętrznych, z drugiej na tych, które generują największe ryzyko. Zakres badania ryzyka zgodności zawsze zależał będzie od obszaru działalności banku, zmian legislacyjnych, wyników poprzednich raportów czy informacji od innych, kluczowych komórek. Niemniej istnieją pewne obszary szczególnej uwagi funkcji compliance przypisane komórce ds. zgodności, które powtarzają się niemal w każdym banku. Należą do nich:

- przepisy i regulacje związane z prawem bankowym (w tym procedury udzielania kredytów[14]),
- tajemnica bankowa, informacje poufne i stanowiące tajemnicę zawodową,
- polityka informacyjna dotycząca ujawnień,
- przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu[15],
- ryzyko braku zgodności związane z klientami i transakcjami, np. tworzenie listy kontrahentów, z którymi bank nie zamierza podejmować współpracy (rekomendacja 14.6 Rekomendacji M KNF),
- zasady etycznego postępowania w prowadzeniu działalności bankowej,

[14] Banki nie zawsze uznają, że obszar udzielania kredytów powinien znajdować się w zakresie szczególnej uwagi funkcji compliance przypisanej komórce compliance, ze względu na dublowanie zadań pracowników najniższego szczebla, departamentu prawnego oraz audytu wewnętrznego.

[15] Czasami w bankach wydzielona jest do tego odrębna komórka.

- przyjmowanie zgłoszeń, postępowanie wyjaśniające, wypracowanie standardów chroniących pracowników zgłaszających nieprawidłowości (w tym *whistleblowing*),
- w przypadku podlegania dyrektywie MiFID w banku (w szczególności: klasyfikacja klientów, testy odpowiedniości i adekwatności, obowiązki informacyjne, świadczenie usług doradztwa inwestycyjnego, zarządzanie konfliktami interesów),
- rozwijanie nowych modeli biznesowych lub tworzenie nowych produktów, w szczególności pod kątem przeciwdziałania obchodzeniu powszechnie obowiązujących przepisów (rekomendacja 14.6 Rekomendacji M KNF),
- zagadnienia dotyczące konfliktów interesów, darowizn i podarunków (tzw. gifty), transakcje własne,
- nadużycia na rynku,
- reklama produktów i usług bankowych,
- procedura *Know Your Customer*,
- outsourcing,
- przeciwdziałanie korupcji,
- ochrona danych osobowych,
- ochrona konsumenta i przeciwdziałanie nieuczciwej konkurencji, analiza wzorców umów, w szczególności pod kątem niedozwolonych klauzul umownych (tzw. klauzul abuzywnych),
- prawo pracy, w tym zwłaszcza mobbing i molestowanie w pracy.

PROCES ZARZĄDZANIA RYZYKIEM BRAKU ZGODNOŚCI

Funkcja compliance, jak wcześniej wskazano, bazuje na modelu COSO, zaś system zarządzania poszczególnymi rodzajami ryzyka w banku bazuje na modelu COSO-ERM. Oba te systemy są dosyć podobne i różnią się od systemu zarządzania ryzykiem np. wedle ISO 31000, choćby skupianiem się na kontroli, czyli obniżaniu ryzyka, a nie na traktowaniu ryzyka w bardziej zróżnicowany sposób jak np. jego unikanie czy akceptacja. Wynika to wprost z ostrożnościowego charakteru norm i wytycznych odnośnie systemu kontroli wewnętrznej i zarządzania ryzykiem, wedle których ryzyko rozumieć należy jako groźbę (*hazard risk*), a nie szansę (*opportunity risk*). Proces zarządzania ryzykiem braku zgodności, według uchwały Nr 258/2011 KNF, skupia się na identyfikacji ryzyka (§ 24 ust. 2). Wszystkie pozostałe, poszczególne elementy zarządzania ryzykiem braku zgodności należy więc wywieść z § 12 uchwały Nr 258/2011 KNF, który opisuje podstawowe elementy każdego procesu zarządzania ryzykiem w banku. Na proces zarządzania ryzykiem braku zgodności w banku składają się więc następujące po sobie elementy takie jak: identyfikacja, ocena, kontrola, monitorowanie oraz, nie wymienione w ww. uchwale, ale równie ważne raportowanie.

Pierwszym elementem zarządzania ryzykiem braku zgodności jest **identyfikacja** ryzyka. Identyfikacja ryzyka pozwala na wstępne zlokalizowanie obszarów ryzyka, które następnie zostaną poddane analizie/ocenie/szacowaniu. Kluczowy dla identyfikacji ryzyka jest sformalizowany dostęp do istotnych źródeł informacji, w tym przede wszystkim takich, jak:

- raporty, rejestry, ewidencje innych departamentów/stanowisk w banku, w tym w szczególności rejestr ryzyka operacyjnego, skargi klientów, zalecenia pokontrolne nadzorcy,
- anonimowe źródło powiadamiania o nadużyciach/niezgodności (tzw. *whistleblowing*), w przypadku, gdy takie źródło informacji zostało przewidziane w banku,
- źródła informacji wynikające z monitorowania otoczenia prawnego oraz reakcje akcjonariuszy i interesariuszy.

Drugim elementem zarządzania ryzykiem braku zgodności jest **ocena** zwana też analizą, pomiarem albo szacowaniem ryzyka. Po zidentyfikowaniu ryzyka w określonych obszarach, bądź w związku z konkretną regulacją (np. wejściem w życie określonej nowelizacji ustawy, Rekomendacji KNF), należy ocenić/przeanalizować/oszacować poziom ryzyka braku zgodności. Ryzyko zgodności jest ryzykiem trudnomierzalnym. Nie oznacza to jednak, iż jest ono zupełnie niemierzalne, ale jedynie, że w jego ocenie metody jakościowe przeważają nad metodami ilościowymi. Stąd tak kluczową rolę pełnią pracownicy komórki zgodności. Istotą tego elementu procesu zarządzania ryzykiem jest nadanie określonych poziomów zidentyfikowanemu ryzyku (np. poziom wysoki, średni, niski) w oparciu o sformalizowaną procedurę. Do katalogu przykładowych metod i technik należą:

- mapy ryzyka,
- analiza scenariuszowa,
- profile ryzyka i odchylenia,
- wskaźniki ryzyka (KRI – *key risk indicators*) i wykonania (KPI – *key performance indicators)*.

Kontrola ryzyka, czyli stosowanie środków/mechanizmów kontrolnych, środków/mechanizmów ograniczających ryzyko, to trzeci, często niestety pomijany, etap zarządzania ryzykiem braku zgodności, który wydaje się kluczowym elementem całego procesu. Samo zidentyfikowanie i oszacowanie ryzyka wskazuje jedynie na obszary, gdzie owe ryzyko jest najwyższe, a więc ma charakter głównie informacyjny. Dopiero poprzez środki/mechanizmy kontrolne bank podejmuje wysiłek, aby zidentyfikowane i oszacowane ryzyko ewentualnie zmniejszyć. Katalog metod i rodzajów środków/mechanizmów kontrolnych wzięty jest wprost z tradycyjnych rozwiązań systemu kontroli wewnętrznej i powinien być stosowany odpowiednio:

- podział obowiązków,
- autoryzacja i zatwierdzenia (np. akceptacja wzorców umów),
- kontrola dostępu i kontrola fizyczna,
- weryfikacja,
- nadzór przełożonego,
- rejestr odstępstw,
- szkolenia.

Monitorowanie ryzyka braku zgodności/zarządzania ryzykiem braku zgodności, jako kolejny etap zarządzania ryzykiem braku zgodności, powinno mieć charakter dwojaki. Po pierwsze, powinno się monitorować, czy ustalony na podstawie identyfikacji i oceny/analizy/oszacowania poziom ryzyka się ewentualnie zmniejszył albo powiększył na skutek zastosowanych środków kontrolnych/ograniczających ryzyko braku zgodności. Nie należy tego mylić z identyfikacją ryzyka, która wskazuje na obszary ryzyka przed oceną jego poziomu. Po drugie, monitorowanie należy rozumieć jako czynności kontrolne w stosunku do wcześniejszych etapów procesu zarządzania ryzykiem, a więc identyfikowania, szacowania i stosowania środków kontrolnych. W tym przypadku, monitorowanie pełni funkcję swoistej „metakontroli". Bez informacji o skuteczności i efektywności poprzedzających etapów procesu zarządzania ryzykiem (czy poziom się zmniejszył, czy zwiększył, czy np. identyfikacja jest efektywna), ani zarząd, ani rada nadzorcza nie są w stanie ocenić tejże skuteczności, czy efektywności. Dlatego podwójny charakter monitoringu jest niezbędny. Poniższy katalog metod/technik monitorowania, to przykład najczęściej spotykanych rozwiązań:

- testy zgodności,
- ankiety, w tym ankiety samooceny,
- oceny dojrzałości modelu compliance (tzw. *compliance maturity model*),
- wskaźniki wykonania (np. odsetek przeszkolonych pracowników, rozpatrywanych skarg i wniosków klientów, zakończonych postępowań wyjaśniających, realizacji celów compliance w stosunku do budżetu, tempo wdrażania przepisów i realizacji rekomendacji wewnętrznych oraz zaleceń pokontrolnych nadzorcy).

Raportowanie jest ostatnim elementem zarządzania ryzykiem braku zgodności. W ramach raportowania należy wyróżnić raporty okresowe (miesięczne, kwartalne, roczne) i bieżące, których szczególnym rodzajem są raporty *ad hoc* dotyczące wewnętrznych postępowań wyjaśniających. Raporty, zwłaszcza kwartalne i roczne, powinny być kierowane jednocześnie do rady nadzorczej (komitetu audytu) i zarządu, tak, aby uniknąć problemu filtrowania informacji przez zarząd. Powinny one również stanowić element raportowania całościowej funkcji zapewniania zgodności, wedle rozwiązania przyjętego przez bank.

ZAKOŃCZENIE

Powyższe rozważania stanowią jedynie ogólny zarys funkcji compliance w bankach w Polsce i wskazują podstawowe akty normatywne odnoszące się do tej funkcji. Zgodnie z przedstawionymi uwagami, organizując compliance w banku, należy mieć na uwadze dualizm funkcji compliance, relacje z innymi funkcjami, procesami i komórkami, niezależność oraz wykonywanie wszystkich elementów zarządzania ryzykiem braku zgodności, w tym zwłaszcza jego kontroli. Pełny obraz compliance możliwy jest jednak tylko w ujęciu jednostkowym, na przykładzie danego banku, ze względu na indywidualny poziom ryzyka braku zgodności, na jaki każdy bank jest narażony.

SŁOWNICZEK POJĘĆ

Funkcja compliance w banku – wyodrębniona funkcja w banku mająca za zadanie zapewnianie zgodności działania banku z przepisami prawa, regulacjami wewnętrznymi oraz przyjętymi przez bank standardami postępowania, na którą składa się co najmniej przestrzeganie przepisów prawa, regulacji wewnętrznych i przyjętych przez bank standardów postępowania oraz zarządzanie ryzykiem braku zgodności, doradztwo i raportowanie.

Komisja Nadzoru Finansowego (KNF) – państwowy organ nadzoru, sprawujący nadzór nad sektorem bankowym, rynkiem kapitałowym, ubezpieczeniowym i emerytalnym, nad instytucjami płatniczymi i biurami usług płatniczych oraz nad spółdzielczymi kasami oszczędnościowo-kredytowymi i Krajową Spółdzielczą Kasą Oszczędnościowo-Kredytową. Celem nadzoru nad rynkiem finansowym jest zapewnienie prawidłowego funkcjonowania tego rynku, jego stabilności, bezpieczeństwa oraz przejrzystości, zaufania do rynku finansowego, a także zapewnienie ochrony interesów uczestników tego rynku.

Polityka zgodności w banku – zgodnie z § 24 ust. 2 uchwały Nr 258/2011 KNF, regulacja wewnętrzna banku zawierająca co najmniej podstawowe zasady działania pracowników banku i wyjaśniająca główne procesy identyfikujące ryzyko braku zgodności i umożliwiające zarządzanie ryzykiem braku zgodności na wszystkich szczeblach organizacji banku.

Ryzyko braku zgodności w banku – zgodnie z § 22 ust. 1 uchwały Nr 258/2011 KNF ryzyko rozumiane jako skutki nieprzestrzegania przepisów prawa, regulacji wewnętrznych oraz przyjętych przez bank standardów postępowania.

Zarządzanie ryzykiem braku zgodności w banku – proces zarządzania realizowany na podstawie polityki zgodności oraz innych polityk i procedur dotyczących identyfikacji, oceny (pomiaru), kontroli, monitorowania oraz raportowania o ryzyku braku zgodności.

Komisja Nadzoru Finansowego
Pl. Powstańców Warszawy 1
Skr. poczt. nr 419, 00-950 Warszawa 1
Tel. (+48) 22 262 50 00
Fax (+48) 22 262 51 11
knf@knf.gov.pl
www.knf.gov.pl

ISBN 978-83-63380-99-1