WYTYCZNE ESMA DLA FUNKCJI COMPLIANCE ROK 2021

Zagadnienia ogólne oraz propozycje wdrożeniowe

CZ I

Implementacja Wytycznych 2021 powinna znaleźć się w kręgu zainteresowania funkcji compliance w domach maklerskich, biurach maklerskich, bankach[8], funduszach inwestycyjnych czy ZAFI.

ZAŁOŻENIA OGÓLNE

Po ponad trzech latach od wejścia w życie pakietu MiFID II (co do zasady z pewnymi wyjątkami wszedł w życie w dniu 3 stycznia 2018 r.) oraz po prawie 9 latach od czasu publikacji pierwszych *Wytycznych w sprawie określonych aspektów wymogów dyrektywy MiFID dotyczących komórki ds. nadzoru zgodności z prawem*[1] (**dalej jako:** Wytyczne 2012), ESMA[2] zaserwowała nam nowe Wytyczne[3] (**dalej jako:** Wytyczne 2021). Tak jak przy dokumencie Wytycznych z 2012 roku pozwoliłem sobie na analizę wdrożeniową[4], tak i przy obecnym postanowiłem zaproponować możliwości wdrożeniowe w firmie inwestycyjnej ale także na potrzeby funkcji compliance dla banków z art. 70 ust 2 ustawy o obrocie[5].

Zacznijmy od kwestii technicznych – Wytyczne 2021 mają 27 stron, podzielone są tematycznie podobnie do Wytycznych 2012 tj. ze „starej" (chociaż często znacząco rozbudowanej) tematyki mamy ocenę ryzyka braku zgodności, obowiązki komórki ds. nadzoru zgodności z prawem w zakresie monitorowania, obowiązki sprawozdawcze komórki ds. nadzoru zgodności z prawem, obowiązki komórki ds. nadzoru zgodności z prawem w zakresie doradztwa (w Wytycznych 2012 jako *„obowiązki komórki ds. nadzoru zgodności z prawem w zakresie doradztwa i pomocy"*), skuteczność komórki ds. nadzoru zgodności z prawem, stałość komórki ds. nadzoru zgodności z prawem, niezależność komórki ds. nadzoru zgodności z prawem, zwolnienia (w Wytycznych 2012 jako *„proporcjonalność w odniesieniu do skuteczności komórki ds. nadzoru zgodności z prawem"*), zapewnienie zgodności komórki ds. nadzoru zgodności z prawem z innymi komórkami ds. kontroli wewnętrznej (wcześniej jako *„łączenie(...)"*), outsourcing komórki ds. nadzoru zgodności z prawem, przegląd komórki ds. nadzoru zgodności z prawem przez właściwe organy. **Zupełną nowością** jest rozdział/wytyczne w zakresie umiejętności, wiedzy, wiedzy fachowej i autorytetu komórki ds. nadzoru zgodności z prawem. Szkoda nieco, że ESMA nie zdecydowała się na załączniki do Wytycznych 2021, analogicznie jak np. w *Wytycznych w sprawie zasad i praktyk dotyczących wynagrodzeń (MiFID)*[6] z 3 czerwca 2013 r. (ESMA/2013/606), w których zostałby opisane przykłady dobrych i niewłaściwych praktyk w zakresie funkcji compliance i zasad jej działania. Wytyczne 2021 oparte są, jak i inne wytyczne ESMA, na zasadzie proporcjonalności, ***comply or explain*** – ESMA oczekuje, że podmioty zobowiązane dołożą należytej staranności aby wdrożyć Wytyczne 2021[7].

Wytyczne 2021 mają zastosowanie do:

- firm inwestycyjnych świadczących usługi inwestycyjne lub prowadzących działalność inwestycyjną lub dokonujących sprzedaży bądź doradzających klientom w zakresie lokat strukturyzowanych (**np. domy maklerskie, biura maklerskie**);
- instytucji kredytowych świadczących usługi inwestycyjne lub prowadzących działalność inwestycyjną lub dokonujących sprzedaży bądź doradzających klientom w zakresie lokat strukturyzowanych (**tu moim zdaniem należy to czytać także jako banki z art. 70 ust. 2 ustawy o obrocie**);
- przedsiębiorstw zbiorowego inwestowania w zbywalne papiery wartościowe (UCITS) w zakresie świadczenia usług, o których mowa w art. 6 ust. 3 dyrektywy UCITS, zgodnie z art. 6 ust. 4 tej dyrektywy;
- zarządzających alternatywnymi funduszami inwestycyjnymi (ZAFI) w zakresie świadczenia usług, o których mowa w art. 6 ust. 4 dyrektywy w sprawie ZAFI, zgodnie z art. 6 ust. 6 tej dyrektywy.

PROPOZYCJE WDROŻENIOWE

Zanim przejdę do konkretnych propozycji wdrożeniowych warto zauważyć, że nie są i nie mogą one być dostosowane do każdego typu i rozmiaru organizacji – inaczej pewne kwestie będą adresowane w domu maklerskim zatrudniającym 50 osób i świadczącym trzy rodzaje usług maklerskich a inaczej w banku zatrudniającym kilka tysięcy pracowników, który działa zarówno jako bank prowadzący działalność maklerską (biuro maklerskie), jak również jako bank z art. 70 ust. 2 ustawy o obrocie.

1. Pkt. 13 Wytycznych 2021: *W ramach swojej odpowiedzialności za zapewnienie wypełniania przez firmę obowiązków wynikających z dyrektywy MiFID II, kadra kierownicza wyższego szczebla jest zobowiązana dopilnować, żeby komórka ds. nadzoru zgodności z prawem wypełniała wymogi określone w art. 22 rozporządzenia delegowanego MiFID II.*

Zerknijmy najpierw do czego odnosi się wspominany w wytycznej art. 22 rozporządzenia 565/2017[9]. Wskazany artykuł ustanawia ramy dla funkcji zgodności z przepisami (compliance) – w ust. 1 stanowi, że firmy (rozumiane w niniejszym artykule jako wszystkie podmioty wskazane obowiązane do wdrożenia Wytycznych 2021 w szczególności domy i biura maklerskie oraz banki) ustanawiają, wdrażają i utrzymują odpowiednie strategie i procedury służące wykrywaniu ryzyka niewypełnienia przez firmę jej zobowiązań wynikających z MiFID II oraz zagrożeń, które temu towarzyszą, jak również wprowadzają odpowiednie środki i procedury, tak by ograniczyć takie ryzyko do minimum (...). Zatem można w zasadzie wskazać, że pkt. 13 Wytycznych 2021 jest niczym innym aniżeli niejako przepisaniem w nieco innej formie art. 22 rozporządzenia 565/2017.

Jak wdrożyć? W odpowiednie postanowienia wewnętrznych aktów normatywnych z zakresu compliance (np. regulamin organizacyjny) wpisać jako zadania tej komórki właśnie te wskazane w art. 22 rozporządzenia 565/2017, dodatkowo wpisać te zadania np. do podziału kompetencji pomiędzy członków zarządu firmy oraz zobowiązać funkcję compliance (czy to w formie uchwały czy innego wewnętrznego aktu normatywnego, co jest rozwiązaniem bezpieczniejszym) do cyklicznego raportowania w tej materii, tak by np. zarząd firmy mógł wykazać, że faktycznie *„dopilnował wypełniania wymogów przez compliance"*

2. Wytyczna nr 1 - Wytyczna dotycząca oceny ryzyka braku zgodności z prawem:

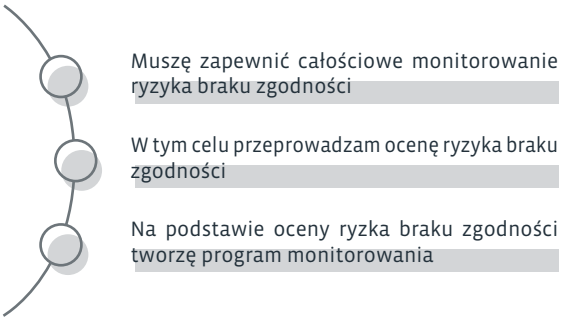
a. Pkt. 14: *Zgodnie z art. 22 ust. 2 rozporządzenia delegowanego MiFID II komórka ds. nadzoru zgodności z prawem przeprowadza w ramach swoich zadań ocenę ryzyka w celu zapewnienia całościowego monitorowania ryzyka braku zgodności.*

Na podstawie przeprowadzonej oceny ryzyka braku zgodności komórka ds. nadzoru zgodności z prawem ustanawia program monitorowania oparty na ocenie ryzyka w celu określenia swoich priorytetów i ukierunkowania działań w zakresie monitorowania, doradztwa i pomocy.

b. Pkt. 15: *Ustalenia z oceny ryzyka braku zgodności powinny być wykorzystywane do określenia programu prac komórki ds. nadzoru zgodności z prawem i efektywnego przydziału zasobów komórki. Ocena ryzyka braku zgodności powinna być poddawana regularnemu przeglądowi i, w razie konieczności, aktualizowana, aby zapewnić aktualność celów, ukierunkowania i zakresu działań służących monitorowaniu zgodności i działań doradczych*

c. Pkt. 16: *Artykuł 22 ust. 1 akapit drugi rozporządzenia delegowanego MiFID II wymaga, aby określając poziom ryzyka braku zgodności, na jakie narażona jest firma, komórka ds. nadzoru zgodności z prawem uwzględniała wszystkie obszary usług inwestycyjnych, działalności inwestycyjnej i usług dodatkowych firmy.*

Powyższe dotyczy rodzajów będących przedmiotem obrotu i dystrybuowanych instrumentów finansowych, kategorii klientów firmy, kanałów dystrybucji oraz, w stosownych przypadkach, wewnętrznej organizacji grupy.



Oznacza to, co uszczegółowię w omawianiu kolejnych wytycznych, że jednym z **podstawowych obowiązków** compliance powinno być kompleksowe monitorowanie ryzyka braku zgodności, zaś **podstawowym narzędziem** do wypełniania tego zadania powinna być cykliczna ocena ryzyka braku zgodności, całościowa ale też np. per linie produktowe, biznesowe, usługi maklerskie etc. – im bardziej szczegółowa tym dokładniejsza będzie ocena. Dodatkowo funkcja compliance na bazie oceny powinna ustanowić program monitorowania w celu określenia swoich priorytetów.

Jak wdrożyć? W odpowiednie postanowienia wewnętrznych aktów normatywnych z zakresu compliance (np. regulamin organizacyjny lub inne) wpisać jako podstawowe zadanie monitorowanie ryzyka braku zgodności. Dodatkowo wdrożyć w wewnętrznych aktach normatywnych takie pojęcia jak ocena ryzyka braku zgodności (np. wykonywana kompleksowo i holistycznie raz do roku oraz comiesięczna) oraz narzędzie jakim jest program monitorowania.

W mojej opinii program monitorowania może być świetnym narzędziem służącym nie tylko do określenia priorytetów na dany rok/półrocze/kwartał ale także do bieżącej oceny ryzyka braku zgodności – wtedy w przypadku np. podwyższenia w danym miesiącu oceny ryzyka braku zgodności może to zostać uwzględnione w programie monitorowania. Docelowo ustalenia i wyniki z całego roku z oceny ryzyka braku zgodności odzwierciedlone w programie monitorowania są niemalże gotowym materiałem do raportowania do organów zarządczych. Warto wskazać, że bardzo przydatnym narzędziem są dziś metodyki np. określające jak program monitorowania będzie wypełniany, jakie pola się tam znajdą, co będziemy badać co miesiąc, co co kwartał itp. Brak takiej metodyki to nie tylko znacząco zwiększone ryzyko błędów ludzkich ale także ryzyko braku zastępowalności i powtarzalności czyli tzw. wiedzy o organizacji.

d. Pkt. 17: *W ocenie ryzyka braku zgodności należy uwzględniać obowiązki wynikające z MiFID II, krajowe przepisy wykonawcze oraz polityki, procedury, systemy i mechanizmy kontrolne wdrożone w firmie w obszarze usług inwestycyjnych i działalności inwestycyjnej.*

W ocenie należy również uwzględnić wyniki działań monitorujących i wszelkie istotne ustalenia audytu wewnętrznego lub zewnętrznego

Wytyczna w tym punkcie uszczegóławia wskazany w pkt. 14 obowiązek stanowiący, że compliance przeprowadza w ramach swoich zadań ocenę ryzyka w celu zapewnienia całościowego monitorowania ryzyka braku zgodności.

Jak wdrożyć? Zatem do oceny ryzyka inherentnego[10] powinny być brane pod uwagę przepisy systemu MiFID II (zatem zarówno sama Dyrektywa, Rozporządzenie MiFIR jak również RTSy/ITSy[11] i wytyczne ESMA), także polskie akty prawne implementujące właściwe przepisy systemu MiFID II (tu widziałbym miejsce także dla stanowisk KNF). W ocenie ryzyka rezydualnego[12] zaś widziałbym wewnętrzne akty normatywne firmy oraz wdrożone mechanizmy kontrolne *(polityki, procedury, systemy i mechanizmy kontrolne wdrożone w firmie w obszarze usług inwestycyjnych i działalności inwestycyjnej)*. Wreszcie ocena ryzyka rezydualnego powinna uwzględniać wyniki działań monitorujących (pierwszej i drugiej linii) i wszelkie istotne ustalenia audytu wewnętrznego lub zewnętrznego (w tym np. kontroli KNF).

Poniżej najprostsza propozycja oceny ryzyka dla fikcyjnej firmy świadczącej usługę doradztwa inwestycyjnego z wykrytymi pewnymi nieprawidłowościami:

Rodzaj działalności	Ocena ryzyka inherentnego	Stosowane mechanizmy kontrolne	Ocena mechanizmów kontrolnych
Świadczenie przez dom maklerski usługi doradztwa inwestycyjnego zależnego	**M-H** (medium-high), jako wynikowa zainteresowania KNF i znacznej ilości przepisów MiFID dotykających tej materii	1. Szkolenia pracowników 2. Nagrywanie rozmów 3. Notatki ze spotkań z klientami 4. Wewnętrzna certyfikacja	Do poprawy = M-L (zdarzają się sytuacje w których pracownicy świadczą usługę doradztwa inwestycyjnego niezgodnie z profilem klienta)

Ustalenia audytu wewnętrznego	Ustalenia audytu zewnętrznego	Ocena ryzyka rezydualnego	Proponowane środki naprawcze
N/A	KNF uznała, że zdarzają się sytuacje w których pracownicy świadczą usługę doradztwa inwestycyjnego niezgodnie z profilem klienta	**M-H** (medium-high) - ryzyko inherentne na poziomie M-H oraz nieprawidłowości w świadczeniu usług	[w zależności od tego jak działa firma]

e. Pkt. 18: *Zidentyfikowane rodzaje ryzyka należy poddawać zarówno regularnemu, jak i w razie potrzeby doraźnemu przeglądowi w celu zagwarantowania, że uwzględnione zostaną wszelkie pojawiające się rodzaje ryzyka (na przykład wynikające z nowych obszarów działalności, innych zmian w strukturze firmy lub zmian obowiązujących ram prawnych)*

Jak wdrożyć? Wpisać odpowiednie postanowienia w wewnętrznych aktach normatywnych oraz wspomnianej wcześniej metodyce – można spokojnie do tego użyć programu monitorowania.

3. Wytyczne nr 2 - Wytyczne dotyczące obowiązków komórki ds. nadzoru zgodności z prawem w zakresie monitorowania:

a. Pkt. 19: *Celem programu monitorowania opartego na analizie ryzyka powinna być ocena, czy działalność firmy inwestycyjnej jest prowadzona zgodnie z jej obowiązkami wynikającymi z dyrektywy MiFID II oraz czy jej wewnętrzne polityki i procedury, środki organizacyjne oraz kontrolne pozostają skuteczne i właściwe, zapewniając całościowe monitorowanie ryzyka braku zgodności*

Obowiązek posiadania i wdrożenia programu monitorowania wynika nie tylko z omówionego wcześniej pkt. 14 Wytycznych 2021 ale także z wspomnianego art. 22 ust. 2 rozporządzenia 565/2017, który stanowi że *„(...)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.”.*

Jak wdrożyć?

1. Firma musi ustanowić dokument/narzędzie jakim jest program monitorowania.
2. Jest to obowiązek nie tylko domów maklerskich czy biur maklerskich ale także banków z art. 70 ust. 2 ustawy o obrocie.
3. Program monitorowania musi ustanowić i wdrożyć funkcja compliance.
4. Program monitorowania musi być oparty na analizie ryzyka (Wytyczne 2021; przepis art. 22 rozporządzenia 565/2017 używa mniej dokładnego sformułowania *„oparty na ryzyku”*).
5. Wszystkie usługi inwestycyjne i usługi dodatkowe muszą być uwzględnione w programie monitorowania.
6. Ocena dokonywana w programie monitorowania musi uwzględniać wnioski z analizy skarg (przy czym w mojej opinii nie analiza skarg nie musi być wykonywana przez funkcję compliance).
7. Program monitorowania jest wynikową oceny ryzyka.
8. Na bazie oceny ryzyka w programie monitorowania ustala się priorytety (jak to zrobić podpowiadam poniżej).

Ocena ryzyka (4 stopnie) = wynik oceny ryzyka rezydualnego	Stopień istotności w programie monitorowania
H	1
M-H	2
M-L	3
L	4

Ocena ryzyka (3 stopnie) = wynik oceny ryzyka rezydualnego	Stopień istotności w programie monitorowania
H	1
M	2
L	3

Takie „zgranie" oceny ryzyka (omawianej wcześniej) z programem monitorowania realizuje w mojej opinii cele, na realizacji których najbardziej zależało ustawodawcy i regulatorowi. Stopień istotności „1" to rzecz jasna taki, któremu poświęcimy najwięcej uwagi, czasu i zaangażowania, jako takiemu który wynika z oceny ryzyka rezydualnego „H" (wysokiej). Dla pozostałych ocen ryzyka rezydualnego stopień istotności przykłada się odpowiednio.

b. Pkt. 20: *W przypadku gdy firma stanowi część grupy, odpowiedzialność za komórkę ds. nadzoru zgodności z prawem spoczywa na każdej firmie w obrębie grupy.*

Każda z firm powinna zatem zagwarantować, żeby jej komórka ds. nadzoru zgodności z prawem pozostawała odpowiedzialna za monitorowanie własnego ryzyka braku zgodności.

Powyższe dotyczy, między innymi, sytuacji, w których firma zleca wykonywanie zadań w zakresie zgodności innej firmie w grupie.

Komórki ds. nadzoru zgodności z prawem w poszczególnych firmach powinny jednak mieć na uwadze grupę, do której należą, współpracując ściśle z pracownikami komórek ds. audytu, prawnych, regulacyjnych i nadzoru zgodności z prawem z innych części grupy.

Wytyczna jest raczej oczywista, co ciekawe wskazuje się, że dla grup kapitałowych odpowiedzialność za compliance spoczywa oddzielnie dla każdej z firm w ramach grupy kapitałowej, aczkolwiek ze wskazaniem, że compliance poszczególnych firm w ramach grupy powinno ze sobą współpracować (także z audytem, komórkami prawnymi itp.).

c. Pkt. 21: *Podstawę określenia właściwych narzędzi i metodyk wykorzystywanych przez komórkę ds. nadzoru zgodności z prawem, jak również zakresu programu monitorowania oraz częstotliwości działań monitorujących prowadzonych przez komórkę ds. nadzoru zgodności z prawem (okresowych, doraźnych lub ciągłych) powinno stanowić podejście do nadzoru zgodności z prawem oparte na ocenie ryzyka.*

Komórka ds. nadzoru zgodności z prawem powinna również zagwarantować, żeby jej działania monitorujące nie ograniczały się do badania dokumentacji, ale obejmowały również weryfikację wdrażania polityk i procedur w praktyce, na przykład poprzez kontrole na miejscu prowadzone w operacyjnych jednostkach organizacyjnych.

Komórka ds. nadzoru zgodności z prawem powinna także rozważyć zakres przeglądów, które należy prowadzić.

Zdanie pierwsze wskazuje na kilka istotnych faktów. Po pierwsze compliance powinno mieć (wdrożyć) metodyki (na co wskazywałem powyżej) oraz narzędzia. Po drugie compliance powinno określić swoje podejście do nadzoru zgodności z prawem oparte na ocenie ryzyka (~apetyt na ryzyko), z którego powinien wynikać zakres programu monitorowania oraz częstotliwości działań monitorujących (ESMA wskazuje, że modelowym rozwiązaniem mogą być działania monitorujące z częstotliwością okresową, doraźną lub ciągłą).

Jak wdrożyć? Odpowiednie zapisy w wewnętrznych aktach normatywnych, do tego opracowanie metodyk, kończąc na faktycznym wykonywaniu zadań w oparciu o nastawienie do ryzyka. Do tego można rozważyć oszacowanie apetytu na ryzyko firmy.

d. Pkt. 22: *Wśród odpowiednich narzędzi i metod prowadzenia działań monitorujących, które może wykorzystywać komórka ds. nadzoru zgodności z prawem, można wymienić między innymi:*

- *(a) wykorzystanie miar zagregowanego ryzyka (na przykład wskaźników ryzyka);*
- *(b) wykorzystanie (dodatkowych) sprawozdań wymagających uwagi kierownictwa, dokumentowanie istotnych rozbieżności między wynikami rzeczywistymi a oczekiwaniami (raport niezgodności) lub sytuacji wymagających rozwiązania (rejestr problemów);*
- *(c) ukierunkowany nadzór nad transakcjami, obserwację procedur, badanie dokumentów lub rozmowy ze stosownymi pracownikami lub, w razie potrzeby, i według uznania komórki ds. nadzoru zgodności z prawem, odpowiedniej próby klientów firmy;*

Jedna z najciekawszych wytycznych, pokazująca, że nawet na tak „wysokim" poziomie, jakim jest poziom wytycznych regulacyjnych kierowanych do rynku, możemy znaleźć konkretne i przydatne narzędzia do codziennej pracy.

Jak wdrożyć? ESMA wskazuje, że jako compliance powinniśmy korzystać z miar zagregowanego ryzyka, na przykładzie wskaźników ryzyka[13]. O ile punkty (b) i (c) powyżej nie powinny w żaden sposób nastręczać problemów wdrożeniowych o tyle pkt. (a) jest nie tylko najciekawszym ale także najtrudniejszym do wdrożenia punktem. Czym są wskaźniki ryzyka, które częściej bywają nazywane Kluczowymi Wskaźnikami Ryzyka (*Key Risk Indicators* – KRI)? W naszym przypadku, dla funkcji compliance, KRI są miarą wrażliwości firmy na zagrożenia związane z ryzykiem braku zgodności. Jak dla ryzyka operacyjnego wskazuje M.Thlon *„KRI występują w postaci statystyk odzwierciedlających dane empiryczne z poszczególnych okresów. Służą do monitorowania ekspozycji na ryzyko i – co najistotniejsze – umożliwiają podjęcie działań wyprzedzających, szczególnie chroniących przed najbardziej dotkliwymi zdarzeniami operacyjnymi”*[14].

Zatem posiłkując się cytowaną definicją można wskazać, że dla ryzyka braku zgodności KRI także będą występować w postaci różnego rodzaju statystyk, które będą służyć funkcji compliance do detekcji symptomów zwiększania się możliwości materializacji ryzyka braku zgodności.

Wyobraźmy sobie zatem hipotetyczny przykład banku oferującego swe usługi dla klientów konsumentów (detalicznych w rozumieniu MiFID), działającego na mocy art. 70 ust. 2 ustawy o obrocie, świadczącego swe usługi „inwestycyjne” za pośrednictwem oddziałów, telefonie oraz poprzez bankowość internetową. Co powinno monitorować compliance, jakie KRI analizować, żeby dostatecznie szybko dowiadywać się o potencjalnie niepożądanych zdarzeniach? Poniżej kilka propozycji dla powyższego hipotetycznego przykładu. Rzecz jasna wskazane KRI nie są gotową odpowiedzią dla każdej organizacji, mają jedynie posłużyć jako przykład. Należy też pamiętać, że samo osiągniecie danego progu jeszcze nie świadczy o tym, że na 100% się coś dzieje, ale raczej, że dziać się może (np. *określony wysoki próg odmówan ankiet odpowiedniości może świadczyć o tym, że doradcy nie zostali właściwie przeszkoleni by wytłumaczyć klientom zalety takiego badania, bądź np. zostały zmienione zasady wynagradzania i firma promuje bardziej ryzykowne produkty, przez co w interesie doradców jest by klient zawierał takie transakcje „na własne żądanie”, bez przeprowadzonego badania*).

KRI mierzone dla konkretnego miesiąca

Wskaźnik odmów wypełnienia ankiet odpowiedniości	H	M-H	M-L	L
1) dla całej organizacji 2) dla wybranego obszaru 3) dla konkretnego pracownika	Pow. 30%	21-30%	11-20%	0-10%

Wskaźnik transakcji zawartych poza profilem klienta	H	M-H	M-L	L
1) dla całej organizacji 2) dla wybranego obszaru 3) dla konkretnego pracownika	Pow. 30%	21-30%	11-20%	0-10%

	H	M-H	M-L	L
Ilość reklamacji/reklamacji za pośrednictwem regulatora	Pow. 16	12-16	6-11	0-5

e. Pkt. 23: *program monitorowania powinien odzwierciedlać zmiany w profilu ryzyka firmy inwestycyjnej, które mogą wynikać np. z istotnych wydarzeń, takich jak przejęcia podmiotów gospodarczych, zmiany systemów informatycznych lub reorganizacja.*

Powinien on również obejmować wdrażanie i skuteczność wszelkich działań naprawczych podejmowanych przez firmę w reakcji na naruszenia MiFID II, powiązanych aktów delegowanych lub wykonawczych lub krajowych przepisów wykonawczych

Jak wdrożyć? Odpowiednie zapisy w wewnętrznych aktach normatywnych, do tego opracowanie metodyk, kończąc na faktycznym wykonywaniu zadań w oparciu o nastawienie do ryzyka.

f. Pkt. 24: *Działania monitorujące komórki ds. nadzoru zgodności z prawem powinny również uwzględniać:*

- *(a) obowiązki związane ze zgodnością danego obszaru działalności z wymogami regulacyjnymi;*
- *(b) mechanizmy kontrolne pierwszego stopnia wykorzystywane w poszczególnych obszarach działalności firmy (tj. kontrola dokonywana przez jednostki operacyjne w odróżnieniu od kontroli drugiego stopnia dokonywanej przez komórkę ds. nadzoru zgodności z prawem); oraz*
- *(c) przeglądy dokonywane przez komórki ds. zarządzania ryzykiem, audytu wewnętrznego lub inne komórki ds. kontroli w obszarze usług inwestycyjnych i działalności inwestycyjnej.*

Jak wdrożyć? Odpowiednie zapisy w wewnętrznych aktach normatywnych, do tego opracowanie metodyk, kończąc na faktycznym wykonywaniu zadań w oparciu o nastawienie do ryzyka.

Dodatkowo wpisanie kompetencji dla funkcji compliance dostępu do przeglądów i kontroli wykonywanych przez 1-ą linię ale także przez inne komórki kontrolne – audyt, ryzyko itp. patrząc z punktu widzenia oceny ryzyka (tabela powyżej) mogłoby wyglądać to w sposób następujący:

Rodzaj działalności	Ocena ryzyka inherentnego	Stosowane mechanizmy kontrolne	Ocena mechanizmów kontrolnych
Świadczenie przez dom maklerski usługi doradztwa inwestycyjnego zależnego	**M-H** (medium-high), jako wynikowa zainteresowania KNF i znacznej ilości przepisów MiFID dotykających tej materii	1. Szkolenia pracowników 2. Nagrywanie rozmów 3. Notatki ze spotkań z klientami 4. Wewnętrzna certyfikacja	Do poprawy = M-L (zdarzają się sytuacje w których pracownicy świadczą usługę doradztwa inwestycyjnego niezgodnie z profilem klienta)

Ustalenia audytu wewnętrznego	Ustalenia z kontroli 1-ej linii	Ustalenia z kontroli ryzyka	Ustalenia audytu zewnętrznego	Ocena ryzyka rezydualnego	Proponowane środki naprawcze
N/A	Pracownicy zgłaszają braki w wiedzy do swoich przełożonych	N/A	KNF uznała, że zdarzają się sytuacje w których pracownicy świadczą usługę doradztwa inwestycyjnego niezgodnie z profilem klienta	**M-H** (medium-high) - ryzyko inherentne na poziomie M-H oraz nieprawidłowości w świadczeniu usług	[w zależności od tego jak działa firma]

g. Pkt. 25: *Przeglądy dokonywane przez komórki ds. kontroli powinny być skoordynowane z działaniami monitorującymi komórki ds. nadzoru zgodności z prawem, z zastrzeżeniem niezależności i uprawnień poszczególnych komórek.*

Jak wdrożyć? Odpowiednie zapisy w wewnętrznych aktach normatywnych, do tego opracowanie metodyk, kończąc na faktycznym wykonywaniu zadań w oparciu o nastawienie do ryzyka.

h. Pkt. 26: *Komórka ds. nadzoru zgodności z prawem powinna odgrywać rolę w nadzorowaniu funkcjonowania procesów związanych ze skargami oraz powinna traktować skargi jako źródło istotnych informacji w kontekście swojej ogólnej odpowiedzialności w dziedzinie monitorowania.*

Nie pociąga to za sobą wymogu, aby komórka ds. nadzoru zgodności z prawem odgrywała rolę w decyzjach o sposobie rozpatrzenia skarg.

W związku z powyższym firmy powinny umożliwić komórce ds. nadzoru zgodności z prawem dostęp do wszystkich skarg klientów otrzymanych przez firmę.

Jak wdrożyć? Odpowiednie zapisy w wewnętrznych aktach normatywnych, do tego opracowanie metodyk, kończąc na faktycznym wykonywaniu zadań w oparciu o nastawienie do ryzyka. Dodatkowo wpisanie kompetencji np. w regulaminie rozpatrywania reklamacji i skarg dla funkcji compliance dostępu do wszystkich skarg klientów otrzymanych przez firmę ale także konieczności uzgadniania odpowiedzi z funkcją compliance.

1 https://www.esma.europa.eu/sites/default/files/library/2015/11/2012-388_pl.pdf [dostęp na maj 2021 r.];
2 Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA) - *jest niezależnym organem UE, którego celem jest poprawa ochrony inwestorów oraz promowanie stabilnych i sprawnych rynków finansowych* (za: https://europa.eu/european-union/about-eu/agencies/esma_pl), [dostęp na maj 2021 r.];
3 https://www.esma.europa.eu/system/files_force/library/guidelines_on_certain_aspects_of_mifid_ii_compliance_function_requirements_pl.pdf?download=1 [dostęp na maj 2021 r.];
4 Więcej na https://compliancemifid.files.wordpress.com/2014/05/guidelines-on-certain-aspects-of-the-mifid-compliance-requirements.pdf [dostęp na maj 2021 r.];
5 http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20051831538/U/D20051538Lj.pdf [dostęp na maj 2021 r.];
6 https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2013_00580000_pl_cor.pdf [dostęp na maj 2021 r.];
7 W terminie dwóch miesięcy od daty publikacji Wytycznych 2021 KNF oraz inni krajowi regulatorzy są zobowiązani powiadomić ESMA, czy (i) stosują się do wytycznych, (ii) nie stosują się do nich, ale zamierzają to czynić, albo czy (iii) nie stosują się i nie zamierzają zastosować się do wytycznych.
8 Pamiętając i czytając postanowienia systemu MiFID II (w tym Wytycznych 2021) łącznie z postanowieniami Rekomendacji H dotyczącej systemu kontroli wewnętrznej w bankach https://www.knf.gov.pl/knf/pl/komponenty/img/knf_170534_Rekomendacja_H_2017_50303.pdf [dostęp na maj 2021 r.] oraz Rozporządzenia Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20170000637/O/D20170637.pdf [dostęp na maj 2021 r.].
9 Rozporządzenie Delegowane Komisji (UE) 2017/565 z dnia 25 kwietnia 2016 r. uzupełniające 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, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32017R0565&from=PL [dostęp na maj 2021 r.].
10 *Za Stanowisko UKNF dotyczące oceny ryzyka instytucji obowiązanej: ryzyko inherentne czyli ryzyko występujące w sytuacji braku działań podjętych w celu zmniejszenia prawdopodobieństwa wystąpienia ryzyka i/lub ograniczenia jego efektów,* https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_oceny_ryzyka_instytucji_obowiazanej.pdf [dostęp na maj 2021 r.], Por. także OCC Comptroller's Handbook, https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk-governance/index-corporate-and-risk-governance.html [dostęp na maj 2021 r.].
11 Patrz. *G.Włodarczyk, Struktura i status aktów prawa Unii Europejskiej ze szczególnym uwzględnieniem RTS, ITS i tzw. Guidelines,* https://compliancemifid.files.wordpress.com/2021/05/struktura-aktow-unii-europejskiej-ze-szczegolnym-uwzglednieniem-rts-its-i-tzw.-guidelines.pdf [dostęp na maj 2021 r.].
12 *Za Stanowisko UKNF dotyczące oceny ryzyka instytucji obowiązanej: ryzyko rezydualne czyli ryzyko pozostającego po wprowadzeniu procedur kontroli ryzyka, mitygantów,* https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_oceny_ryzyka_instytucji_obowiazanej.pdf [dostęp na maj 2021 r.],
13 Por. *G. Włodarczyk, Parametry zarządzania ryzykiem braku zgodności w MiFID,* 2014 r., https://compliancemifid.files.wordpress.com/2014/05/parametry-zarzc485dzania-ryzykiem-w-mifid.pdf [dostęp na maj 2021 r.]; także M.S. Beasley, B. C. Branson, B. V. Hancock, *Developing Key Risk Indicators to Strengthen Enterprise Risk Management - How Key Risk Indicators can Sharpen Focus on Emerging Risks,* https://www.coso.org/Documents/COSO-KRI-Paper-Full-FINAL-for-Web-Posting-Dec110-000.pdf [dostęp na maj 2021 r.].
14 M.Thlon, *Kluczowe wskaźniki ryzyka w procesie zarządzania w warunkach ryzyka operacyjnego w banku,* Zeszyty Naukowe 5 (929), Uniwersytet Ekonomiczny w Krakowie, https://zeszyty-naukowe.uek.krakow.pl/article/view/570/355 [dostęp na maj 2021 r.].

Więcej w kolejnych częściach artykułu.