



Guidelines on certain aspects of the MiFID compliance requirements - cz. 2 - jak wdrożyć?

Grzegorz Włodarczyk

Starszy ekspert ds. compliance

O samych Guidelines pisałem już w odrębnym artykule wcześniej dlatego tym razem daruję sobie wstęp i przejdę od razu do pomysłów na wdrożenie zapisów Wytycznych do konkretnych polityk dotyczących MiFID czy obszaru ryzyka braku zgodności.

I. Regulamin Organizacyjny jednostki compliance

1. **Właściwe zarządzanie ryzykiem braku zgodności w firmie inwestycyjnej** – poprzez opracowanie i wdrożenie wymaganych przez MiFID polityk i procedur, przegląd ryzyk, testy zgodności etc. – wydaje się, że tego typu ogólne zapisy można bez problemu wdrożyć do regulaminu organizacyjnego jednostki compliance poprzez odwołanie do konkretnych polityk, procedur etc. Mogą więc to być w szczególności zapisy tj.:
 - a. *Jednostka compliance jest odpowiedzialna za wdrożenie oraz monitorowanie przestrzegania polityk i procedur w następujących zakresach(...)* – nie widzę przeszkód formalnych, aby w zależności od wielkości jednostki compliance zdefiniować w/w albo w zadaniach jednostki bądź już konkretnie z przypisaniem do obszarów (AML/etyka czy MiFID) z przypisaniem do zakresu zadań wydziału/biura etc.
 - b. *Jednostka compliance obowiązana jest, w ramach efektywnego zarządzania ryzykiem braku zgodności, do wykonywania cyklicznych testów zgodności w następujących obszarach* – np. obszar *Best Execution* – rokrocznie, obszar *poprawności sprzedaży produktów inwestycyjnych* – rokrocznie oraz dodatkowo wykonywanie kontroli w sposób ciągły, tj. nie rzadziej niż raz na tydzień sprawdzanie transakcji klientów na wybranej próbie, zgodnie z metodologią wykonywania testów i kontroli compliance – dobrą praktyką jest by jednostka

compliance posiadała opisaną metodologię zarządzania ryzykiem braku zgodności oraz metodologię wykonywania testów i kontroli zgodności (ważna uwaga – kontrole zgodności nie są kontrolami, które wykonuje jednostka audytu wewnętrznego a zatem nie mogą być, także przez ogólną zasadę transparentności, wykonywane przez tę jednostkę!).

- c. Właściwe zarządzanie ryzykiem braku zgodności to zarządzanie wielopoziomowe (od biznesu, przez compliance na audycie wewnętrznym i ryzyku operacyjnym skończywszy) – w Regulaminie Organizacyjnym mogą znaleźć się także ogólne zapisy mówiące, iż „(...) *Za zarządzanie ryzykiem braku zgodności odpowiada Zarząd firmy inwestycyjnej. Zarząd wykonuje w/w za pomocą jednostki compliance, która wspierana jest w zarządzaniu ryzykiem braku zgodności przez jednostkę ds. ryzyka operacyjnego oraz jednostkę ds. ryzyka reputacyjnego.*

Modelowa struktura może wyglądać w sposób następujący:

§ 1. Nadzór nad zarządzaniem ryzykiem braku zgodności sprawuje Rada Nadzorcza.

§ 2. Nadzór jest sprawowany w szczególności poprzez przyjmowanie raportu Zarządu z zarządzania ryzykiem braku zgodności za rok ubiegły.

§ 3. Za zarządzanie ryzykiem braku zgodności odpowiedzialny jest Zarząd.

§ 4. Zarząd wykonuje zadania określone w § 3 za pomocą jednostki compliance, która wspierana jest przez jednostkę ds. ryzyka operacyjnego oraz jednostkę ds. ryzyka reputacyjnego.

§ 5. Struktura zarządzania ryzykiem braku zgodności wygląda następująco:

Ust. 1 Wszyscy pracownicy firmy inwestycyjnej – w zakresie wykonywanych zadań,

Ust. 2 Linie biznesowe – w zakresie I linii kontroli ryzyka braku zgodności,



Ust. 3 Jednostka compliance we współpracy z jednostką ds. ryzyka operacyjnego oraz jednostką ds. ryzyka reputacyjnego,

Ust. 4 Jednostka ds. audytu wewnętrznego – w zakresie kontroli poprawności zarządzania ryzykiem braku zgodności

Ust. 5 Zarząd

Ust. 6 Rada Nadzorcza – w zakresie nadzoru nad zarządzaniem ryzykiem braku zgodności.

2. **Sprawowanie nadzoru funkcjonalnego nad rozpatrywaniem reklamacji, w kontekście MiFID'u** – *Jednostka compliance sprawuje nadzór nad poprawnością rozpatrywania reklamacji z zakresu MiFID (zdefiniowanego wcześniej). Dodatkowe zapisy powinny się znaleźć w procedurze rozpatrywania reklamacji – np. na zasadzie (...) jednostka rozpatrująca reklamację w zakresie MiFID jest obowiązana uzgodnić, przed wysłaniem odpowiedzi do osoby składającej reklamację, treść odpowiedzi z jednostką compliance.*
3. **Szkolenia, bieżące doradztwo, opiniowanie polityk, procedur etc.:** *Jednostka compliance wykonuje swe zadania, określone w §, w szczególności poprzez:*
 - a. *Szkolenie pracowników – dobrą praktyką jest aby powstała krótka procedura, np. w formie zarządzenia wewnętrznego dyrektora jednostki compliance, określająca rodzaj i częstotliwość wykonywanych szkoleń;*
 - b. *Bieżące doradztwo dla pracowników poprzez udzielnie wyjaśnień, rekomendacji i opinii, przy czym (kolejna dobra praktyka) przyjmuje się zasadę, że opinia, rekomendacja etc. każdorazowo powinna wskazywać, oprócz stwierdzonych ryzyk, także propozycje rozwiązania problemu czy zmitygowania ryzyka;*
 - c. *Opiniowanie wewnętrznych aktów prawnych – szczegółowe zasady powinny zostać wpisane do procedury legislacyjnej firmy inwestycyjnej (zasad opiniowania);*

II. Polityka zgodności, metodologia zarządzania ryzykiem braku zgodności

1. **Wdrożenie programu monitorowania ryzyk**– powinna zostać określona metodologia zarządzania ryzykiem braku zgodności, jako odrębny dokument, który oparty byłby de facto o kontrole następczą, bądź w określonych przypadkach bieżącą. W szczególności metodologia taka powinna zawierać:
 - a. Szczegółowe zasady wykonywania testów zgodności oraz kontroli ad hoc,
 - b. Pokazywać matrycę testu zgodności (modelowego) – tj. określić przynajmniej podstawowe zasady metodologii jakie zawsze taki test musi wypełniać,
 - c. Kontrole i testy ad hoc – przyczyny oraz zasady ich wykonywania,
 - d. Monitorowanie zmian w prawie – częstotliwość oraz jakie akty są monitorowane (w przypadku MiFID będą to w szczególności prace ustawodawcze w Polsce, rekomendacje KNF, UOKiK, ZBP czy KDPW i NBP a także w zakresie ustawodawstwa europejskiego – prace Komisji Europejskiej, Parlamentu Europejskiego, ESMA plus dodatkowo mogą być to naukowe instytuty jak ECMI) – dobrą praktyką będzie wskazanie konkretnych stron WWW.
 - e. Określenie form kontroli wykonywanej przez biznes,
 - f. Fazy wykonywania testów zgodności,
 - g. Fazy raportowania wyników,
 - h. Kryteria oceny i nadawania ratingów rekomendacjom oraz całym testom,
 - i. Dokumentacja i archiwizacja,
 - j. Określenie metodyki doboru próby kontrolowanej przy testach, celem wyeliminowania uznaniowości,
 - k. Określenie załączników.

2. **Kwestia raportowania**– proponowane przeze mnie zapisy to np.:
 - a. *Compliance nie rzadziej niż raz na pół roku (na rok, na kwartał) sporządza raport z wykonywanych działań w ramach zarządzania ryzykiem braku zgodności, który przekazuje do wiadomości Zarządu,*
 - b. *Compliance raz do roku sporządza raport roczny z wykonywanych działań w ramach zarządzania ryzykiem braku zgodności, który przekazuje za pośrednictwem Zarządu do Rady Nadzorczej,*



- c. *Compliance, każdorazowo po zakończeniu testu zgodności, kontroli ad hoc, sporządza raport z przeprowadzonego testu, kontroli, który przekazuje do wiadomości nadzorującego Członka Zarządu (Prezesa Zarządu).*

3. Właściwe zasoby jednostki compliance:

- a. *Pracownicy jednostki compliance powinni charakteryzować się znaczną wiedzą z zakresu działalności firmy inwestycyjnej, którą nadzorują oraz kompetencjami i przymiotami osobistymi, pozwalającymi na efektywne wykonywanie powierzonych im zadań.*
- b. *Pracownicy jednostki compliance zobligowani są do uczestniczenia, nie rzadziej niż raz na kwartał, w szkoleniach merytorycznych (stacjonarnych bądź e-learningowych) z zakresu działalności, którą wykonują. Obowiązek skierowania na w/w spoczywa na dyrektorze jednostki ds. compliance.*