WIERZBOWSKI
EVERSHEDS
SUTHERLAND

Nasze publikacje

Model trzech linii obrony w sektorze bankowym a wymogi organizacyjne funkcji zgodności wedle rozporządzenia 2017/565/UE

Wbrew dość powszechnemu przekonaniu przejście na model trzech linii obrony[1] systemu kontroli wewnętrznej w sektorze bankowym tylko formalnie jest aktem jednorazowym. Faktycznie musi się ono dokonywać za każdym razem, gdy bank implementuje do swoich procesów (zwłaszcza istotnych) kolejne wymogi regulacyjne. System kontroli wewnętrznej obejmuje bowiem nie tylko komórkę audytu wewnętrznego, ale także funkcję kontroli, wpisaną we wszystkie procesy funkcjonujące w banku oraz komórkę do spraw zgodności. Ta ostatnia, zgodnie z Rekomendacją H KNF z 2017 r., pełni w banku podwójną rolę. Po pierwsze, uczestniczy w monitorowaniu pionowym (w ramach funkcji kontroli) mechanizmów kontrolnych zapewniających zgodność procesów funkcjonujących w banku z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi. Po drugie, niejako w imieniu zarządu, zarządza ryzykiem braku zgodności.

Zadanie, przed jakim staje więc bank w przypadku implementacji każdego nowego wymogu regulacyjnego, polega na wpisaniu tegoż wymogu w system kontroli wewnętrznej albo – patrząc z innej perspektywy – na nałożeniu siatki pojęciowej Rekomendacji H KNF np. na język wymogów technicznych i organizacyjnych używany w ramach danego wymogu regulacyjnego. Niniejszy artykuł wskazuje, jak tego dokonać w stosunku do wymogów organizacyjnych firm inwestycyjnych, dotyczących *funkcji zgodności z przepisami,* wskazanych w art. 22 *Rozporządzenia delegowanego Komisji (UE) 2017/565 z dnia 25 kwietnia 2016 r. uzupełniającego Dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do wymogów organizacyjnych i warunków prowadzenia działalności przez firmy inwestycyjne oraz pojęć zdefiniowanych na potrzeby tej dyrektywy* (dalej rozporządzenie 2017/565/UE).

Jednocześnie należy zauważyć, iż rozporządzenie 2017/565/UE nie różnicuje firm inwestycyjnych na banki, o których mowa w art. 70 ust 2 ustawy o obrocie instrumentami finansowymi oraz na banki prowadzące działalność maklerską poprzez biuro maklerskie lub wyodrębnioną jednostkę organizacyjną, tak jak czynią to rozporządzenie Ministra Rozwoju i Finansów z dnia 6 marca 2017 *w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach* (dalej: rozporządzenie SKW) oraz rozporządzenie z dnia 25 kwietnia 2017 r. *w sprawie 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*. Oznacza to, że wymogi organizacyjne z art. 22 rozporządzenia 2017/565/UE spełnić ma każdy bank będący firmą inwestycyjną, a więc również i ten, do którego jednocześnie zastosowanie mają przepisy o systemie kontroli wewnętrznej wedle rozporządzenia SKW oraz Rekomendacji H KNF z 2017.

Zgodnie z art. 22 ust. 1 rozporządzenia 2017/565/UE

> Firmy inwestycyjne ustanawiają, wdrażają i utrzymują odpowiednie strategie i procedury służące **wykrywaniu ryzyka niewypełnienia**

Kontakt do autora

W celu uzyskania dodatkowych informacji prosimy o kontakt:

Dr Łukasz Cichy
Of Counsel
T: +48 22 50 50 733
lukasz.cichy
@eversheds-sutherland.pl

przez firmę jej zobowiązań wynikających z dyrektywy 2014/65/UE oraz zagrożeń, które temu towarzyszą, jak również wprowadzają **odpowiednie środki i procedury, tak by ograniczyć takie ryzyko do minimum** oraz umożliwić właściwym organom skuteczne wykonywanie uprawnień przysługujących im na mocy tej dyrektywy.

Firmy inwestycyjne biorą pod uwagę charakter, skalę i stopień złożoności prowadzonej przez siebie działalności gospodarczej, a także charakter i zasięg usług i działań inwestycyjnych wykonywanych w toku takiej działalności.

Przekładając ten wymóg na język rozporządzenia SKW i Rekomendacji H KNF, nietrudno zauważyć, iż **wykrywanie ryzyka niewypełnienia przez firmę jej zobowiązań wynikających z dyrektywy 2014/65/UE** należy rozumieć jako identyfikację ryzyka braku zgodności, o której mowa w art. 9c ust. 2 pkt 2 ustawy – Prawo bankowe, §37 pkt 4 rozporządzenia SKW oraz rekomendacji 15 Rekomendacji H KNF. Podobnie wprowadzanie odpowiednich środków i procedur tak, żeby ograniczyć ryzyko do minimum, należy rozumieć jako kontrolę ryzyka braku zgodności, o której mowa w art.9c ust. 2 pkt 2 ustawy – Prawo bankowe, czy *też projektowanie i wprowadzanie, bazujących na ocenie ryzyka braku zgodności, mechanizmów kontroli ryzyka braku zgodności*, o którym mowa w §37 pkt 6 rozporządzenia SKW oraz rekomendacji 17 Rekomendacji H KNF. Rozporządzenie 2017/565/UE używa co prawda pojęcia „strategii i procedur", ale katalog mechanizmów kontroli ryzyka braku zgodności jest otwarty i można jako takowe mechanizmy traktować wszelkie działania ograniczające ryzyko braku zgodności. Co ciekawe, w stosunku do ww. rozwiązań krajowych opisany w rozporządzeniu 2017/565/UE proces jest niekompletny, brakuje przede wszystkim oceny ryzyka braku zgodności, albowiem o monitorowaniu i raportowaniu o ryzyku braku zgodności jest mowa w art. 22 ust. 2 tego rozporządzenia. Ważnym rozwiązaniem jest natomiast zwrot „ograniczenia ryzyka do minimum", co oznacza, że unijny prawodawca odwołuje się do koncepcji ryzyka rezydualnego (szczątkowego), jakie zostaje po zastosowaniu mechanizmów kontroli ryzyka. W kontekście ryzyka braku zgodności jest to o tyle ważne, że bardzo często ujęcie regulacyjne zakłada wymóg absolutnej zgodności, nie dopuszczając świadomości, że każde ryzyko, w tym także ryzyko braku zgodności, ma swój element rezydulany. Ponadto, wnioskując *a contrario,* należy zauważyć, że ryzyko braku zgodności nie przynależy do systemu zarządzania ryzykiem, o czym świadczy wprost choćby poświęcony zarządzaniu ryzykiem (innym niż ryzyko braku zgodności) art. 23 rozporządzenia 2017/565/UE.

Zgodnie z art. 22 ust. 2 rozporządzenia 2017/565/UE

2. Firmy inwestycyjne ustanawiają i utrzymują stałą i skutecznie działającą funkcję zgodności z przepisami, która działa niezależnie i odpowiada za:

a) stałe monitorowanie i regularną ocenę adekwatności i skuteczności środków, strategii i procedur wprowadzonych zgodnie z ust. 1 akapit pierwszy oraz działań podjętych w celu wyeliminowania wszelkich nieprawidłowości w wypełnianiu przez firmę jej zobowiązań;

b) doradztwo i pomoc dla osób zaangażowanych odpowiedzialnych za wykonywanie usług i działalności inwestycyjnej, służące wypełnianiu przez firmę jej zobowiązań wynikających z dyrektywy 2014/65/UE;

c) przekazywanie kierownictwu, co najmniej raz do roku, sprawozdań dotyczących wdrażania i skuteczności ogólnego środowiska kontroli w odniesieniu do usług i działalności inwestycyjnej, zidentyfikowanych zagrożeń oraz składania sprawozdań dotyczących rozpatrywania skarg, a także podjętych lub planowanych działań naprawczych;

d) monitorowanie funkcjonowania procesu rozpatrywania skarg i uznawanie skarg za źródło istotnych informacji w kontekście ogólnych obowiązków w zakresie monitorowania

Jak wskazano powyżej „stałe monitorowanie i regularną ocenę adekwatności i skuteczności środków, strategii i procedur… „należy rozumieć jako monitorowanie ryzyka braku zgodności, o którym mowa w art. 9c ust. 2 pkt 2 ustawy – Prawo bankowe, §37 pkt 7 rozporządzenia SKW oraz rekomendacji 18 Rekomendacji H KNF. Co niezwykle istotne, unijny prawodawca wskazał, że monitorowanie i ocena ma dotyczyć zastosowanych już mechanizmów kontroli ryzyka braku zgodności, a więc jest czynnością następującą po wprowadzeniu tychże mechanizmów. Dokładnie w taki sam sposób jest to wskazane w rekomendacji 18.1 Rekomendacji H KNF, wedle której *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).* Częstym problemem banków jest utożsamianie monitorowania z identyfikacją, podczas gdy identyfikacja ryzyka jest działaniem poprzedzającym zastosowanie środków ograniczających ryzyko w postaci mechanizmów kontrolnych, a monitorowanie jest działaniem następującym dopiero po zastosowaniu tych mechanizmów.

W przypadku art. 22 ust. 2b rozporządzenia 2017/565/UE tj. *doradztwie i pomocy* przez komórkę do spraw zgodności, problem prawidłowej implementacji doradztwa do Rekomendacji H KNF został szczegółowo omówiony w artykule „Doradztwo komórki do spraw zgodności i komórki audytu wewnętrznego w świetle projektu Rekomendacji H KNF" w magazynie *Compliance i Zarządzanie* (wiosna 2017) Nie referując szczegółowych uwag z artykułu, należy jedynie wskazać, że najlepszym sposobem adaptacji czynności doradztwa przez komórkę do spraw zgodności jest potraktowanie jej jako mechanizmu kontroli ryzyka braku zgodności.

O ile sam obowiązek *przekazywania kierownictwu, co najmniej raz do roku, sprawozdań* oczywiście wpisuje się w raportowanie o ryzyku braku zgodności, o którym mowa w art. 9c ust. 2 pkt 2 ustawy – Prawo bankowe, §37 pkt 8 rozporządzenia SKW oraz rekomendacji 19 Rekomendacji H KNF, o tyle nieco odmiennie określony jest zakres tego raportowania (sprawozdawczości). Art. 22 ust.2d rozporządzenia 2017/565/UE nakłada bowiem obowiązek *wdrażania i skuteczności ogólnego środowiska kontroli w odniesieniu do usług i działalności inwestycyjnej, zidentyfikowanych zagrożeń oraz składania sprawozdań dotyczących rozpatrywania skarg, a także podjętych lub planowanych działań naprawczych.* Działania naprawcze, tudzież zagrożenia stosunkowo łatwo jest przełożyć na język Rekomendacji H. Te pierwsze, to *środki naprawcze i dyscyplinujące*, o których mowa choćby w rekomendacji 1.5 Rekomendacji H, a te drugie to po prostu ryzyka braku zgodności w określonych procesach funkcjonujących w banku. W przypadku środowiska kontroli należy pamiętać, że samo pojęcie swoją popularność zawdzięcza modelowi systemu kontroli wewnętrznej COSO, i jako takie przeniknęło, często bez wyraźnego zdefiniowania, do różnych krajowych modelów i wymogów regulacyjnych odnośnie systemu kontroli wewnętrznej. Przykładem tego są choćby *Rekomendacje dotyczące funkcjonowania Komitetu Audytu* KNF z 2010 r. Dlatego najlepiej chyba środowisko kontroli (*control environment*) definiować w ślad właśnie za modelem COSO[2].

Najtrudniejszym – nie tyle z punktu widzenia samej Rekomendacji H, co dotychczasowego pojmowania zarządzania ryzykiem braku zgodności – jest obowiązek *monitorowania funkcjonowania procesu rozpatrywania skarg i uznawanie skarg za źródło istotnych informacji w kontekście ogólnych obowiązków w zakresie monitorowania,* o którym mowa w art. 22 ust. 1d rozporządzenia 2017/565/UE. Trudno bowiem zakwalifikować samo monitorowanie *rozpatrywania skarg* jako któryś z elementów zarządzania ryzykiem braku zgodności, polegającego na identyfikacji, ocenie, kontroli, monitorowaniu i raportowaniu o ryzyku braku zgodności. Monitorowanie ryzyka braku zgodności polega bowiem, o czym była mowa powyżej, na monitorowaniu spadku lub wzrostu **poziomu ryzyka** braku zgodności już po zastosowaniu mechanizmów kontroli ryzyka braku zgodności. Z pomocą przychodzi jednak tzw. funkcja kontroli, a konkretnie zapewnianie zgodności w ramach funkcji kontroli przez komórkę do spraw zgodności. Zgodnie bowiem z rekomendacją 13.4 Rekomendacji H KNF *Zakres dokonywanej przez komórkę do spraw zgodności weryfikacji bieżącej pionowej może obejmować w szczególności weryfikację przestrzegania mechanizmów*

kontrolnych (np. procedur), przez pierwszą linię obrony w takich obszarach ***jak skargi i reklamacje****.* Jako że weryfikacja bieżąca jest elementem monitorowania, toteż wymóg monitorowania *funkcjonowania procesu rozpatrywania skarg* będzie oczywiście spełniony. Podobnie w przypadku *uznawanie skarg za źródło istotnych informacji w kontekście ogólnych obowiązków w zakresie monitorowania* zastosować można wprost rekomendację 15.2d Rekomendacji H, wedle której *Do podstawowych informacji wykorzystywanych w ramach identyfikacji ryzyka braku zgodności powinny należeć co najmniej ustalenia dokonane przez komórkę do spraw zgodności, w związku z bieżącą weryfikacją oraz testowaniem, wykonywanymi przez tę komórkę.*

Nieco kłopotliwy w interpretacji może być obowiązek wskazany w akapicie drugim art. 22 ust. 2 rozporządzenia 2017/565/UE, zgodnie z którym *Aby zapewnić zgodność z lit. a) i b) niniejszego ustępu, funkcja zgodności z przepisami przeprowadza ocenę, na podstawie której ustala oparty na ryzyku program monitorowania, w którym uwzględnia się wszystkie obszary świadczonych przez firmę inwestycyjną usług i działalności inwestycyjnej oraz właściwych usług dodatkowych, w tym istotne informacje zgromadzone w odniesieniu do monitorowania rozpatrywania skarg. W programie monitorowania ustala się priorytety określone na podstawie oceny ryzyka zgodności, zapewniając całościowe monitorowanie ryzyka zgodności.*

Wydaje się, że ocena *na podstawie której ustala oparty na ryzyku program monitorowania* bynajmniej nie powinna być traktowana jako ocena ryzyka braku zgodności, będącą jednym z kluczowych elementów zarządzania ryzykiem braku zgodności, o którym mowa w mowa w art. 9c ust. 2 pkt 2 ustawy – Prawo bankowe, §37 pkt 5 rozporządzenia SKW oraz rekomendacji 15 Rekomendacji H KNF. Ocena, *na podstawie której ustala oparty na ryzyku program monitorowania,* powinna być traktowana analogicznie jak analiza ryzyka sporządzania na potrzeby badania audytowego, o czym mowa §38 pkt 4 rozporządzenia SKW oraz rekomendacji 25.2 i 26.1e Rekomendacji H KNF. Analiza ryzyka, której wynikiem jest konkretna ocena tego ryzyka sporządzana jest po to, aby dokonać wyboru, które konkretnie obszary i procesy powinny być badane przez komórkę audytu wewnętrznego z największą częstotliwością. Pamiętając jednocześnie, że zgodnie z rekomendacją 8.5c Rekomendacji H KNF zakres testowania, a więc elementu monitorowania, powinien uwzględniać ryzyko zaistnienia nieprawidłowości, co jest analogiczne do ww. analizy ryzyka na potrzeby badania audytowego, łatwo zauważyć, że to właśnie o tego rodzaju ryzyko chodzi w akapicie drugim art. 22 ust. 2 rozporządzenia 2017/565/UE. Innymi słowy, zarówno monitorowanie wedle model trzech linii obrony Rekomendacji H, jak i monitorowanie wedle rozporządzenia 2017/565/UE, nie powinno być obarczone całkowitą dowolnością, a poprzedzone analizą ryzyka przeprowadzoną na potrzeby tegoż monitorowania.

W przypadku art. 22 ust. 3 rozporządzenia 2017/565/UE, gdzie mowa o statusie komórki do spraw zgodności, status ten jest analogicznie zapewniany mocą rozporządzenia SKW oraz Rekomendacji H. Wymóg szeroko rozumianych odpowiednich zasobów, o których mowa w art. 22 ust. 3a rozporządzenia 2017/565/UE określony jest także w §40 ust. 2 rozporządzenia SKW. Podobnie jak wymóg wyboru kierującego komórką do spraw zgodności, który wskazany jest zarówno w art. 22 ust. 3b rozporządzenia 2017/565/UE, jak i wynika z §39 ust. 6 i 7 rozporządzenia SKW. Z kolei obowiązek raportowania o istotnym ryzyku, co przewiduje art. 22 ust. 3c rozporządzenia 2017/565/UE, wskazany jest wprost w rekomendacji 19.2 Rekomendacji H, która stanowi, iż 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*. Zakaz uczestniczenia w czynnościach, które są monitorowane (tzw. zakaz kontroli samego siebie) jest wprost wskazany w art. 22 ust. 3c rozporządzenia 2017/565/UE i jednocześnie leży u podstaw całego podziału na model 3 linii obrony oraz koncepcji monitorowania pionowego, o czym mowa w rekomendacji 6.4 Rekomendacji H. Podobnie w przypadku wynagrodzenia, które zgodnie art. 22 ust. 3c rozporządzenia 2017/565/UE nie powinno wpływać ani faktycznie ani potencjalnie na obiektywizm pracowników komórki do spraw zgodności. Zapis mający ten sam cel przewidziany jest choćby w §39 ust. 8 rozporządzenia SKW.

Jedyną rozbieżnością między rozporządzeniem 2017/565/UE a rozporządzeniem SKW jest niemożliwość odstąpienia od wymogów organizacyjnych wskazanych w art. 22 ust. 3d i e rozporządzenia 2017/565/UE, albowiem rozporządzenie SKW takiego odstąpienia nie przewiduje.

Reasumując wymogi organizacyjne, o których mowa w art. 22 rozporządzenia 2017/565/UE są wręcz zadziwiająco zbieżne z wymogami modelu trzech linii obrony w sektorze bankowym, co z jednej strony zdecydowanie ułatwia ich adaptację, a z drugiej wskazuje pewien wspólny kierunek, ku któremu podąża unijny i polski prawodawca oraz regulator krajowy w sektorze bankowym.

Lipiec, 2017

[1] Model trzech linii obrony został wprowadzony mocą art. 9c ustawy- Prawo bankowe, Rozporządzeniem Ministra Rozwoju i Finansów z dnia 6 marca 2017 *w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach* oraz Rekomendacją H KNF dotyczącą systemu kontroli wewnętrznej w bankach, którą banki powinny implementować najpóźniej do 31 grudnia 2017r.

[2] Zgodnie z definicją COSO, INTERNAL CONTROL – INTEGRATED FRAMEWORK, 1994, s. 4
Control Environment — The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.