EBA/GL/2017/11

21/03/2018

Wytyczne

w sprawie zarządzania wewnętrznego

1. Zgodność i obowiązki sprawozdawcze

Status niniejszych wytycznych

1. Niniejszy dokument zawiera wytyczne wydane zgodnie z art. 16 rozporządzenia (UE) nr 1093/2010[1]. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy i instytucje finansowe dokładają wszelkich starań, aby zastosować się do tych wytycznych i zaleceń.

2. Wytyczne przedstawiają stanowisko EUNB w sprawie odpowiednich praktyk nadzoru w ramach Europejskiego Systemu Nadzoru Finansowego lub tego, jak należy stosować prawo europejskie w konkretnym obszarze. Właściwe organy określone w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010, do których wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez wprowadzenie ich odpowiednio do swoich praktyk (np. poprzez dostosowanie swoich ram prawnych lub procesów nadzorczych), również jeżeli wytyczne są skierowane przede wszystkim do instytucji.

Wymogi dotyczące sprawozdawczości

3. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy muszą poinformować EUNB, czy stosują się lub czy zamierzą zastosować się do niniejszych wytycznych lub danego zalecenia lub podają powody niestosowania się do dnia 21/05/2018 W przypadku braku informacji w tym terminie właściwe organy zostaną uznane przez EUNB za niestosujące się do niniejszych wytycznych. Informacje należy przekazać poprzez wysłanie formularza dostępnego na stronie internetowej EUNB na compliance@eba.europa.eu z dopiskiem „EBA/GL/2017/11”. Informacje przekazują osoby upoważnione do informowania o niestosowaniu się do wytycznych w imieniu właściwych organów. Wszelkie zmiany dotyczące stosowania się do wytycznych także należy zgłaszać do EUNB.

4. Zgodnie z art. 16 ust. 3 przekazywane informacje publikuje się na stronie internetowej EUNB.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

2. Przedmiot, zakres stosowania i definicje

Przedmiot

5. W niniejszych wytycznych określa się zasady zarządzania wewnętrznego, procesy oraz mechanizmy, które instytucje kredytowe i firmy inwestycyjne muszą wdrożyć zgodnie z art. 74 ust. 1 dyrektywy 2013/36/UE[2] w celu zapewnienia skutecznego i ostrożnego zarządzania instytucją.

Adresaci

6. Niniejsze wytyczne są skierowane do właściwych organów określonych w art. 4 ust. 1 pkt 40 rozporządzenia (UE) nr 575/2013[3], w tym Europejskiego Banku Centralnego w odniesieniu do spraw dotyczących zadań powierzonych mu rozporządzeniem (UE) nr 1024/2013, oraz do instytucji określonych w art. 4 ust. 1 pkt 3 rozporządzenia (UE) nr 575/2013.

Zakres stosowania

7. Niniejsze wytyczne mają zastosowanie do zasad zarządzania instytucjami, w tym ich struktury organizacyjnej oraz odpowiednich hierarchii odpowiedzialności, procesów służących identyfikacji ryzyka, na które instytucje są lub mogą być narażone, zarządzaniu tym ryzykiem, jego monitorowaniu i sprawozdawczości oraz ram kontroli wewnętrznej.

8. Celem wytycznych jest uwzględnienie wszystkich istniejących struktur zarządzania bez opowiadania się za jakąkolwiek konkretną strukturą. Wytyczne nie wpływają na ogólny podział kompetencji w myśl krajowego prawa spółek. W związku z tym powinny one być stosowane niezależnie od zastosowanej struktury zarządzania (monistycznej, dualistycznej lub innej) we wszystkich państwach członkowskich. Organ zarządzający określony w art. 3 ust. 1 pkt 7 i 8 dyrektywy 2013/36/UE powinien być rozumiany jako pełniący funkcję zarządczą (wykonawczą) i nadzorczą (niewykonawczą)[4].

9. Terminy „organ zarządzający pełniący funkcję zarządczą” i „organ zarządzający pełniący funkcję nadzorczą” są stosowane w niniejszych wytycznych bez odnoszenia się do jakiejkolwiek konkretnej struktury zarządzania, a wszelkie odniesienia do funkcji zarządczej (wykonawczej)

[2] 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 (Dz.U. L 176 z 27.6.2013, s. 338).

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 176 z 27.6.2013, s. 1–337).

[4] Zob. też motyw 56 dyrektywy 2013/36/UE.

lub nadzorczej (niewykonawczej) powinny być rozumiane jako mające zastosowanie do organów lub członków organu zarządzającego odpowiedzialnych za tę funkcję zgodnie z prawem krajowym. Wdrażając niniejsze wytyczne, właściwe organy powinny uwzględnić krajowe prawo spółek i określić, w razie konieczności, do którego organu lub członków organu zarządzającego powinny mieć zastosowanie te funkcje.

10. W państwach członkowskich, w których organ zarządzający przekazuje funkcje wykonawcze w części lub w całości osobie bądź wewnętrznemu organowi wykonawczemu (np. dyrektorowi generalnemu, zespołowi zarządzającemu lub komitetowi wykonawczemu), osoby pełniące te funkcje wykonawcze na podstawie takiej delegacji należy uznawać za wykonujące funkcję zarządczą organu zarządzającego. Do celów niniejszych wytycznych wszelkie odniesienia do organu zarządzającego pełniącego funkcję zarządczą należy rozumieć jako obejmujące również członków organu wykonawczego lub dyrektora generalnego określonych w niniejszych wytycznych, nawet jeżeli ich kandydatur nie wysunięto lub nie powołano ich w formalny sposób na członków organu bądź organów zarządzających instytucji na mocy prawa krajowego.

11. W państwach członkowskich, w których niektóre obowiązki są sprawowane bezpośrednio przez akcjonariuszy, udziałowców lub właścicieli instytucji, nie zaś przez organ zarządzający, instytucje powinny dopilnować, aby takie obowiązki i związane z nimi decyzje były, o ile to możliwe, zgodne z wytycznymi mającymi zastosowanie do organu zarządzającego.

12. Definicje dyrektora generalnego, dyrektora finansowego oraz osoby pełniącej najważniejsze funkcje użyte w niniejszych wytycznych mają charakter wyłącznie funkcjonalny i nie mają w zamiarze nałożenia obowiązku mianowania takich funkcjonariuszy bądź utworzenia takich stanowisk, chyba że jest to wymagane na mocy stosownych przepisów prawa UE lub prawa krajowego.

13. Instytucje powinny przestrzegać niniejszych wytycznych na zasadzie indywidualnej, subskonsolidowanej i skonsolidowanej zgodnie z poziomem stosowania określonym w art. 109 dyrektywy 2013/36/UE, a właściwe organy powinny zapewnić ich przestrzeganie.

Definicje

14. O ile nie określono inaczej, pojęcia stosowane i zdefiniowane w dyrektywie 2013/36/UE mają w niniejszych wytycznych takie samo znaczenie. Ponadto do celów niniejszych wytycznych stosuje się następujące definicje:

Skłonność do podejmowania ryzyka	oznacza łączny poziom i rodzaje ryzyka, jakie instytucja jest skłonna podejmować w ramach swojej zdolności do ponoszenia ryzyka, zgodnie ze swoim modelem działalności, w celu realizacji swoich celów strategicznych.
Zdolność do ponoszenia ryzyka	oznacza maksymalny poziom ryzyka, jaki instytucja jest w stanie przyjąć, biorąc pod uwagę jej bazę kapitałową, możliwości

	zarządzania ryzykiem i mechanizmy kontrolne oraz ograniczenia regulacyjne.
Kultura ryzyka	oznacza normy instytucji, postawy i zachowania odnoszące się do jej świadomości ryzyka, podejmowania przez nią ryzyka oraz zarządzania ryzykiem, a także mechanizmów kontrolnych kształtujących decyzje dotyczące ryzyka. Kultura ryzyka wpływa na decyzje podejmowane przez kierownictwo i pracowników w trakcie bieżącej działalności oraz ma wpływ na podejmowane przez nich ryzyko.
Instytucje	oznacza instytucje kredytowe i firmy inwestycyjne określone odpowiednio w art. 4 ust. 1 pkt 1 i 2 rozporządzenia (UE) nr 575/2013.
Pracownicy	oznacza wszystkich pracowników instytucji i jej jednostek zależnych objętych zakresem konsolidacji, w tym jednostek zależnych nieobjętych dyrektywą 2013/36/UE, oraz wszystkich członków organu zarządzającego pełniącego funkcję zarządczą i funkcję nadzorczą.
Dyrektor generalny	oznacza osobę odpowiedzialną za zarządzanie i sterowanie ogólną działalnością biznesową instytucji.
Dyrektor finansowy	oznacza osobę ponoszącą ogólną odpowiedzialność za zarządzanie wszystkimi poniższymi działaniami: zarządzaniem zasobami finansowymi, planowaniem finansowym i sprawozdawczością finansową.
Kierownicy komórek kontroli wewnętrznej	oznacza osoby na najwyższym szczeblu hierarchii odpowiedzialne za skuteczne zarządzanie codziennym funkcjonowaniem niezależnych komórek ds. zarządzania ryzykiem, ds. nadzoru zgodności z prawem i audytu wewnętrznego.
Osoby pełniące najważniejsze funkcje	oznacza osoby mające znaczący wpływ na kierunek instytucji, ale niebędące członkami organu zarządzającego ani dyrektorem generalnym. Należą do nich kierownicy komórek kontroli wewnętrznej i dyrektor finansowy w przypadku, gdy nie są oni członkami organu zarządzającego, a także inne osoby pełniące najważniejsze funkcje, jeżeli zostały one zidentyfikowane przez instytucje w wyniku analizy ryzyka. Inne osoby pełniące najważniejsze funkcje mogą być dyrektorami znaczących linii biznesowych, oddziałów na terenie Europejskiego Obszaru Gospodarczego / Europejskiego Stowarzyszenia Wolnego Handlu, jednostek zależnych w państwach trzecich bądź innych komórek wewnętrznych.
Konsolidacja ostrożnościowa	oznacza stosowanie zasad ostrożnościowych określonych w dyrektywie 2013/36/UE i rozporządzeniu (UE) nr 575/2013 na

	zasadzie skonsolidowanej lub subskonsolidowanej, zgodnie z przepisami części 1, tytułu 2, rozdziału 2 rozporządzenia (UE) nr 575/2013. Konsolidacja ostrożnościowa obejmuje wszystkie jednostki zależne będące instytucjami lub instytucjami finansowymi określonymi odpowiednio w art. 4 pkt 3 i pkt 26 rozporządzenia (UE) nr 575/2013, jak też może obejmować przedsiębiorstwa usług pomocniczych określone w art. 2 pkt 18 tego rozporządzenia, mające siedziby w UE i poza jej terytorium.
Instytucja konsolidująca	oznacza instytucję, która ma obowiązek przestrzegania wymogów ostrożnościowych na podstawie skonsolidowanej sytuacji, zgodnie z częścią 1, tytułem 2, rozdziałem 2 rozporządzenia (UE) nr 575/2013.
Istotne instytucje	oznaczają instytucje, o których mowa w art. 131 dyrektywy 2013/36/UE (globalne instytucje o znaczeniu systemowym i inne instytucje o znaczeniu systemowym), oraz w stosownych przypadkach inne instytucje określone przez właściwe organy lub na mocy prawa krajowego w oparciu o ocenę wielkości i organizacji wewnętrznej instytucji, jak również charakteru, zakresu i złożoności jej działalności.
Giełdowe instytucje CRD	oznaczają instytucje, których instrumenty finansowe są dopuszczone do obrotu na rynku regulowanym lub na wielostronnej platformie obrotu określonych w art. 4 pkt 21 i 22 dyrektywy 2014/65/UE w jednym lub większej liczbie państw członkowskich[5].
Akcjonariusz	oznacza osobę będącą właścicielem akcji instytucji lub, w zależności od formy prawnej instytucji, innym właścicielem lub udziałowcem instytucji.
Dyrektor	oznacza stanowisko członka organu zarządzającego instytucji lub innego podmiotu prawnego.

3. Wdrożenie

Data rozpoczęcia stosowania

[5] Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.U. L 173 z 12.6.2014, s. 349).

15. Niniejsze wytyczne stosuje się od dnia 30 czerwca 2018 r.

Uchylenie

16. Uchyla się wytyczne EUNB w sprawie zarządzania wewnętrznego (GL 44) z dnia 27 września 2011 r. ze skutkiem od dnia 30 czerwca 2018 r.

4. Wytyczne

Tytuł I – Proporcjonalność

17. Zasada proporcjonalności zapisana w art. 74 ust. 2 dyrektywy 2013/36/UE ma na celu zapewnienie, aby zasady zarządzania wewnętrznego były zgodne z indywidualnym profilem ryzyka i modelem biznesowym instytucji w celu skutecznego zrealizowania celów wyznaczonych w ramach wymogów regulacyjnych.

18. Podczas opracowywania i wdrażania zasad zarządzania wewnętrznego instytucje powinny uwzględnić swoją wielkość i organizację wewnętrzną, a także charakter, skalę oraz złożoność swojej działalności. Istotne instytucje powinny posiadać bardziej wyrafinowane zasady zarządzania, natomiast mniejsze i mniej złożone instytucje mogą wdrożyć prostsze zasady zarządzania.

19. Do celów zastosowania zasady proporcjonalności oraz w celu zapewnienia odpowiedniego wdrożenia wymogów instytucje i właściwe organy powinny wziąć pod uwagę następujące kryteria:

    a. wielkość pod względem sumy bilansowej instytucji oraz jej jednostek zależnych objętych zakresem konsolidacji ostrożnościowej;

    b. obecność geograficzną instytucji oraz wielkość jej działalności w każdej jurysdykcji;

    c. formę prawną instytucji, w tym to, czy instytucja jest częścią grupy, a jeżeli tak, ocenę proporcjonalności dla tej grupy;

    d. czy dana instytucja jest notowana na giełdzie, czy też nie;

    e. czy instytucja posiada pozwolenie na stosowanie modeli wewnętrznych do pomiaru wymogów kapitałowych (np. metody wewnętrznych ratingów);

    f. rodzaj dozwolonej działalności i usług świadczonych przez instytucję (np. zob. też załącznik 1 do dyrektywy 2013/36/UE i załącznik 1 do dyrektywy 2014/65/UE);

    g. model i strategię biznesową instytucji; charakter i złożoność jej działalności biznesowej oraz strukturę organizacyjną instytucji;

    h. strategię w zakresie ryzyka, skłonność do podejmowania ryzyka i rzeczywisty profil ryzyka instytucji, również z uwzględnieniem wyników BION dotyczących kapitału i płynności;

i. strukturę własnościową i finansowania instytucji;

j. rodzaj klientów (np. detaliczni, korporacyjni, instytucjonalni, małe firmy, podmioty publiczne) oraz złożoność produktów lub umów;

k. czynności objęte outsourcingiem i kanały dystrybucji; oraz

l. dotychczasowe systemy informatyczne, w tym systemy służące utrzymaniu ciągłości działalności i czynności objęte outsourcingiem w tym obszarze.

Tytuł II – Rola i skład organu zarządzającego oraz komitetów

1 Rola i obowiązki organu zarządzającego

20. Zgodnie z art. 88 ust. 1 dyrektywy 2013/36/UE organ zarządzający musi ponosić ostateczną i ogólną odpowiedzialność za instytucję oraz określa zasady zarządzania w obrębie instytucji, które zapewniają skuteczne i ostrożne zarządzanie instytucją, nadzoruje wdrożenie tych zasad i jest za to wdrożenie odpowiedzialny.

21. Obowiązki organu zarządzającego powinny być jasno określone, z rozróżnieniem obowiązków funkcji zarządczej (wykonawczej) i funkcji nadzorczej (niewykonawczej). Zakres odpowiedzialności i obowiązki organu zarządzającego powinny zostać jasno określone w formie pisemnej oraz w należyty sposób zatwierdzone przez organ zarządzający.

22. Wszyscy członkowie organu zarządzającego powinni być w pełni świadomi jego struktury i zakresu odpowiedzialności, a także podziału zadań między poszczególnymi funkcjami organu zarządzającego i jego komitetami. W celu zapewnienia odpowiednich mechanizmów kontroli i równowagi jego proces decyzyjny nie powinien być zdominowany przez jednego członka lub niewielką grupę członków. Organ zarządzający pełniący funkcję nadzorczą oraz organ zarządzający pełniący funkcję zarządczą powinny skutecznie współdziałać. Obydwie funkcje powinny dostarczać sobie nawzajem informacji wystarczających do tego, aby mogły wykonywać swoje role.

23. Do obowiązków organu zarządzającego powinny należeć ustalanie, zatwierdzanie i nadzorowanie wdrażania:

a. ogólnej strategii biznesowej instytucji i jej najważniejszej polityki w obrębie obowiązujących ram prawnych i regulacyjnych przy uwzględnieniu długoterminowego interesu finansowego oraz wypłacalności instytucji;

b. ogólnej strategii w zakresie ryzyka, w tym skłonności instytucji do podejmowania ryzyka oraz jej ram zarządzania ryzykiem, a także środków zapewniających, aby organ zarządzający poświęcał wystarczająco dużo czasu na zagadnienia związane z ryzykiem;

c. odpowiednich i skutecznych ram zarządzania wewnętrznego oraz kontroli wewnętrznej, obejmujących jasną strukturę organizacyjną i dobrze funkcjonujące, niezależne wewnętrzne komórki ds. zarządzania ryzykiem, ds. nadzoru zgodności z prawem i audytu, które dysponują wystarczającymi uprawnieniami, statusem i zasobami, aby móc wykonywać swoje funkcje;

d. wielkości, rodzajów oraz struktury kapitału wewnętrznego i funduszy własnych wystarczających do odpowiedniego pokrycia ryzyka podejmowanego przez instytucję;

e. celów zarządzania płynnością instytucji;

f. polityki wynagrodzeń zgodnej z zasadami wynagradzania określonymi w art. 92–95 dyrektywy 2013/36/UE oraz wytycznymi EUNB dotyczącymi prawidłowej polityki wynagrodzeń wydanymi na mocy art. 74 ust. 3 i art. 75 ust. 2 dyrektywy 2013/36/UE[6];

g. zasad mających na celu zapewnienie skutecznego przeprowadzenia indywidualnych i zbiorowych ocen kwalifikacji organu zarządzającego, odpowiedniego składu organu zarządzającego i planowania sukcesji w jego obrębie oraz skutecznego pełnienia funkcji przez organ zarządzający[7];

h. procesu wyboru i oceny kwalifikacji osób pełniących najważniejsze funkcje[8];

i. zasad mających na celu zapewnienie wewnętrznego funkcjonowania każdego ustanowionego komitetu organu zarządzającego, z wyszczególnieniem:

    i. roli, składu i zadań każdego z tych komitetów;

    ii. odpowiedniego przepływu informacji, w tym dokumentacji zaleceń i wniosków, oraz hierarchii podległości służbowej między każdym komitetem a organem zarządzającym, właściwymi organami i innymi stronami;

j. kultury ryzyka zgodnie z sekcją 9 niniejszych wytycznych, odnoszącej się do świadomości ryzyka i zachowań związanych z podejmowaniem ryzyka w instytucji;

k. kultury korporacyjnej i wartości zgodnie z sekcją 10, które powinny promować odpowiedzialne i etyczne postępowanie, w tym kodeksu postępowania lub podobnego dokumentu;

[6] Wytyczne EUNB dotyczące prawidłowej polityki wynagrodzeń, o których mowa w art. 74 ust. 3 i 75 ust. 2 dyrektywy 2013/36/UE, i ujawniania informacji zgodnie z art. 450 rozporządzenia (UE) nr 575/2013 (EBA/GL/2015/22).

[7] Zob. też wspólne wytyczne ESMA i EUNB w sprawie oceny kwalifikacji członków organu zarządzającego i osób pełniących najważniejsze funkcje wydane na mocy dyrektywy 2013/36/UE i dyrektywy 2014/65/UE.

[8] Zob. też wspólne wytyczne ESMA i EUNB w sprawie oceny kwalifikacji członków organu zarządzającego i osób pełniących najważniejsze funkcje wydane na mocy dyrektywy 2013/36/UE i dyrektywy 2014/65/UE.

l. polityki przeciwdziałania konfliktom interesów na poziomie instytucjonalnym zgodnie z sekcją 11 oraz dla pracowników zgodnie z sekcją 12; oraz

m. zasad mających na celu zapewnienie rzetelności systemów rachunkowości i sprawozdawczości finansowej, w tym finansowych i operacyjnych mechanizmów kontrolnych, a także zgodności z przepisami i odpowiednimi standardami.

24. Organ zarządzający musi nadzorować proces ujawniania informacji i ich przekazywania w kontaktach z zewnętrznymi zainteresowanymi stronami i właściwymi organami.

25. Wszyscy członkowie organu zarządzającego powinni być informowani o ogólnej działalności instytucji oraz jej sytuacji finansowej i pod względem ryzyka, z uwzględnieniem środowiska gospodarczego, a także o podejmowanych decyzjach mających znaczny wpływ na działalność instytucji.

26. Członek organu zarządzającego może odpowiadać za komórkę kontroli wewnętrznej, o której mowa w tytule V, sekcji 19.1, pod warunkiem, że członek ten nie posiada innych uprawnień, które mogłyby negatywnie wpływać na jego działania w zakresie kontroli wewnętrznej i niezależność komórki kontroli wewnętrznej.

27. Organ zarządzający powinien monitorować wszelkie uchybienia zidentyfikowane w odniesieniu do wdrażania procesów, strategii i polityki wymienionych w pkt 23 i 24, dokonywać ich okresowego przeglądu oraz je naprawiać. Ramy zarządzania wewnętrznego i ich wdrażanie powinny być poddawane okresowemu przeglądowi i aktualizacji z uwzględnieniem zasady proporcjonalności, co wyjaśniono bardziej szczegółowo w tytule I. W przypadku istotnych zmian mających wpływ na instytucję należy przeprowadzić bardziej dogłębny przegląd.

2 Funkcja zarządcza organu zarządzającego

28. Organ zarządzający pełniący funkcję zarządczą powinien aktywnie angażować się w działalność instytucji oraz podejmować decyzje w prawidłowy i świadomy sposób.

29. Organ zarządzający pełniący funkcję zarządczą powinien ponosić odpowiedzialność za wdrażanie strategii określonych przez organ zarządzający oraz regularnie omawiać wdrażanie i odpowiedniość tych strategii z organem zarządzającym pełniącym funkcję nadzorczą. Wdrożenie operacyjne może zostać przeprowadzone przez kierownictwo instytucji.

30. Dokonując osądu i podejmując decyzje, organ zarządzający pełniący funkcję zarządczą powinien konstruktywnie kwestionować oraz krytycznie oceniać przedstawiane mu propozycje, wyjaśnienia i informacje. Organ zarządzający pełniący funkcję zarządczą powinien składać kompleksowe sprawozdania oraz informować regularnie, a także w razie potrzeby bez zbędnej zwłoki organ zarządzający pełniący funkcję nadzorczą o elementach istotnych dla oceny sytuacji, ryzyku i wydarzeniach mających wpływ lub mogących mieć wpływ na instytucję, np. istotnych decyzjach dotyczących podejmowanych działań biznesowych i ponoszonego

ryzyka, dla oceny otoczenia gospodarczego i biznesowego instytucji, jej płynności oraz solidnej bazy kapitałowej, a także dla oceny jej istotnych ekspozycji na ryzyko.

3 Funkcja nadzorcza organu zarządzającego

31. Rola członków organu zarządzającego pełniącego funkcję nadzorczą powinna obejmować monitorowanie i konstruktywne kwestionowanie strategii instytucji.

32. Bez uszczerbku dla prawa krajowego w skład organu zarządzającego pełniącego funkcję nadzorczą powinni wchodzić członkowie niezależni zgodnie z sekcją 9.3 wspólnych wytycznych ESMA i EUNB w sprawie oceny kwalifikacji członków organu zarządzającego i osób pełniących najważniejsze funkcje wydanych na mocy dyrektywy 2013/36/UE i dyrektywy 2014/65/UE.

33. Bez uszczerbku dla zadań przydzielonych mu na mocy stosownego krajowego prawa spółek organ zarządzający pełniący funkcję nadzorczą powinien:

    a. nadzorować i monitorować proces podejmowania decyzji przez kierownictwo oraz jego działania, jak też zapewnić skuteczny nadzór nad organem zarządzającym pełniącym funkcję zarządczą, w tym monitorowanie oraz kontrolę jego indywidualnych i zbiorowych wyników, jak też realizacji strategii i celów instytucji;

    b. konstruktywnie kwestionować i krytycznie oceniać propozycje oraz informacje dostarczane przez członków organu zarządzającego pełniącego funkcję zarządczą, a także jego decyzje;

    c. uwzględniając zasadę proporcjonalności określoną w tytule I, należycie wypełniać obowiązki i rolę komitetu ds. ryzyka, komitetu ds. wynagrodzeń oraz komitetu ds. mianowań w przypadku, gdy takie komitety nie zostały ustanowione;

    d. zapewnić i okresowo oceniać skuteczność ram zarządzania wewnętrznego instytucji oraz podejmować odpowiednie kroki w celu usunięcia wszelkich stwierdzonych uchybień;

    e. nadzorować i monitorować konsekwentne wdrażanie celów strategicznych instytucji, jej struktury organizacyjnej i strategii w zakresie ryzyka, w tym jej skłonności do podejmowania ryzyka oraz ram zarządzania ryzykiem i innych obszarów polityki (np. polityki wynagrodzeń), a także zasad ujawniania informacji;

    f. monitorować konsekwentne wdrażanie kultury ryzyka w instytucji;

    g. nadzorować wdrażanie i utrzymywanie kodeksu postępowania lub podobnych skutecznych zasad w celu określenia faktycznych i potencjalnych konfliktów interesów, zarządzania nimi oraz ich minimalizacji;

h. nadzorować rzetelność informacji finansowych i sprawozdawczości oraz ram kontroli wewnętrznej, w tym skutecznych i prawidłowych ram zarządzania ryzykiem;

i. zapewnić, aby kierownicy komórek kontroli wewnętrznej mogli działać w sposób niezależny oraz aby w razie potrzeby mogli oni niezależnie od relacji podległości służbowej łączących te komórki z innymi wewnętrznymi organami, liniami biznesowymi lub jednostkami bezpośrednio zgłaszać organowi zarządzającemu pełniącemu funkcję nadzorczą wszelkie obawy i ostrzeżenia w przypadku wystąpienia niekorzystnych tendencji dotyczących ryzyka wpływających lub mogących wpływać na instytucję; oraz

j. monitorować wdrożenie planu audytu wewnętrznego po uprzednim zaangażowaniu komitetów ds. ryzyka i ds. audytu w przypadku, gdy takie komitety zostały ustanowione.

4 Rola przewodniczącego organu zarządzającego

34. Przewodniczący organu zarządzającego powinien kierować organem zarządzającym, przyczyniać się do efektywnego przepływu informacji w obrębie organu zarządzającego oraz między organem zarządzającym a jego komitetami w przypadku, gdy zostały one ustanowione, oraz powinien być odpowiedzialny za jego ogólne skuteczne funkcjonowanie.

35. Przewodniczący powinien zachęcać do otwartej i krytycznej dyskusji, sprzyjać takiej dyskusji oraz zapewnić możliwość wyrażania i omawiania odmiennych poglądów w ramach procesu decyzyjnego.

36. Co do zasady przewodniczący organu zarządzającego powinien być członkiem niewykonawczym. W przypadku gdy przewodniczący ma prawo do wykonywania obowiązków wykonawczych, instytucja powinna ustanowić środki mające na celu złagodzenie niekorzystnego wpływu tego faktu na mechanizmy kontroli i równowagi instytucji (np. przez wyznaczenie głównego członka rady lub najstarszego stażem niezależnego członka rady bądź zwiększenie liczby członków niewykonawczych w organie zarządzającym pełniącym funkcję nadzorczą). W szczególności zgodnie z art. 88 ust. 1 lit. e) dyrektywy 2013/36/UE przewodniczący organu zarządzającego pełniącego funkcję nadzorczą w instytucji nie może pełnić jednocześnie funkcji dyrektora wykonawczego w tej samej instytucji, chyba że zostało to uzasadnione przez instytucję, a właściwe organy wydały na to zezwolenie.

37. Przewodniczący powinien ustalać porządek posiedzeń i zapewniać priorytetowe poruszanie kwestii strategicznych. Powinien on zapewnić podejmowanie decyzji organu zarządzającego w prawidłowy i świadomy sposób, a także otrzymywanie dokumentów i informacji przez jego członków z wystarczającym wyprzedzeniem przed posiedzeniami.

38. Przewodniczący organu zarządzającego powinien przyczyniać się do jasnego podziału obowiązków między jego członkami, a także efektywnego przepływu informacji między nimi,

aby członkowie organu zarządzającego pełniącego funkcję nadzorczą mogli w sposób konstruktywny wnosić wkład do dyskusji oraz głosować w prawidłowy i świadomy sposób.

5 Komitety organu zarządzającego pełniącego funkcję nadzorczą

5.1 Ustanawianie komitetów

39. Zgodnie z art. 109 ust. 1 dyrektywy 2013/36/UE w związku z art. 76 ust. 3, art. 88 ust. 2 i art. 95 ust. 1 dyrektywy 2013/36/UE wszystkie instytucje istotne w ujęciu indywidualnym, subskonsolidowanym lub skonsolidowanym mają obowiązek ustanowić komitety ds. ryzyka, mianowań [9] i wynagrodzeń [10] doradzające organowi zarządzającemu pełniącemu funkcję nadzorczą i przygotowujące decyzje, które ma podjąć ten organ. Instytucje nieistotne, również w przypadku, gdy są objęte zakresem konsolidacji ostrożnościowej instytucji istotnej w ujęciu subskonsolidowanym lub skonsolidowanym, nie mają obowiązku ustanawiania tych komitetów.

40. W przypadku gdy komitet ds. ryzyka lub mianowań nie został ustanowiony, odniesienia w niniejszych wytycznych do tych komitetów powinny być interpretowane jako mające zastosowanie do organu zarządzającego pełniącego funkcję nadzorczą, z uwzględnieniem zasady proporcjonalności określonej w tytule I.

41. Z uwzględnieniem kryteriów określonych w tytule I niniejszych wytycznych instytucje mogą ustanawiać inne komitety (np. ds. etyki, postępowania i zgodności z prawem).

42. Instytucje powinny zapewnić jasny przydział obowiązków i zadań oraz ich podział między wyspecjalizowanymi komitetami organu zarządzającego.

43. Każdy komitet powinien mieć udokumentowany mandat (określający także zakres jego obowiązków) od organu zarządzającego pełniącego funkcję nadzorczą, a także powinien ustanowić odpowiednie procedury robocze.

44. Komitety powinny wspierać funkcję nadzorczą w poszczególnych obszarach oraz ułatwiać opracowywanie i wdrażanie solidnych ram zarządzania wewnętrznego. Przekazanie uprawnień komitetom w żaden sposób nie zwalnia organu zarządzającego pełniącego funkcję nadzorczą ze zbiorowego wykonywania jego obowiązków i zadań.

5.2 Skład komitetów[11]

[9] Zob. też wspólne wytyczne ESMA i EUNB w sprawie oceny kwalifikacji członków organu zarządzającego i osób pełniących najważniejsze funkcje wydane na mocy dyrektywy 2013/36/UE i dyrektywy 2014/65/UE.

[10] W odniesieniu do komitetu ds. wynagrodzeń proszę zapoznać się z wytycznymi EUNB dotyczącymi prawidłowych praktyk w zakresie wynagrodzeń.

[11] Niniejszą sekcję należy interpretować w powiązaniu ze wspólnymi wytycznymi ESMA i EUNB w sprawie oceny kwalifikacji członków organu zarządzającego i osób pełniących najważniejsze funkcje wydanymi na mocy dyrektywy 2013/36/UE i dyrektywy 2014/65/UE.

45. Wszystkie komitety powinny być kierowane przez niewykonawczego członka organu zarządzającego, który jest zdolny do obiektywnego osądu.

46. Członkowie niezależni[12] organu zarządzającego pełniącego funkcję nadzorczą powinni być aktywnie zaangażowani w pracę komitetów.

47. W przypadku gdy komitety muszą zostać ustanowione zgodnie z dyrektywą 2013/36/UE lub prawem krajowym, powinny one składać się z co najmniej trzech członków.

48. Instytucje powinny zapewnić, z uwzględnieniem wielkości organu zarządzającego oraz liczby członków niezależnych organu zarządzającego pełniącego funkcję nadzorczą, aby różne komitety nie składały się z tej samej grupy członków.

49. Instytucje powinny rozważyć dokonywanie co pewien czas rotacji przewodniczących i członków komitetów, uwzględniając konkretne doświadczenie, wiedzę i umiejętności wymagane indywidualnie lub zbiorowo od członków tych komitetów.

50. Komitety ds. ryzyka i mianowań powinny składać się z członków niewykonawczych organu zarządzającego pełniącego funkcję nadzorczą danej instytucji. Skład komitetu ds. audytu powinien być zgodny z art. 41 dyrektywy 2006/43/WE[13]. Skład komitetu ds. wynagrodzeń powinien być zgodny z sekcją 2.4.1 wytycznych EUNB dotyczących prawidłowej polityki wynagrodzeń[14].

51. W przypadku globalnych instytucji o znaczeniu systemowym i innych instytucji o znaczeniu systemowym komitet ds. mianowań powinien składać się w większości z członków niezależnych oraz powinien mu przewodniczyć członek niezależny. W innych istotnych instytucjach określonych przez właściwe organy lub prawo krajowe w skład komitetu ds. mianowań powinna wchodzić wystarczająca liczba członków niezależnych; instytucje takie mogą również uznać za dobrą praktykę taką, zgodnie z którą przewodniczącym komitetu ds. mianowań jest członek niezależny.

52. Członkowie komitetu ds. mianowań powinni posiadać indywidualnie i zbiorowo odpowiednią wiedzę, w tym wiedzę fachową, oraz umiejętności w odniesieniu do procesu selekcji i wymagań dotyczących kwalifikacji.

53. W przypadku globalnych instytucji o znaczeniu systemowym i innych instytucji o znaczeniu systemowym komitet ds. ryzyka powinien składać się w większości z członków niezależnych. W przypadku globalnych instytucji o znaczeniu systemowym i innych instytucji o znaczeniu

[12] Określeni w sekcji 9.3 wspólnych wytycznych ESMA i EUNB w sprawie oceny kwalifikacji członków organu zarządzającego i osób pełniących najważniejsze funkcje wydanych na mocy dyrektywy 2013/36/UE i dyrektywy 2014/65/UE.

[13] 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 (Dz.U. L 157 z 9.6.2006, s. 87) zmieniona dyrektywą Parlamentu Europejskiego i Rady 2014/56/UE z dnia 16 kwietnia 2014 r.

[14] Wytyczne EUNB dotyczące prawidłowej polityki wynagrodzeń, o których mowa w art. 74 ust. 3 i 75 ust. 2 dyrektywy 2013/36/UE, i ujawniania informacji zgodnie z art. 450 rozporządzenia (UE) nr 575/2013 (EBA/GL/2015/22).

systemowym przewodniczący komitetu ds. ryzyka powinien być członkiem niezależnym. W innych istotnych instytucjach określonych przez właściwe organy lub prawo krajowe w skład komitetu ds. ryzyka powinna wchodzić wystarczająca liczba członków niezależnych, a przewodniczącym komitetu ds. ryzyka powinien być w miarę możliwości członek niezależny. We wszystkich instytucjach przewodniczącym komitetu ds. ryzyka nie powinien być przewodniczący organu zarządzającego ani przewodniczący żadnego innego komitetu.

54. Członkowie komitetu ds. ryzyka powinni posiadać indywidualnie i zbiorowo odpowiednią wiedzę, w tym wiedzę fachową, oraz umiejętności w odniesieniu do praktyk dotyczących zarządzania ryzykiem i mechanizmów kontrolnych.

5.3 Procesy komitetów

55. Komitety powinny regularnie składać sprawozdania organowi zarządzającemu pełniącemu funkcję nadzorczą.

56. Komitety powinny w stosownych przypadkach współdziałać ze sobą. Bez uszczerbku dla pkt 48 współdziałanie takie może przyjąć formę łączenia udziału polegającego na tym, że przewodniczący lub członek komitetu może być zarazem członkiem innego komitetu.

57. Członkowie komitetów powinni prowadzić otwarte i krytyczne dyskusje, podczas których odmienne poglądy są omawiane w konstruktywny sposób.

58. Komitety powinny dokumentować porządek swoich posiedzeń oraz ich główne wyniki i wnioski.

59. Komitety ds. ryzyka i mianowań powinny co najmniej:

    a. mieć dostęp do wszystkich istotnych informacji i danych niezbędnych w celu pełnienia ich roli, w tym informacji i danych ze stosownych komórek korporacyjnych oraz kontrolnych (ds. prawnych, finansowych, kadrowych, informatycznych, ryzyka, nadzoru zgodności z prawem, audytu itp.);

    b. otrzymywać regularne sprawozdania, informacje doraźne, komunikaty i opinie od kierowników komórek kontroli wewnętrznej dotyczące aktualnego profilu ryzyka instytucji, jej kultury ryzyka i limitów ryzyka, a także wszelkich istotnych naruszeń, do których mogło dojść, ze szczegółowymi informacjami i zaleceniami dotyczącymi podjętych, planowanych lub sugerowanych środków naprawczych służących ich usunięciu;

    c. dokonywać okresowego przeglądu przekazywanych im informacji o ryzyku oraz podejmować decyzje dotyczące ich treści, formatu i częstotliwości; oraz

    d. gdy jest to niezbędne, zapewnić odpowiednie zaangażowanie komórek kontroli wewnętrznej i innych stosownych komórek (ds. kadrowych, prawnych i finansowych) w zakresie ich specjalizacji lub zasięgać porady zewnętrznych ekspertów.

5.4 Rola komitetu ds. ryzyka

60. W przypadku jego ustanowienia komitet ds. ryzyka powinien co najmniej:

a. doradzać organowi zarządzającemu pełniącemu funkcję nadzorczą i wspierać go w zakresie monitorowania ogólnej obecnej i przyszłej skłonności instytucji do podejmowania ryzyka oraz strategii w zakresie ryzyka, z uwzględnieniem wszystkich rodzajów ryzyka, w celu zapewnienia, aby były one zgodne z strategią biznesową, celami, kulturą korporacyjną i wartościami instytucji;

b. wspomagać organ zarządzający pełniący funkcję nadzorczą w zakresie nadzoru nad wdrażaniem strategii w zakresie ryzyka instytucji i odpowiednich limitów;

c. nadzorować wdrażanie strategii zarządzania kapitałem i płynnością, a także wszystkimi innymi istotnymi rodzajami ryzyka, na które narażona jest instytucja, takimi jak ryzyko rynkowe, kredytowe, operacyjne (w tym ryzyko prawne i informatyczne) oraz ryzyko utraty reputacji, aby ocenić ich odpowiedniość z punktu widzenia zatwierdzonej skłonności do podejmowania ryzyka i strategii w zakresie ryzyka;

d. dostarczać organowi zarządzającemu pełniącemu funkcję nadzorczą zaleceń dotyczących niezbędnych korekt strategii w zakresie ryzyka, wynikających m.in. ze zmian w modelu biznesowym instytucji, wydarzeń rynkowych lub zaleceń wydanych przez komórkę ds. zarządzania ryzykiem;

e. świadczyć doradztwo dotyczące mianowania konsultantów zewnętrznych proszonych przez organ zarządzający pełniący funkcję nadzorczą o radę lub wsparcie;

f. dokonywać przeglądu możliwych scenariuszy, w tym scenariuszy warunków skrajnych, w celu określenia reakcji profilu ryzyka instytucji na wydarzenia zewnętrzne i wewnętrzne;

g. nadzorować dostosowanie wszystkich istotnych produktów finansowych i usług oferowanych klientom do modelu biznesowego instytucji oraz jej strategii w zakresie ryzyka [15] . Komitet ds. ryzyka powinien ocenić ryzyko związane z oferowanymi produktami oraz usługami finansowymi, uwzględniając przy tym stosunek cen tych produktów i usług do czerpanych z nich zysków; oraz

h. dokonywać oceny zaleceń audytorów wewnętrznych lub zewnętrznych i podejmować działania następcze związane z odpowiednim wdrożeniem podjętych środków.

61. Komitet ds. ryzyka powinien współpracować z innymi komitetami, których działalność może mieć wpływ na strategię w zakresie ryzyka (np. komitetami ds. audytu i mianowań), oraz

[15] Zob. też wytyczne EUNB dotyczące zasad nadzoru nad produktami i ustaleń zarządczych dla produktów bankowości detalicznej dostępne pod adresem http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products.

regularnie komunikować się z komórkami kontroli wewnętrznej instytucji, zwłaszcza z komórką ds. zarządzania ryzykiem.

62. Jeżeli ustanowiony został komitet ds. ryzyka, komitet ten musi zbadać, bez uszczerbku dla zadań komitetu ds. wynagrodzeń, czy zachęty, jakie stwarza polityka i praktyka w zakresie wynagrodzeń, uwzględniają ryzyko, kapitał i płynność instytucji oraz prawdopodobieństwo i perspektywę czasową uzyskania przez nią zysków.

5.5 Rola komitetu ds. audytu

63. Zgodnie z dyrektywą 2006/43/WE[16], w przypadku gdy został on ustanowiony, komitet audytu powinien między innymi:

a. monitorować skuteczność wewnętrznych systemów kontroli jakości i zarządzania ryzykiem instytucji oraz, w stosownych przypadkach, jej komórki audytu wewnętrznego w odniesieniu do sprawozdawczości finansowej badanej instytucji, bez naruszania jej niezależności;

b. nadzorować ustanowienie przez instytucję polityki rachunkowości;

c. monitorować proces sprawozdawczości finansowej i przedstawiać zalecenia mające na celu zapewnienie jego rzetelności;

d. dokonywać przeglądu i monitorowania niezależności biegłych rewidentów lub firm audytorskich zgodnie z art. 22, 22a, 22b, 24a i 24b dyrektywy 2006/43/UE oraz art. 6 rozporządzenia (UE) nr 537/2014[17], w szczególności odpowiedniości świadczenia usług niebędących badaniem sprawozdań finansowych zgodnie z art. 5 tego rozporządzenia;

e. monitorować badanie ustawowe rocznego i skonsolidowanego sprawozdania finansowego, w szczególności jego przeprowadzenie, uwzględniając wszelkie ustalenia i wnioski właściwego organu zgodnie z art. 26 ust. 6 rozporządzenia (UE) nr 537/2014;

f. ponosić odpowiedzialność za procedurę wyboru zewnętrznego biegłego rewidenta lub rewidentów bądź firmy audytorskiej lub firm audytorskich i zalecać zatwierdzenie ich powołania (zgodnie z art. 16 rozporządzenia (UE) nr 537/2014, z wyjątkiem przypadków, w których zastosowanie ma art. 16 ust. 8 rozporządzenia (UE) nr 537/2014), wynagrodzenia oraz odwołania przez właściwe organy instytucji;

[16] 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 (Dz.U. L 157 z 9.6.2006, s. 87) zmieniona dyrektywą Parlamentu Europejskiego i Rady 2014/56/UE z dnia 16 kwietnia 2014 r.

[17] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 537/2014 z dnia 16 kwietnia 2014 r. w sprawie szczegółowych wymogów dotyczących ustawowych badań sprawozdań finansowych jednostek interesu publicznego, uchylające decyzję Komisji 2005/909/WE (Dz.U. L 158 z 27.5.2014, s. 77).

g. dokonywać przeglądu zakresu i częstotliwości badania ustawowego rocznych lub skonsolidowanych sprawozdań finansowych;

h. zgodnie z art. 39 ust. 6 lit. a) dyrektywy 2006/43/UE poinformować organ administracyjny lub nadzorczy badanej jednostki o wynikach badania ustawowego i wyjaśnić, w jaki sposób badanie to przyczyniło się do rzetelności sprawozdawczości finansowej i jaka była rola komitetu ds. audytu w tym procesie; oraz

i. otrzymywać i uwzględniać sprawozdania z badań.

5.6 Połączone komitety

64. Zgodnie z art. 76 ust. 3 dyrektywy 2013/36/UE właściwe organy mogą zezwolić instytucjom, które nie są uznawane za istotne, na połączenie komitetu ds. ryzyka z komitetem ds. audytu, o którym mowa w art. 39 dyrektywy 2006/43/WE, jeżeli ten ostatni został ustanowiony.

65. Jeżeli w instytucji nieistotnej zostały ustanowione komitety ds. ryzyka i mianowań, mogą one zostać połączone. W takim przypadku instytucje te powinny udokumentować powody, dla których zdecydowały się połączyć komitety, oraz wskazać, w jaki sposób to podejście służy osiągnięciu celów komitetów.

66. Instytucje powinny w każdym przypadku zapewnić, aby członkowie połączonych komitetów posiadali indywidualnie i zbiorowo niezbędną wiedzę, w tym wiedzę fachową, oraz umiejętności umożliwiające im pełne zrozumienie obowiązków połączonego komitetu[18].

Tytuł III – Ramy zarządzania

6 Ramy i struktura organizacyjna

6.1 Ramy organizacyjne

67. Organ zarządzający instytucji powinien zapewnić odpowiednią i przejrzystą strukturę organizacyjną i operacyjną tej instytucji, a także powinien posiadać opis tej struktury w formie pisemnej. Struktura ta powinna przyczyniać się do zapewnienia oraz wykazania skutecznego i ostrożnego zarządzania instytucją w ujęciu indywidualnym, subskonsolidowanym oraz skonsolidowanym. Organ zarządzający powinien zapewnić, aby komórki kontroli wewnętrznej były niezależne od kontrolowanych przez nie linii biznesowych, w tym zapewnić właściwy podział obowiązków, a także odpowiednie zasoby finansowe i ludzkie oraz uprawnienia umożliwiające skuteczne pełnienie ich roli. Hierarchia służbowa oraz podział obowiązków, zwłaszcza między osobami pełniącymi najważniejsze funkcje w obrębie instytucji, powinny być jasne, dobrze określone, spójne, możliwe do wyegzekwowania oraz należycie udokumentowane. Dokumentacja powinna być odpowiednio uaktualniana.

[18] Zob. też wspólne wytyczne ESMA i EUNB w sprawie oceny kwalifikacji członków organu zarządzającego i osób pełniących najważniejsze funkcje wydane na mocy dyrektywy 2013/36/UE i dyrektywy 2014/65/UE.

68. Struktura instytucji nie powinna utrudniać organowi zarządzającemu nadzoru nad ryzykiem, na jakie narażona jest instytucja lub grupa, oraz skutecznego zarządzania nim, ani też utrudniać właściwemu organowi skutecznego nadzorowania tej instytucji.

69. Organ zarządzający powinien ocenić, czy i w jaki sposób istotne zmiany w strukturze grupy (np. tworzenie nowych jednostek zależnych, połączenia i przejęcia, sprzedaż lub likwidacja części grupy bądź wydarzenia zewnętrzne) wpływają na stabilność ram organizacyjnych. W przypadku stwierdzenia uchybień organ zarządzający powinien niezwłocznie dokonywać wszelkich niezbędnych korekt.

6.2 Znajomość struktury

70. Organ zarządzający powinien w pełni znać i rozumieć strukturę prawną, organizacyjną i operacyjną instytucji („znajomość struktury") oraz zapewnić jej zgodność z zatwierdzoną strategią biznesową i w zakresie ryzyka, jak też skłonnością do podejmowania ryzyka.

71. Organ zarządzający powinien być odpowiedzialny za zatwierdzanie prawidłowych strategii i polityki ustanawiania nowych struktur. W przypadku gdy instytucja ustanawia w obrębie swojej grupy wiele podmiotów prawnych, ich liczba, a zwłaszcza wzajemne powiązania i transakcje między nimi nie powinny utrudniać projektowania jej zarządzania wewnętrznego oraz skutecznego zarządzania ryzykiem grupy jako całości i nadzoru nad nim. Organ zarządzający powinien zapewnić, aby struktura instytucji, a w stosownych przypadkach również struktury w obrębie grupy, z uwzględnieniem kryteriów określonych w sekcji 7, były jasne, efektywne i przejrzyste dla pracowników instytucji, jej akcjonariuszy i innych zainteresowanych stron, a także dla właściwego organu.

72. Organ zarządzający powinien kształtować strukturę instytucji, jej ewolucję i ograniczenia, jak też zapewnić, aby struktura ta była uzasadniona i efektywna oraz nie cechowała się nadmierną lub nieodpowiednią złożonością.

73. Organ zarządzający instytucji konsolidującej powinien rozumieć nie tylko strukturę prawną, organizacyjną i operacyjną grupy, ale także cel poszczególnych podmiotów, ich działalność oraz związki i relacje między nimi. Oznacza to zrozumienie rodzajów ryzyka operacyjnego specyficznych dla grupy, ekspozycji wewnątrzgrupowych oraz sposobu, w jaki normalne i niekorzystne okoliczności mogą wpłynąć na finansowanie grupy, jej kapitał, płynność oraz profil ryzyka. Organ zarządzający powinien także zapewnić zdolność instytucji do przedstawiania w terminowy sposób informacji na temat grupy w odniesieniu do rodzaju, charakterystyki, struktury organizacyjnej, struktury własnościowej i działalności każdego podmiotu prawnego, a także zgodność instytucji wchodzących w skład grupy ze wszystkimi wymogami nadzorczymi w zakresie sprawozdawczości w ujęciu indywidualnym, subskonsolidowanym oraz skonsolidowanym.

74. Organ zarządzający instytucji konsolidującej powinien zapewnić poszczególnym podmiotom w obrębie grupy (w tym samej instytucji konsolidującej) wystarczającą ilość informacji, aby

wszystkie uzyskały jasny ogląd ogólnych celów grupy, jej strategii i profilu ryzyka, a także tego, w jaki sposób dany podmiot grupy wpisuje się w jej strukturę i funkcjonowanie operacyjne. Takie informacje oraz ich zmiany powinny być dokumentowane i udostępniane stosownym komórkom, w tym organowi zarządzającemu, liniom biznesowym i komórkom kontroli wewnętrznej. Członkowie organu zarządzającego instytucji konsolidującej powinni zasięgać informacji o ryzyku wynikającym ze struktury grupy, uwzględniając kryteria określone w sekcji 7 wytycznych. Obejmuje to otrzymywanie:

a. informacji na temat najważniejszych czynników ryzyka;

b. regularnych sprawozdań zawierających ocenę ogólnej struktury instytucji i zgodności działalności poszczególnych podmiotów z zatwierdzoną strategią grupową; oraz

c. regularnych sprawozdań na tematy, w przypadku których na mocy ram regulacyjnych wymagana jest zgodność na poziomie indywidualnym, subskonsolidowanym i skonsolidowanym.

6.3 Złożone struktury i niestandardowe lub nieprzejrzyste działania

75. Instytucje powinny unikać tworzenia złożonych i potencjalnie nieprzejrzystych struktur. Instytucje powinny uwzględniać w swoim procesie decyzyjnym wyniki przeprowadzonej oceny ryzyka w celu ustalenia, czy takie struktury mogłyby być wykorzystywane w celu związanym z praniem pieniędzy lub innymi przestępstwami finansowymi, a także ustanowione mechanizmy kontrolne i ramy prawne[19]. W tym celu instytucje powinny uwzględniać co najmniej:

a. stopień, w jakim jurysdykcja, w której zostanie ustanowiona struktura, skutecznie spełnia unijne i międzynarodowe standardy w zakresie przejrzystości podatkowej, przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu;

b. stopień, w jakim struktura służy oczywistemu, zgodnemu z prawem celowi ekonomicznemu;

c. stopień, w jakim struktura mogłaby zostać wykorzystana do ukrycia tożsamości ostatecznego beneficjenta rzeczywistego;

d. stopień, w jakim wniosek klienta skutkujący ewentualnym utworzeniem struktury budzi obawy;

[19] Aby uzyskać bardziej szczegółowe informacje na temat oceny ryzyka kraju oraz ryzyka związanego z poszczególnymi produktami i klientami, instytucje powinny również zapoznać się z ostatecznymi wspólnymi wytycznymi dotyczącymi czynników ryzyka (po ich wydaniu): https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence/-/regulatory-activity/consultation-paper.

e. czy struktura może utrudniać odpowiedni nadzór przez organ zarządzający instytucją lub zdolność instytucji do zarządzania powiązanym ryzykiem; oraz

f. czy struktura stwarza przeszkody w skutecznym nadzorze ze strony właściwych organów.

76. W każdym przypadku instytucje nie powinny ustanawiać nieprzejrzystych lub niepotrzebnie złożonych struktur, które nie mają jasnego uzasadnienia ekonomicznego ani celu prawnego, lub też w przypadkach, gdy instytucje te mają obawy, że struktury takie mogłyby być wykorzystywane w celach związanych z przestępczością finansową.

77. Przy ustanawianiu takich struktur organ zarządzający powinien rozumieć ich funkcjonowanie, cel oraz szczególne rodzaje ryzyka z nimi związane, a także zapewnić odpowiednie zaangażowanie komórek kontroli wewnętrznej. Takie struktury powinny być zatwierdzane i utrzymywane jedynie wtedy, gdy ich cel został w pełni określony i zrozumiany, a organ zarządzający jest przekonany, że zidentyfikowano wszystkie istotne rodzaje ryzyka, w tym ryzyko utraty reputacji, a wszystkimi tymi rodzajami ryzyka można skutecznie zarządzać i prowadzić odpowiednią sprawozdawczość ich dotyczącą, jak też zapewniono skuteczny nadzór. Im bardziej złożona oraz nieprzejrzysta jest struktura organizacyjna i operacyjna, i im większe jest ryzyko, tym ściślejszy powinien być nadzór nad daną strukturą.

78. Instytucje powinny dokumentować swoje decyzje i być w stanie je uzasadnić wobec właściwych organów.

79. Organ zarządzający powinien zapewnić podjęcie odpowiednich działań w celu uniknięcia lub minimalizacji ryzyka związanego z działalnością w obrębie takich struktur. Obejmuje to zapewnienie:

a. ustanowienia przez instytucję odpowiedniej polityki i procedur oraz udokumentowanych procesów (np. stosownych limitów, wymogów informacyjnych) w związku z rozważaniem, zapewnieniem zgodności i zatwierdzaniem takiej działalności oraz zarządzaniem związanym z nią ryzykiem, przy uwzględnieniu konsekwencji dla struktury organizacyjnej i operacyjnej grupy, jej profilu ryzyka oraz jej ryzyka utraty reputacji;

b. dostępności informacji na temat takiej działalności i związanego z nią ryzyka dla instytucji konsolidującej oraz audytorów wewnętrznych i zewnętrznych, jak też przedkładania ich w sprawozdaniach organowi zarządzającemu pełniącemu funkcję nadzorczą i właściwemu organowi, który wydał zezwolenie; oraz

c. dokonywania przez instytucję okresowej oceny, czy nadal zachodzi potrzeba utrzymywania takich struktur.

80. Te struktury i działalność, w tym ich zgodność z ustawodawstwem i standardami zawodowymi, powinny podlegać regularnemu przeglądowi przez komórkę audytu wewnętrznego w oparciu o analizę ryzyka.

81. Instytucje powinny podejmować te same środki zarządzania ryzykiem jak w przypadku własnej działalności biznesowej, gdy prowadzą niestandardową lub nieprzejrzystą działalność na rzecz klientów (np. udzielanie pomocy w zakładaniu spółek w zagranicznych jurysdykcjach, opracowywanie złożonych struktur i transakcji ich finansowania lub świadczenie usług powierniczych) skutkującą podobnymi trudnościami w dziedzinie zarządzania wewnętrznego oraz mogącą stwarzać znaczące ryzyko operacyjne i utraty reputacji. W szczególności instytucje powinny analizować przyczyny, dla których klient chce utworzyć konkretną strukturę.

7 Ramy organizacyjne w kontekście grupowym

82. Zgodnie z art. 109 ust. 2 dyrektywy 2013/36/UE jednostki dominujące i jednostki zależne objęte dyrektywą powinny zapewnić spójność i właściwe wdrożenie zasad, procesów oraz mechanizmów zarządzania w ujęciu skonsolidowanym i subskonsolidowanym. W tym celu jednostki dominujące i jednostki zależne objęte zakresem konsolidacji ostrożnościowej powinny wdrożyć takie zasady, procesy i mechanizmy w swoich jednostkach zależnych nieobjętych dyrektywą 2013/36/UE, aby zapewnić solidne zasady zarządzania w ujęciu skonsolidowanym i subskonsolidowanym. Właściwe komórki w instytucji konsolidującej i jej podmiotach zależnych powinny w odpowiedni sposób współdziałać oraz wymieniać dane i informacje. Zasady zarządzania, procesy i mechanizmy powinny zapewniać, aby instytucja konsolidująca dysponowała wystarczającymi danymi oraz informacjami i mogła ocenić ogólny profil ryzyka grupy, o którym mowa jest w sekcji 6.2.

83. Organ zarządzający jednostki zależnej objętej dyrektywą 2013/36/UE powinien przyjąć i wdrożyć na poziomie indywidualnym ogólnogrupową politykę w zakresie zarządzania ustanowioną na poziomie skonsolidowanym lub subskonsolidowanym w sposób zgodny ze wszystkimi szczegółowymi wymogami prawa unijnego i krajowego.

84. Na poziomie skonsolidowanym i subskonsolidowanym instytucja konsolidująca powinna zapewnić przestrzeganie ogólnogrupowej polityki w zakresie zarządzania przez wszystkie instytucje i inne podmioty objęte zakresem konsolidacji ostrożnościowej, w tym jednostek zależnych, które nie są same objęte dyrektywą 2013/36/UE. Wdrażając politykę w zakresie zarządzania, instytucja konsolidująca powinna zapewnić, aby dla każdej jednostki zależnej ustanowiono solidne zasady zarządzania, oraz rozważyć szczegółowe zasady, procesy i mechanizmy w przypadkach, gdy działalność biznesowa nie jest zorganizowana w ramach osobnych podmiotów prawnych, lecz w ramach złożonych linii biznesowych obejmujących większą liczbę podmiotów prawnych.

85. Instytucja konsolidująca powinna rozważyć interesy wszystkich swoich jednostek zależnych oraz ustalić, w jaki sposób strategie i polityka wnoszą wkład w realizację interesów każdej jednostki zależnej oraz interesów całej grupy w perspektywie długookresowej.

86. Jednostki dominujące i ich jednostki zależne powinny zapewnić spełnianie przez instytucje i podmioty należące do grupy wszystkich szczegółowych wymagań w każdej stosownej jurysdykcji.

87. Instytucja konsolidująca powinna zapewnić, aby jednostki zależne z siedzibą w państwach trzecich i objęte zakresem konsolidacji ostrożnościowej ustanowiły zasady zarządzania, procesy oraz mechanizmy zgodne z ogólnogrupową polityką zarządzania i zgodne z wymogami art. 74–96 dyrektywy 2013/36/UE oraz niniejszymi wytycznymi, o ile nie jest to niezgodne z prawem danego państwa trzeciego.

88. Wymogi dotyczące zarządzania określone w dyrektywie 2013/36/UE i niniejszych wytycznych stosuje się do instytucji niezależnie od tego, czy są one jednostkami zależnymi jednostki dominującej z państwa trzeciego. W przypadku gdy jednostka zależna w UE jednostki dominującej w państwie trzecim jest instytucją konsolidującą, zakres konsolidacji ostrożnościowej nie obejmuje poziomu jednostki dominującej z państwa trzeciego ani innych bezpośrednich jednostek zależnych tej jednostki dominującej. Instytucja konsolidująca powinna zapewnić, aby grupowa polityka zarządzania instytucji dominującej w państwie trzecim została uwzględniona w jej własnej polityce zarządzania, o ile nie jest to sprzeczne z wymogami określonymi we właściwych przepisach prawa UE lub prawa krajowego, w tym w dyrektywie 2013/36/UE i niniejszych wytycznych.

89. Ustanawiając politykę i dokumentując zasady zarządzania, instytucje powinny uwzględnić aspekty wymienione w załączniku I do wytycznych. Chociaż polityka i dokumentacja mogą być zawarte w osobnych dokumentach, instytucje powinny rozważyć połączenie ich lub odniesienie się do nich we wspólnym ramowym dokumencie dotyczącym zarządzania.

8 Polityka w zakresie outsourcingu[20]

90. Organ zarządzający powinien zatwierdzić politykę instytucji w zakresie outsourcingu oraz poddawać ją regularnemu przeglądowi i aktualizacji, zapewniając terminowe wdrożenie odpowiednich zmian.

91. Polityka w zakresie outsourcingu powinna uwzględniać jego wpływ na działalność instytucji oraz na jej ryzyko (np. ryzyko operacyjne, w tym prawne i informatyczne; ryzyko utraty reputacji; oraz ryzyko koncentracji). Polityka ta powinna obejmować rozwiązania w zakresie sprawozdawczości i monitorowania, które należy wdrażać od etapu rozważania umowy outsourcingowej do zakończenia jej obowiązywania (w tym podczas analizy kosztów i korzyści outsourcingu, zawierania umowy outsourcingowej, realizacji umowy do chwili jej wygaśnięcia, wdrażania planów awaryjnych i strategii wyjścia). Instytucja pozostaje w pełni odpowiedzialna za wszystkie usługi i rodzaje działalności podlegające outsourcingowi oraz wynikające z nich decyzje kierownictwa. W związku z tym w polityce w zakresie outsourcingu należy jasno

[20] Niniejsze wytyczne są ograniczone do ogólnej polityki w zakresie outsourcingu; szczegółowe aspekty outsourcingu omówiono w wytycznych CEBS w sprawie outsourcingu, które mają zostać poddane przeglądowi. Wytyczne te są dostępne pod adresem https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing.

wskazać, że rozwiązanie to nie zwalnia instytucji z jej obowiązków regulacyjnych oraz wobec klientów.

92. W polityce należy zawrzeć stwierdzenie, że outsourcing nie powinien utrudniać skutecznego nadzoru inspekcyjnego lub analitycznego nad instytucją oraz nie powinien naruszać żadnych ograniczeń nadzorczych dotyczących usług i działalności. Polityka powinna też obejmować outsourcing wewnątrzgrupowy (np. usługi świadczone przez odrębny podmiot prawny w ramach grupy, do której należy instytucja) i wszelkie konkretne uwarunkowania grupowe.

93. W polityce powinno się zawrzeć wymaganie, aby przy wyborze istotnego dostawcy usług zewnętrznych lub w przypadku outsourcingu usług instytucja musiała uwzględnić to, czy usługodawca ustanowił odpowiednie standardy etyczne lub kodeks postępowania, czy też nie.

Tytuł IV – Kultura ryzyka i prowadzenie działalności

9 Kultura ryzyka

94. Prawidłowa i spójna kultura ryzyka powinna być kluczowym elementem skutecznego zarządzania ryzykiem przez instytucje oraz powinna umożliwiać im podejmowanie prawidłowych i świadomych decyzji.

95. Instytucje powinny wypracować zintegrowaną, obejmującą całość ich działalności kulturę ryzyka opartą na pełnym zrozumieniu i całościowym oglądzie ryzyka, na jakie są narażone, oraz sposobu zarządzania nim, uwzględniając swoją skłonność do podejmowania ryzyka.

96. Instytucje powinny rozwijać kulturę ryzyka przez wdrażanie polityki, komunikację i szkolenia dla pracowników dotyczące działalności, strategii i profilu instytucji, a także dostosować komunikację i szkolenia dla pracowników w celu uwzględnienia obowiązków tych pracowników w zakresie podejmowania ryzyka i zarządzania nim.

97. Pracownicy powinni mieć pełną świadomość swoich obowiązków związanych z zarządzaniem ryzykiem. Zarządzanie ryzykiem nie powinno ograniczać się do specjalistów ds. ryzyka lub komórek kontroli wewnętrznej. Główną odpowiedzialność za bieżące zarządzanie ryzykiem, przy uwzględnieniu skłonności instytucji do podejmowania ryzyka oraz jej zdolności do jego ponoszenia, w zgodzie z jej polityką, procedurami i mechanizmami kontrolnymi, powinny ponosić jednostki biznesowe przy nadzorze ze strony organu zarządzającego.

98. Ugruntowana kultura ryzyka powinna w szczególności obejmować:

    a. Przykład z góry: organ zarządzający powinien być odpowiedzialny za ustalanie oraz komunikowanie podstawowych wartości i oczekiwań instytucji. Zachowanie jego członków powinno odzwierciedlać przyjęte wartości. Kierownictwo instytucji, w tym osoby pełniące najważniejsze funkcje, powinno wnosić wkład w komunikowanie podstawowych wartości i oczekiwań pracownikom w jej obrębie. Pracownicy powinni działać zgodnie ze wszystkimi obowiązującymi przepisami prawa i regulacjami oraz

niezwłocznie przekazywać informacje o zaobserwowanym braku zgodności z nimi na wyższy szczebel w obrębie instytucji lub poza nią (np. do właściwego organu przez proces sygnalizowania nieprawidłowości). Organ zarządzający powinien nieustannie promować, monitorować i oceniać kulturę ryzyka instytucji; rozważyć wpływ kultury ryzyka na stabilność finansową, profil ryzyka i stabilne zarządzanie instytucją; oraz w razie potrzeby wprowadzić zmiany.

b. Odpowiedzialność: stosowni pracownicy na wszystkich szczeblach powinni znać i rozumieć podstawowe wartości instytucji oraz, w zakresie niezbędnym dla wykonywania swojej roli, jej skłonność do podejmowania ryzyka i zdolność do jego ponoszenia. Powinni oni być zdolni do wykonywania swoich ról i mieć świadomość, że będą ponosić odpowiedzialność za swoje działania związane z zachowaniami instytucji w zakresie podejmowania ryzyka.

c. Skuteczna komunikacja i krytyka: prawidłowa kultura ryzyka powinna sprzyjać otwartej komunikacji i skutecznej krytyce – procesy decyzyjne powinny zachęcać do wyrażania szerokiej gamy poglądów, umożliwiać testowanie bieżących praktyk, stymulować konstruktywną krytykę wśród pracowników oraz sprzyjać kreowaniu otwartego i konstruktywnego zaangażowania w całej organizacji.

d. Zachęty: odpowiednie zachęty powinny odgrywać kluczową rolę w dostosowywaniu zachowań w zakresie podejmowania ryzyka do profilu ryzyka instytucji i jej długoterminowych interesów[21].

10 Wartości instytucji i kodeks postępowania

99. Organ zarządzający powinien opracować i przyjąć wysokie standardy etyczne i zawodowe, a następnie powinien ich przestrzegać i je upowszechniać, uwzględniając szczególne potrzeby oraz cechy instytucji, jak też powinien zapewnić wdrożenie takich standardów (przez przyjęcie kodeksu postępowania lub podobnego dokumentu). Powinien on także nadzorować przestrzeganie tych standardów przez pracowników. W stosownych przypadkach organ zarządzający może przyjąć i wdrożyć standardy obowiązujące w całej grupie, do której należy instytucja, bądź wspólne standardy wydane przez stowarzyszenia lub inne stosowne organizacje.

100. Wdrożone standardy powinny mieć na celu zmniejszenie ryzyka, na jakie narażona jest instytucja, w szczególności ryzyka operacyjnego i utraty reputacji, które mogą wywierać znaczący niekorzystny wpływ na rentowność i stabilność instytucji w wyniku kar pieniężnych, kosztów postępowań sądowych, ograniczeń nałożonych przez właściwe organy, innych konsekwencji finansowych i karnych, a także utraty wartości marki i zaufania konsumentów.

[21] Proszę też zapoznać się z wytycznymi EUNB dotyczącymi prawidłowej polityki wynagrodzeń, o których mowa w art. 74 ust. 3 i 75 ust. 2 dyrektywy 2013/36/UE, i ujawniania informacji zgodnie z art. 450 rozporządzenia (UE) nr 575/2013 (EBA/GL/2015/22), dostępnymi pod adresem https://www.eba.europa.eu/regulation-and-policy/remuneration.

101. Organ zarządzający powinien ustanowić jasną i udokumentowaną politykę w zakresie przestrzegania tych standardów. Polityka ta powinna:

    a. zawierać postanowienia wskazujące, że wszystkie działania instytucji powinny być prowadzone zgodnie z obowiązującym prawem i przyjętymi przez nią wartościami;

    b. krzewić świadomość ryzyka, budując ugruntowaną kulturę ryzyka zgodnie z sekcją 9 wytycznych i komunikując oczekiwania organu zarządzającego, zgodnie z którymi działalność nie może wykraczać poza określony poziom skłonności do podejmowania ryzyka i limity określone przez instytucję, a zarazem wskazując odpowiednie obowiązki pracowników;

    c. określać zasady oraz przedstawiać przykłady dopuszczalnych i niedopuszczalnych zachowań związanych w szczególności z nieprawidłowościami w sprawozdawczości finansowej i innymi wykroczeniami w tej dziedzinie, przestępczością gospodarczą oraz finansową (w tym nadużyciami, praniem pieniędzy i praktykami monopolistycznymi, omijaniem sankcji finansowych, przekupstwem i korupcją, manipulacjami rynkowymi, nieprawidłowościami związanymi ze sprzedażą oraz innymi naruszeniami przepisów dotyczących ochrony konsumentów);

    d. wyjaśniać, że oprócz spełnienia wymogów prawnych i regulacyjnych oraz zgodności z polityką wewnętrzną od pracowników oczekuje się uczciwego postępowania oraz wystarczająco umiejętnego i starannego wykonywania obowiązków; oraz

    e. informować pracowników o potencjalnych wewnętrznych i zewnętrznych postępowaniach dyscyplinarnych, postępowaniach sądowych i sankcjach, jakimi mogą skutkować wykroczenia oraz niedopuszczalne zachowania.

102. Instytucje powinny monitorować zgodność z takimi standardami oraz zapewniać, aby pracownicy byli ich świadomi, np. przez szkolenia. Instytucje powinny wyznaczyć komórkę odpowiedzialną za monitorowanie zgodności z kodeksem postępowania lub podobnym dokumentem i ocenę jego naruszeń, a także ustanowić proces postępowania w przypadkach niezgodności. Organ zarządzający powinien otrzymywać regularne sprawozdania z wynikami.

11 Polityka przeciwdziałania konfliktom interesów na poziomie instytucjonalnym

103. Organ zarządzający powinien być odpowiedzialny za ustanawianie, zatwierdzanie i nadzorowanie wdrażania oraz utrzymywania skutecznej polityki w celu identyfikacji i oceny rzeczywistych oraz potencjalnych konfliktów interesów na poziomie instytucjonalnym, zarządzania nimi i ich minimalizacji lub zapobiegania im; konflikty takie mogą powstawać np. związku z różnymi działaniami i rolami danej instytucji lub różnych instytucji objętych zakresem konsolidacji ostrożnościowej bądź różnych linii biznesowych lub też jednostek w obrębie instytucji, bądź też mogą odnosić się do zewnętrznych zainteresowanych stron.

104. Instytucje powinny w ramach swoich zasad organizacyjnych i administracyjnych podjąć odpowiednie kroki w celu wykluczenia niekorzystnego wpływu konfliktów interesów na interesy ich klientów.

105. Środki podejmowane przez instytucje w celu zarządzania konfliktami interesów lub, w stosownych przypadkach, ich minimalizacji powinny być udokumentowane i obejmować między innymi:

    a. odpowiedni podział obowiązków, np. powierzenie czynności będących w konflikcie w związku z przetwarzaniem transakcji lub świadczeniem usług różnym osobom bądź powierzenie odpowiedzialności za nadzór i sprawozdawczość w odniesieniu do czynności będących w konflikcie różnym osobom;

    b. ustanowienie barier informacyjnych, np. przez fizyczne rozdzielenie określonych linii biznesowych lub jednostek; oraz

    c. ustanowienie odpowiednich procedur w odniesieniu do transakcji dokonywanych z jednostkami powiązanymi, np. wymogu, aby były one dokonywane na zasadach rynkowych.

12 Polityka przeciwdziałania konfliktom interesów dla pracowników[22]

106. Organ zarządzający powinien być odpowiedzialny za ustanawianie, zatwierdzanie i nadzorowanie wdrażania oraz utrzymywania skutecznej polityki w celu identyfikacji i oceny rzeczywistych oraz potencjalnych konfliktów między interesami instytucji a prywatnymi interesami pracowników i ich minimalizacji lub zapobiegania im; obejmuje to także konflikty z interesami członków organu zarządzającego, które mogłyby niekorzystnie wpływać na wykonywanie ich obowiązków. Instytucja konsolidująca powinna uwzględniać wszystkie interesy w ujęciu skonsolidowanym lub subskonsolidowanym w ramach ogólnogrupowej polityki przeciwdziałania konfliktom interesów.

107. Polityka ta powinna mieć na celu identyfikację konfliktów interesów pracowników, w tym interesów ich najbliższych członków rodziny. Instytucje powinny uwzględniać fakt, że konflikty interesów mogą wynikać nie tylko z obecnych, ale także z przeszłych relacji osobistych lub zawodowych. W przypadku wystąpienia konfliktów interesów instytucje powinny ocenić ich istotność, podjąć decyzje i w stosownych przypadkach wdrożyć środki w celu ich minimalizacji.

108. W odniesieniu do konfliktów interesów wynikających z wcześniejszych relacji instytucje powinny ustalić odpowiednie ramy czasowe, w których pracownicy powinni zgłaszać takie

[22] Niniejszą sekcję należy interpretować w powiązaniu ze wspólnymi wytycznymi ESMA i EUNB w sprawie oceny kwalifikacji członków organu zarządzającego i osób pełniących najważniejsze funkcje wydanymi na mocy dyrektywy 2013/36/UE i dyrektywy 2014/65/UE.

konflikty interesów, z uwagi na to, że mogą one nadal mieć wpływ na zachowanie pracowników i ich udział w podejmowaniu decyzji.

109. Polityka ta powinna obejmować co najmniej następujące sytuacje lub relacje, w związku z którymi mogą powstawać konflikty interesów:

    a. interesy gospodarcze (np. akcje, inne prawa własności i udziały, holdingi finansowe oraz inne interesy gospodarcze związane z klientami komercyjnymi, prawa własności intelektualnej, kredyty udzielone przez instytucję spółce należącej do pracowników, członkostwo w organie bądź prawo własności organu lub podmiotu mającego sprzeczne interesy);

    b. relacje osobiste lub zawodowe z właścicielami znacznych pakietów akcji w instytucji;

    c. relacje osobiste lub zawodowe z pracownikami instytucji lub podmiotów objętych zakresem konsolidacji ostrożnościowej (np. relacje rodzinne);

    d. inne zatrudnienie oraz poprzednie zatrudnienie w niedawnej przeszłości (np. w ostatnich pięciu latach);

    e. relacje osobiste lub zawodowe z odpowiednimi zewnętrznymi zainteresowanymi stronami (np. związki z istotnymi dostawcami, firmami doradczymi lub innymi dostawcami usług); oraz

    f. wpływy lub relacje polityczne.

110. Niezależnie od powyższego instytucje powinny uwzględnić fakt, że bycie akcjonariuszem instytucji bądź posiadanie prywatnych rachunków, zaciąganie kredytów lub korzystanie z innych usług instytucji nie powinno prowadzić do sytuacji, w której uznaje się, że pracownicy znajdują się w konflikcie interesów, jeśli relacje takie nie przekraczają odpowiedniego progu *de minimis*.

111. W polityce należy określić procesy sprawozdawczości i komunikowania informacji komórce odpowiedzialnej na mocy tej polityki. Pracownicy powinni mieć obowiązek niezwłocznego wewnętrznego ujawniania wszelkich okoliczności mogących skutkować lub skutkujących konfliktem interesów.

112. W polityce należy odróżnić konflikty interesów utrzymujące się i wymagające stałego zarządzania od konfliktów interesów, które zachodzą nieoczekiwanie w odniesieniu do pojedynczego zdarzenia (np. transakcji, wyboru dostawcy usług itp.), i w celu zarządzania nimi wystarczy zazwyczaj zastosować jednorazowy środek. We wszystkich przypadkach w podejmowanych decyzjach należy uwzględniać przede wszystkim interes instytucji.

113. W polityce należy określić procedury, środki, wymagania w zakresie dokumentacji oraz zadania odnoszące się do identyfikacji konfliktów interesów i zapobiegania im, oceny ich istotności oraz

podejmowania środków je minimalizujących. Takie procedury, wymagania, zadania i środki powinny obejmować:

a. powierzanie czynności lub transakcji będących w konflikcie różnym osobom;

b. zapobieganie wywieraniu niewłaściwego wpływu przez pracowników aktywnych również poza instytucją na kwestie związane z taką ich aktywnością;

c. ustanowienie obowiązku wstrzymania się przez członków organu zarządzającego od głosowania nad wszelkimi sprawami, w przypadku których dany członek znajduje się lub może znajdować się w konflikcie interesów bądź jego obiektywność lub też zdolność do należytego wypełniania obowiązków wobec instytucji może ulec zmniejszeniu w inny sposób;

d. ustanowienie odpowiednich procedur dotyczących transakcji z podmiotami powiązanymi (instytucje mogą między innymi rozważyć wymóg, aby transakcje te były dokonywane na warunkach rynkowych, wymóg, aby do takich transakcji pełne zastosowanie miały wszystkie odnośne procedury kontroli wewnętrznej, wymóg wiążących konsultacji z członkami niezależnymi organu zarządzającego, wymóg zatwierdzenia najważniejszych transakcji przez akcjonariuszy oraz ograniczenia ekspozycji na takie transakcje); oraz

e. uniemożliwienie członkom organu zarządzającego pełnienia funkcji dyrektora w konkurencyjnych instytucjach, chyba że funkcje te dotyczą instytucji należących do tego samego instytucjonalnego systemu ochrony, o których mowa w art. 113 ust. 7 rozporządzenia (UE) nr 575/2013, instytucji kredytowych trwale powiązanych z organem centralnym, o których mowa w art. 10 rozporządzenia (UE) nr 575/2013, lub instytucji objętych zakresem konsolidacji ostrożnościowej.

114. W polityce takiej należy w szczególności uwzględnić ryzyko konfliktu interesów na szczeblu organu zarządzającego i dostarczyć wystarczających wskazówek w zakresie identyfikacji konfliktów interesów, które mogłyby zmniejszać zdolność członków organu zarządzającego do podejmowania obiektywnych i bezstronnych decyzji leżących w najlepszym interesie instytucji, oraz w zakresie zarządzania takimi konfliktami interesów. Instytucje powinny uwzględnić fakt, że konflikty interesów mogą mieć wpływ na niezależność myślenia członków organu zarządzającego[23].

115. Rzeczywiste lub potencjalne konflikty interesów, które zostały ujawnione odpowiedzialnej komórce w obrębie instytucji, należy odpowiednio ocenić i zarządzać nimi. Jeżeli stwierdzono konflikt interesów pracowników, instytucja powinna udokumentować podjętą decyzję, w szczególności to, czy konflikt interesów i związane z nim ryzyko zostały zaakceptowane, a jeżeli zostały one zaakceptowane, należy udokumentować, w jaki sposób ten konflikt interesów został w zadowalającym stopniu zminimalizowany lub wyeliminowany.

[23] Zob. też wspólne wytyczne ESMA i EUNB w sprawie oceny kwalifikacji członków organu zarządzającego i osób pełniących najważniejsze funkcje wydane na mocy dyrektywy 2013/36/UE i dyrektywy 2014/65/UE.

116. Wszelkie rzeczywiste i potencjalne konflikty interesów na szczeblu organu zarządzającego powinny być odpowiednio udokumentowane i komunikowane organowi zarządzającemu w ujęciu zarówno indywidualnym, jak i zbiorowym, a organ zarządzający powinien je omawiać, podejmować związane z nimi decyzje i należycie nimi zarządzać.

13 Wewnętrzne procedury ostrzegania

117. Instytucje powinny ustanowić i utrzymywać odpowiednią wewnętrzną politykę ostrzegania oraz procedury umożliwiające pracownikom zgłaszanie potencjalnych lub rzeczywistych naruszeń wymogów regulacyjnych lub wewnętrznych, w tym w szczególności wynikających z przepisów rozporządzenia (UE) nr 575/2013 oraz przepisów krajowych transponujących dyrektywę 2013/36/UE lub zasad zarządzania wewnętrznego, za pośrednictwem określonego, niezależnego i autonomicznego kanału. Od zgłaszających pracowników nie powinno się wymagać dowodów na naruszenie; powinni oni jednak mieć wystarczającą pewność, aby uzasadnione było wszczęcie dochodzenia.

118. Aby uniknąć konfliktów interesów, powinna istnieć możliwość zgłaszania przez pracowników naruszeń poza normalną hierarchią służbową (np. za pośrednictwem komórki ds. nadzoru zgodności z prawem, komórki audytu wewnętrznego lub niezależnej wewnętrznej procedury sygnalizowania nieprawidłowości). Procedury ostrzegania powinny zapewniać ochronę danych osobowych zarówno osoby zgłaszającej naruszenie, jak i osoby fizycznej, której zarzuca się popełnienie naruszenia, zgodnie z dyrektywą 95/46/WE.

119. Procedury ostrzegania powinny być dostępne dla wszystkich pracowników instytucji.

120. Informacje dostarczone przez pracowników za pośrednictwem procedur ostrzegania należy udostępnić organowi zarządzającemu oraz innym odpowiedzialnym komórkom określonym w polityce wewnętrznego ostrzegania. W przypadku gdy żąda tego pracownik zgłaszający naruszenie, informacje powinny być przekazywane organowi zarządzającemu i innym odpowiedzialnym komórkom w sposób anonimowy. Instytucje mogą również ustanowić proces sygnalizowania nieprawidłowości, który umożliwia przekazywanie informacji w sposób anonimowy.

121. Instytucje powinny zapewnić, aby osoba zgłaszająca naruszenie była odpowiednio chroniona przed wszelkimi negatywnymi skutkami, np. odwetem, dyskryminacją lub innymi rodzajami niesprawiedliwego traktowania. Instytucja powinna zapewnić, aby żadna osoba pozostająca pod jej kontrolą nie represjonowała osoby, która zgłosiła naruszenie, a także powinna podjąć odpowiednie środki przeciw osobom odpowiedzialnym za jakiekolwiek tego rodzaju represje.

122. Instytucje powinny również chronić osoby, których dotyczą zgłoszenia, przed wszelkimi negatywnymi skutkami w przypadku, gdy w trakcie dochodzenia nie znaleziono dowodów uzasadniających podjęcie środków przeciwko danej osobie. W przypadku podjęcia środków instytucja powinna podjąć je w taki sposób, aby chronić daną osobę przed niezamierzonymi negatywnymi skutkami wykraczającymi poza cel podjętych środków.

123. W szczególności wewnętrzne procedury ostrzegania powinny:

a. być udokumentowane (np. podręczniki dla pracowników);

b. zawierać jasne reguły zapewniające traktowanie informacji dotyczących osób zgłaszających i zgłaszanych oraz naruszenia jako poufnych zgodnie z dyrektywą 95/46/WE, chyba że ich ujawnienie jest wymagane na mocy prawa krajowego w kontekście dalszych dochodzeń lub późniejszych postępowań sądowych;

c. chronić pracowników, którzy zgłaszają obawy, przed represjami za ujawnienie naruszeń podlegających zgłoszeniu;

d. zapewniać, aby zgłaszane potencjalne lub rzeczywiste naruszenia podlegały ocenie i przekazaniu na wyższy szczebel, w tym w stosownych przypadkach odpowiednim właściwym organom lub organom ścigania;

e. zapewniać, w miarę możliwości, potwierdzenie otrzymania informacji dla pracowników zgłaszających potencjalne lub rzeczywiste naruszenia;

f. zapewniać monitorowanie wyniku dochodzenia w sprawie zgłoszonego naruszenia; oraz

g. zapewniać właściwe prowadzenie ewidencji.

14 Zgłaszanie naruszeń właściwym organom

124. Właściwe organy powinny ustanowić skuteczne i niezawodne mechanizmy umożliwiające pracownikom instytucji zgłaszanie właściwym organom stosownych potencjalnych lub rzeczywistych naruszeń wymogów regulacyjnych, w tym w szczególności wynikających z przepisów rozporządzenia (UE) nr 575/2013 oraz przepisów krajowych transponujących dyrektywę 2013/36/UE. Mechanizmy te powinny obejmować przynajmniej:

a. szczegółowe procedury przyjmowania zgłoszeń dotyczących naruszeń i działań następczych, np. ustanawiające specjalny dział, jednostkę lub komórkę ds. sygnalizowanych nieprawidłowości;

b. odpowiednią ochronę, o której mowa w sekcji 13;

c. ochronę danych osobowych zarówno osoby fizycznej, która zgłasza naruszenie, jak i osoby fizycznej, której zarzuca się popełnienie naruszenia, zgodnie z dyrektywą 95/46/WE; oraz

d. jasne procedury określone w pkt 123.

125. Bez uszczerbku dla możliwości zgłaszania naruszeń za pośrednictwem mechanizmów właściwych organów, właściwe organy mogą zachęcać pracowników, aby najpierw próbowali skorzystać z wewnętrznych procedur ostrzegania swoich instytucji.

Tytuł V – Ramy i mechanizmy kontroli wewnętrznej

15 Ramy kontroli wewnętrznej

126. Instytucje powinny wypracować oraz utrzymywać kulturę zachęcającą do pozytywnego nastawienia do kontroli ryzyka i zgodności z przepisami w ramach instytucji, a także solidne i kompleksowe ramy kontroli wewnętrznej. W tych ramach linie biznesowe instytucji powinny ponosić odpowiedzialność za zarządzanie ryzykiem, jakie ponoszą w związku z prowadzeniem działalności, oraz powinny ustanowić mechanizmy kontrolne mające na celu zapewnienie zgodności z wewnętrznymi i zewnętrznymi wymogami. W związku z tymi ramami instytucje powinny mieć komórki kontroli wewnętrznej dysponujące wystarczającymi uprawnieniami, statusem i dostępem do organu zarządzającego, aby móc wypełniać swoją funkcję, jak też ustanowić ramy zarządzania ryzykiem.

127. Ramy kontroli wewnętrznej instytucji powinny być dostosowane indywidualnie do specyfiki jej działalności, jej złożoności i związanego z nią ryzyka, uwzględniając przy tym kontekst grupy. Instytucje muszą zorganizować wymianę informacji niezbędną w celu zapewnienia, aby każdy organ zarządzający, linia biznesowa i jednostka wewnętrzna, w tym każda komórka kontroli wewnętrznej, mogły wypełniać swoje obowiązki. Oznacza to na przykład niezbędną wymianę odpowiednich informacji między liniami biznesowymi a komórką ds. nadzoru zgodności z prawem na poziomie grupy oraz między kierownikami komórek kontroli wewnętrznej na szczeblu grupy a organem zarządzającym instytucji.

128. Ramy kontroli wewnętrznej powinny obejmować całą organizację, w tym obowiązki i zadania organu zarządzającego oraz działalność wszystkich linii biznesowych i jednostek wewnętrznych, w tym komórek kontroli wewnętrznej, czynności objęte outsourcingiem i kanały dystrybucji.

129. Ramy kontroli wewnętrznej instytucji powinny zapewniać:

a. skuteczną i efektywną działalność;

b. ostrożne prowadzenie działalności;

c. odpowiednią identyfikację, pomiar i minimalizację ryzyka;

d. wiarygodność informacji finansowych i niefinansowych objętych sprawozdawczością zarówno wewnętrzną, jak i zewnętrzną;

e. właściwe procedury administracyjne i księgowe; oraz

f. zgodność z przepisami, regulacjami, wymogami nadzorczymi oraz polityką wewnętrzną instytucji, jej procesami, regulaminami i decyzjami.

16 Wdrażanie ram kontroli wewnętrznej

130. Organ zarządzający powinien być odpowiedzialny za ustanowienie i monitorowanie adekwatności oraz skuteczności ram kontroli wewnętrznej, procesów i mechanizmów, a także za nadzorowanie wszystkich linii biznesowych i jednostek wewnętrznych, w tym komórek kontroli wewnętrznej (takich jak komórki ds. zarządzania ryzykiem, ds. nadzoru zgodności z prawem i audytu wewnętrznego). Instytucje powinny ustanowić, utrzymywać i regularnie aktualizować odpowiednią pisemną politykę, mechanizmy i procedury kontroli wewnętrznej, które powinny zostać zatwierdzone przez organ zarządzający.

131. Instytucja powinna mieć jasny, przejrzysty i udokumentowany proces decyzyjny oraz jasny podział obowiązków i uprawnień związanych z ramami kontroli wewnętrznej, obejmujący jej linie biznesowe, jednostki wewnętrzne i komórki kontroli wewnętrznej.

132. Instytucje powinny komunikować tę politykę, mechanizmy i procedury wszystkim pracownikom za każdym razem, gdy zostają w nich wprowadzone istotne zmiany.

133. Wdrażając ramy kontroli wewnętrznej, instytucje powinny ustanowić odpowiedni podział obowiązków, np. powierzenie czynności będących w konflikcie w związku z przetwarzaniem transakcji lub świadczeniem usług różnym osobom bądź powierzenie odpowiedzialności za nadzór i sprawozdawczość w odniesieniu do czynności będących w konflikcie różnym osobom – oraz ustanowić bariery informacyjne, np. przez fizyczne rozdzielenie określonych działów.

134. Komórki kontroli wewnętrznej powinny sprawdzać, czy polityka, mechanizmy i procedury określone w ramach kontroli wewnętrznej są prawidłowo wdrażane w ich poszczególnych obszarach właściwości.

135. Komórki kontroli wewnętrznej powinny regularnie przedkładać organowi zarządzającemu sprawozdania dotyczące zidentyfikowanych ważnych uchybień. W sprawozdaniach należy zawrzeć w przypadku każdego nowego zidentyfikowanego ważnego uchybienia opis związanego z nim ryzyka, ocenę skutków, zalecenia oraz wskazanie środków naprawczych, jakie należy podjąć. Organ zarządzający powinien podjąć w stosownym czasie skuteczne działania następcze w związku z ustaleniami komórek kontroli wewnętrznej oraz zażądać odpowiednich działań naprawczych. Należy ustanowić formalną procedurę działań następczych związanych z ustaleniami i podjętymi środkami naprawczymi.

17 Ramy zarządzania ryzykiem

136. W ramach ogólnych ram kontroli wewnętrznej instytucje powinny posiadać całościowe ramy zarządzania ryzykiem obejmujące wszystkie linie biznesowe i jednostki wewnętrzne w obrębie instytucji, w tym komórki kontroli wewnętrznej, które to ramy powinny w pełni uwzględniać

ekonomiczną istotę wszystkich ekspozycji instytucji na ryzyko. Ramy zarządzania ryzykiem powinny umożliwiać instytucji podejmowanie w pełni świadomych decyzji w sprawie podejmowanego ryzyka. Ramy zarządzania ryzykiem powinny obejmować zarówno ryzyko ujęte w bilansie, jak i pozabilansowe, a także rzeczywiste i przyszłe ryzyko, na jakie może być narażona instytucja. Ocena ryzyka powinna mieć charakter oddolny i odgórny oraz być dokonywana w obrębie poszczególnych linii biznesowych i między nimi, z wykorzystaniem spójnej terminologii i konsekwentnej metodyki w obrębie całej instytucji, a także na poziomie skonsolidowanym lub subskonsolidowanym. W ramach zarządzania ryzykiem należy wziąć pod uwagę wszystkie istotne rodzaje ryzyka, z należytym uwzględnieniem ryzyka zarówno finansowego, jak i niefinansowego, w tym ryzyka kredytowego, rynkowego, płynności, koncentracji, operacyjnego, informatycznego, utraty reputacji, prawnego, związanego z postępowaniem, zgodnością z prawem i strategicznego.

137. Ramy zarządzania ryzykiem instytucji powinny obejmować politykę, procedury, limity ryzyka i mechanizmy jego kontrolowania umożliwiające odpowiednią, dokonywaną w stosownym czasie i nieustanną identyfikację, pomiar lub ocenę, monitorowanie, minimalizację i sprawozdawczość ryzyka na poziomie linii biznesowej, całej instytucji oraz na poziomie skonsolidowanym lub subskonsolidowanym, a także zarządzanie tym ryzykiem.

138. Ramy zarządzania ryzykiem instytucji powinny dostarczać konkretnych wskazówek na temat wdrażania jej strategii. W stosownych przypadkach we wskazówkach tych należy ustanowić i utrzymywać limity wewnętrzne zgodne ze skłonnością instytucji do podejmowania ryzyka oraz dostosowane do potrzeb jej prawidłowego działania, siły finansowej, bazy kapitałowej i celów strategicznych. Profil ryzyka instytucji nie powinien przekraczać tych limitów. Ramy zarządzania ryzykiem powinny zapewniać, aby w przypadku wystąpienia naruszeń limitów następowało ich przekazanie na wyższy poziom kompetencji w celu zajęcia się nimi wraz z podjęciem odpowiednich działań następczych.

139. Ramy zarządzania ryzykiem powinny podlegać niezależnemu przeglądowi wewnętrznemu, np. dokonywanemu przez komórkę audytu wewnętrznego, oraz regularnej ocenie pod kątem skłonności instytucji do podejmowania ryzyka, przy uwzględnieniu informacji od komórki ds. zarządzania ryzykiem oraz w stosownych przypadkach komitetu ds. ryzyka. Należy przy tym rozważyć takie czynniki, jak wydarzenia wewnętrzne i zewnętrzne, w tym zmiany sumy bilansowej i przychodów; wszelki wzrost złożoności działalności instytucji, profilu ryzyka lub struktury operacyjnej; ekspansję geograficzną; połączenia i przejęcia; oraz wprowadzanie nowych produktów lub linii biznesowych.

140. W odniesieniu do identyfikacji oraz pomiaru lub oceny ryzyka instytucja powinna opracować odpowiednie metodyki obejmujące zarówno narzędzia prognostyczne, jak i retrospektywne. Metodyki te powinny umożliwiać agregację ekspozycji na ryzyko w obrębie różnych linii biznesowych oraz pomagać w identyfikacji koncentracji ryzyka. Narzędzia powinny obejmować ocenę rzeczywistego profilu ryzyka w porównaniu do skłonności instytucji do podejmowania ryzyka, a także określenie i ocenę potencjalnych ekspozycji na ryzyko, także w warunkach skrajnych, w różnych zakładanych niekorzystnych okolicznościach w porównaniu do zdolności

instytucji do ponoszenia ryzyka. Narzędzia powinny dostarczać informacji o wszelkich niezbędnych korektach profilu ryzyka. Instytucje powinny przyjmować odpowiednio ostrożne założenia przy opracowywaniu scenariuszy warunków skrajnych.

141. Instytucje powinny brać pod uwagę, że wyniki ocen ilościowych, w tym testów warunków skrajnych, są silnie uzależnione od ograniczeń i założeń związanych z modelami (w tym wagi i czasu trwania szoku oraz związanych z nim rodzajów ryzyka). Na przykład wyniki sugerujące bardzo wysoką stopę zwrotu z kapitału ekonomicznego mogą wynikać z niedoskonałości modelu (np. nieuwzględnienia części istotnych rodzajów ryzyka), nie zaś z doskonałości strategii lub jej znakomitego wdrożenia przez instytucję. W związku z tym poziomu podejmowanego ryzyka nie należy określać wyłącznie w oparciu o informacje ilościowe czy wyniki modeli, lecz także z zastosowaniem podejścia jakościowego (z uwzględnieniem oceny ekspertów i krytycznej analizy). Należy wyraźnie uwzględnić istotne tendencje i dane makroekonomiczne, aby zidentyfikować ich potencjalny wpływ na ekspozycje oraz portfele.

142. Ostateczna odpowiedzialność za ocenę ryzyka spoczywa wyłącznie na instytucji, która powinna w związku z tym dokonać krytycznej analizy ryzyka, nie polegając wyłącznie na ocenach zewnętrznych. Instytucja powinna na przykład dokonać walidacji zakupionego modelu ryzyka i skalibrować go odpowiednio do swojej sytuacji, aby zapewnić dokładne i kompleksowe ujęcie ryzyka oraz jego analizę.

143. Instytucje powinny być w pełni świadome ograniczeń modeli i metryk oraz wykorzystywać nie tylko ilościowe, ale również jakościowe narzędzia oceny ryzyka (w tym ocenę ekspertów i krytyczną analizę).

144. Oprócz własnych ocen instytucji mogą one wykorzystywać zewnętrzne oceny ryzyka (w tym zewnętrzne ratingi kredytowe lub modele ryzyka zakupione od dostawców zewnętrznych). Instytucje powinny być w pełni świadome dokładnego zakresu takich ocen i ich ograniczeń.

145. Należy ustanowić regularne i przejrzyste mechanizmy sprawozdawczości, tak aby organ zarządzający, jego komitet ds. ryzyka (jeżeli został ustanowiony) i wszystkie stosowne jednostki w obrębie instytucji otrzymywały w stosownym czasie dokładne, zwięzłe, zrozumiałe i istotne sprawozdania oraz mogły wymieniać stosowne informacje dotyczące identyfikacji, pomiaru lub oceny i monitorowania ryzyka oraz zarządzania nim. Ramy sprawozdawczości powinny być dobrze określone i udokumentowane.

146. Skuteczne przekazywanie informacji i poziom świadomości na temat ryzyka oraz strategii w zakresie ryzyka jest bardzo ważnym elementem całego procesu zarządzania ryzykiem, a także procesów przeglądu i decyzyjnych, oraz pomaga zapobiegać decyzjom mogącym nieświadomie zwiększać ryzyko. Skuteczna sprawozdawczość ryzyka wymaga wnikliwego wewnętrznego rozważenia i prawidłowego zakomunikowania strategii w zakresie ryzyka oraz stosownych danych na jego temat (np. o ekspozycjach i kluczowych wskaźnikach ryzyka) zarówno horyzontalnie w obrębie instytucji, jak i w górę oraz w dół hierarchii służbowej.

18 Nowe produkty i znaczące zmiany[24]

147. Instytucja powinna ustanowić zatwierdzoną przez organ zarządzający, dobrze udokumentowaną politykę zatwierdzania nowych produktów („PZNP"), która obejmuje rozwój nowych rynków, produktów i usług oraz znaczące zmiany dotychczasowych rynków, produktów i usług, jak też wyjątkowe transakcje. Polityka ta powinna ponadto obejmować istotne zmiany powiązanych procesów (np. nowe zasady outsourcingu) i systemów (np. procesów zmian w zakresie informatyki). PZNP powinna zapewnić, aby zatwierdzone produkty i zmiany były spójne ze strategią w zakresie ryzyka i skłonnością instytucji do podejmowania ryzyka oraz z odpowiednimi limitami, bądź też powinna zapewnić wprowadzenie niezbędnych zmian.

148. Do istotnych zmian lub wyjątkowych transakcji mogą należeć połączenia i przejęcia, w tym potencjalne konsekwencje niewystarczających procedur *due diligence*, w trakcie których nie zidentyfikowano ryzyka oraz zobowiązań pojawiających się po połączeniu; tworzenie struktur (np. nowych jednostek zależnych lub spółek celowych); nowe produkty; zmiany systemów bądź ram lub procedur zarządzania ryzykiem; oraz zmiany organizacji instytucji.

149. Instytucja powinna mieć konkretne procedury oceny zgodności z tą polityką, uwzględniając wkład komórki ds. zarządzania ryzykiem. Powinny one obejmować systematyczną uprzednią ocenę i udokumentowaną opinię wydaną przez komórkę ds. nadzoru zgodności z prawem w odniesieniu do nowych produktów lub znaczących zmian dotychczasowych produktów.

150. PZNP instytucji powinna uwzględniać wszystkie czynniki, które należy wziąć pod uwagę przed podjęciem decyzji o wejściu na nowe rynki, obrocie nowymi produktami, wdrożeniu nowej usługi lub wprowadzeniu znaczących zmian dotychczasowych produktów lub usług. PZNP powinna także zawierać definicje „nowego produktu/rynku/działalności" oraz „znaczących zmian" wykorzystywaną w obrębie organizacji i komórek wewnętrznych mających uczestniczyć w procesie decyzyjnym.

151. PZNP powinna wskazywać najważniejsze zagadnienia, którym należy poświęcić uwagę przed podjęciem decyzji. Są to między innymi zgodność z regulacjami; rachunkowość; modele wyceny; wpływ na profil ryzyka; adekwatność kapitałowa i rentowność, dostępność wystarczających zasobów w jednostkach operacyjnych (ang. *front office*), rozliczeniowych (ang. *back office*) oraz odpowiedzialnych za zarządzanie ryzykiem i infrastrukturą informatyczną (ang. *middle office*); oraz dostępność narzędzi wewnętrznych i wiedzy fachowej wystarczającej, aby zrozumieć i monitorować stosowne ryzyko. W decyzji o podjęciu nowej działalności należy wyraźnie wskazać jednostkę biznesową i osoby za nią odpowiedzialne. Nowej działalności nie należy podejmować do chwili uzyskania zasobów wystarczających dla zrozumienia związanego z nią ryzyka i zarządzania nim.

[24] Zob. też wytyczne EUNB dotyczące zasad nadzoru nad produktami i wymogów zarządczych dla producentów i dystrybutorów produktów bankowości detalicznej dostępne pod adresem https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products.

152. W zatwierdzaniu nowych produktów lub znaczących zmian dotychczasowych produktów, procesów i systemów powinny uczestniczyć komórka ds. zarządzania ryzykiem i komórka ds. nadzoru zgodności z prawem. Ich wkład powinien obejmować pełną i obiektywną ocenę ryzyka wynikającego z nowej działalności w różnych scenariuszach, ocenę wszelkich potencjalnych uchybień w zarządzaniu ryzykiem przez instytucję oraz ramach kontroli wewnętrznej, jak też ocenę zdolności instytucji do skutecznego zarządzania nowym ryzykiem. Komórka ds. zarządzania ryzykiem powinna też mieć jasny ogląd wdrażania nowych produktów (lub znaczących zmian dotychczasowych produktów, procesów i systemów) w ramach poszczególnych linii biznesowych i portfeli oraz uprawnienia pozwalające żądać poddania zmian dotychczasowych produktów formalnemu procesowi PZNP.

19 Komórki kontroli wewnętrznej

153. Wśród komórek kontroli wewnętrznej powinna znaleźć się komórka ds. zarządzania ryzykiem (zob. sekcję 20), komórka ds. nadzoru zgodności z prawem (zob. sekcję 21) oraz komórka audytu wewnętrznego (zob. sekcję 22). Komórki ds. zarządzania ryzykiem i ds. nadzoru zgodności z prawem powinny podlegać przeglądowi ze strony komórki audytu wewnętrznego.

154. Zadania operacyjne komórek kontroli wewnętrznej mogą zostać zlecone w ramach outsourcingu, z uwzględnieniem kryteriów proporcjonalności wymienionych w tytule I, instytucji konsolidującej lub innemu podmiotowi należącemu do grupy bądź podmiotowi spoza niej za zgodą organów zarządzających danych instytucji. Nawet w przypadku gdy zadania operacyjne w zakresie kontroli wewnętrznej zostały częściowo lub w pełni objęte outsourcingiem, kierownik danej komórki kontroli wewnętrznej i organ zarządzający pozostają odpowiedzialni za te działania oraz za utrzymanie komórki kontroli wewnętrznej w instytucji.

19.1 Kierownicy komórek kontroli wewnętrznej

155. Kierownicy komórek kontroli wewnętrznej powinni znajdować się na odpowiednim poziomie hierarchii, który zapewnia kierownikowi komórki kontrolnej odpowiednie uprawnienia i status niezbędny do wypełniania jego obowiązków. Niezależnie od ogólnej odpowiedzialności organu zarządzającego kierownicy komórek kontroli wewnętrznej powinni być niezależni od kontrolowanych przez siebie linii biznesowych lub jednostek. W tym celu kierownicy komórek ds. zarządzania ryzykiem, ds. nadzoru zgodności z prawem i audytu wewnętrznego powinni podlegać organowi zarządzającemu oraz ponosić bezpośrednią odpowiedzialność przed nim, a oceny ich wyników powinien dokonywać organ zarządzający.

156. Gdy jest to niezbędne, kierownicy komórek kontroli wewnętrznej powinni mieć dostęp do organu zarządzającego pełniącego funkcję nadzorczą, aby zgłaszać mu swoje obawy i ostrzegać go w stosownych przypadkach o konkretnych wydarzeniach wpływających lub mogących wpływać na instytucję. Nie powinno to uniemożliwiać kierownikom komórek kontroli wewnętrznej sprawozdawczości w obrębie swojej regularnej hierarchii podległości służbowej.

157. Instytucje powinny ustanowić udokumentowane procesy mianowania kierownika komórki kontroli wewnętrznej oraz cofania jego uprawnień. W każdym przypadku kierowników komórek kontroli wewnętrznej nie powinno się – a na mocy art. 76 ust. 5 dyrektywy 2013/36/UE kierownika komórki ds. zarządzania ryzykiem nie wolno – usuwać bez uprzedniej zgody organu zarządzającego pełniącego funkcję nadzorczą. W istotnych instytucjach właściwe organy powinny być niezwłocznie informowane o zatwierdzeniu i głównych powodach usunięcia kierownika komórki kontroli wewnętrznej.

19.2 Niezależność komórek kontroli wewnętrznej

158. Aby komórki kontroli wewnętrznej były uznawane za niezależne, powinny zostać spełnione następujące warunki:

a. ich pracownicy nie wykonują żadnych zadań operacyjnych wchodzących w zakres działalności, którą komórki kontroli wewnętrznej mają monitorować i kontrolować;

b. są one oddzielone organizacyjnie od działalności, którą mają monitorować i kontrolować;

c. niezależnie od ogólnej odpowiedzialności członków organu zarządzającego za instytucję kierownik komórki kontroli wewnętrznej nie powinien podlegać osobie ponoszącej odpowiedzialność za zarządzanie działalnością, którą monitoruje i kontroluje komórka kontroli wewnętrznej; oraz

d. wynagrodzenie pracowników komórek kontroli wewnętrznej nie powinno być uzależnione od wyników działalności, którą monitoruje i kontroluje komórka kontroli wewnętrznej, oraz nie powinno w inny sposób potencjalnie negatywnie wpływać na ich obiektywizm[25].

19.3 Łączenie komórek kontroli wewnętrznej

159. Z uwzględnieniem kryteriów proporcjonalności określonych w tytule I, komórka ds. zarządzania ryzykiem i komórka ds. nadzoru zgodności z prawem mogą być łączone. Komórka audytu wewnętrznego nie powinna być łączona z żadną inną komórką kontroli wewnętrznej.

19.4 Zasoby komórek kontroli wewnętrznej

160. Komórki kontroli wewnętrznej powinny dysponować wystarczającymi zasobami. Powinny one dysponować odpowiednią liczbą wykwalifikowanych pracowników (zarówno na poziomie jednostki dominującej, jak i na poziomie jednostek zależnych). Poziom kwalifikacji pracowników powinien być utrzymywany na bieżąco i powinni oni odbywać niezbędne szkolenia.

[25] Zob. też wytyczne EUNB dotyczące prawidłowej polityki wynagrodzeń dostępne pod adresem https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

161. Komórki kontroli wewnętrznej powinny dysponować odpowiednimi systemami informatycznymi i wsparciem oraz dostępem do informacji wewnętrznych i zewnętrznych niezbędnych w celu wykonywania ich zadań. Powinny one mieć dostęp do wszelkich niezbędnych informacji dotyczących wszystkich linii biznesowych i odpowiednich jednostek zależnych ponoszących ryzyko, w szczególności tych, które mogą potencjalnie generować istotne ryzyko dla instytucji.

20 Komórka ds. zarządzania ryzykiem

162. Instytucje powinny ustanowić komórkę ds. zarządzania ryzykiem (KZR) obejmującą całą instytucję. KZR powinna dysponować wystarczającymi uprawnieniami, statusem i zasobami, uwzględniając kryteria proporcjonalności wymienione w tytule I, aby wdrażać politykę w zakresie ryzyka i ramy zarządzania ryzykiem określone w sekcji 17.

163. KZR powinna dysponować, w razie konieczności, bezpośrednim dostępem do organu zarządzającego pełniącego funkcję nadzorczą i jego komitetów, o ile zostały one ustanowione, w szczególności do komitetu ds. ryzyka.

164. KZR powinna mieć dostęp do wszystkich linii biznesowych i innych jednostek wewnętrznych, które mogą generować ryzyko, a także do odpowiednich jednostek zależnych i stowarzyszonych.

165. Pracownicy KZR powinni posiadać wystarczającą wiedzę, umiejętności i doświadczenie w odniesieniu do technik i procedur zarządzania ryzykiem, a także rynków i produktów, jak też powinni mieć dostęp do regularnych szkoleń.

166. KZR powinna być niezależna od linii biznesowych i jednostek, których ryzyko kontroluje, ale nie można jej uniemożliwiać współdziałania z nimi. Współdziałanie między komórkami operacyjnymi a KZR powinno przyczyniać się do osiągnięcia celu, którym jest odpowiedzialność wszystkich pracowników instytucji za zarządzanie ryzykiem.

167. KZR powinna być centralnym elementem organizacyjnym instytucji, a struktura komórki powinna umożliwiać jej wdrażanie polityki w zakresie ryzyka oraz kontrolę ram zarządzania ryzykiem. KZR powinna odgrywać kluczową rolę w zapewnieniu, aby instytucja ustanowiła skuteczne procesy zarządzania ryzykiem. KZR powinna aktywnie uczestniczyć w podejmowaniu wszystkich istotnych decyzji dotyczących zarządzania ryzykiem.

168. Istotne instytucje mogą rozważyć ustanowienie specjalnych KZR dla wszystkich istotnych linii biznesowych. Powinna jednak funkcjonować centralna KZR, w tym grupowa KZR w instytucji konsolidującej, w celu dostarczenia obejmującego całą instytucję i grupę oglądu wszystkich rodzajów ryzyka oraz w celu zapewnienia przestrzegania strategii w zakresie ryzyka.

169. KZR powinna dostarczać stosownych niezależnych informacji, analiz oraz ocen ekspertów dotyczących ekspozycji na ryzyko, jak też porad na temat propozycji i decyzji dotyczących ryzyka podejmowanych przez linie biznesowe lub jednostki wewnętrzne, oraz powinna

informować organ zarządzający, czy są one zgodne ze skłonnością instytucji do podejmowania ryzyka i jej strategią w zakresie ryzyka. KZR może zalecać usprawnienie ram zarządzania ryzykiem oraz środki naprawcze w celu zaradzenia naruszeniom polityki, procedur i limitów w zakresie ryzyka.

20.1 Rola KZR w odniesieniu do strategii i decyzji w zakresie ryzyka

170. KZR powinna aktywnie uczestniczyć na wczesnym etapie w opracowywaniu strategii instytucji w zakresie ryzyka oraz w zapewnieniu, aby instytucja ustanowiła skuteczne procesy zarządzania ryzykiem. KZR powinna dostarczyć organowi zarządzającemu wszelkich istotnych informacji związanych z ryzykiem, aby umożliwić mu ustalenie poziomu skłonności instytucji do podejmowania ryzyka. KZR powinna ocenić solidność i trwałość strategii w zakresie ryzyka oraz skłonności do jego podejmowania. Powinna ona zapewnić, aby skłonność do podejmowania ryzyka przekładała się na konkretne limity ryzyka. KZR powinna również ocenić strategie w zakresie ryzyka jednostek biznesowych, oraz powinna zaangażować się w podejmowanie decyzji dotyczących strategii w zakresie ryzyka przez organ zarządzający. Cele powinny być wiarygodne i spójne ze strategią instytucji w zakresie ryzyka.

171. Zaangażowanie KZR w proces decyzyjny powinno zapewnić uwzględnienie w odpowiedni sposób zagadnień związanych z ryzykiem. Odpowiedzialność za podejmowane decyzje powinny wszakże ponosić jednostki biznesowe i wewnętrzne, a w ostatecznym rozrachunku organ zarządzający.

20.2 Rola KZR w odniesieniu do istotnych zmian

172. Zgodnie z sekcją 18, zanim zostaną podjęte decyzje dotyczące istotnych zmian lub wyjątkowych transakcji, KZR powinna wziąć udział w ocenie skutków takich zmian i wyjątkowych transakcji dla ogólnego ryzyka instytucji oraz grupy, oraz powinna przedstawić swoje ustalenia bezpośrednio organowi zarządzającemu przed podjęciem decyzji.

173. KZR powinna ocenić wpływ, jaki wszelkie zidentyfikowane rodzaje ryzyka mogą wywrzeć na zdolność instytucji lub grupy do zarządzania jej profilem ryzyka, jej płynność oraz solidność bazy kapitałowej w normalnych i niekorzystnych okolicznościach.

20.3 Rola KZR w identyfikacji, pomiarze, ocenie, minimalizacji, monitorowaniu i raportowaniu ryzyka oraz zarządzaniu nim

174. KZR powinna zapewnić, aby wszystkie rodzaje ryzyka były identyfikowane, oceniane, mierzone, monitorowane, zarządzane i odpowiednio raportowane przez odpowiednie jednostki w instytucji.

175. KZR powinna zapewnić, aby identyfikacja i ocena nie opierały się wyłącznie na danych ilościowych lub wynikach modeli, lecz uwzględniały także podejścia jakościowe. KZR powinna na bieżąco informować organ zarządzający o przyjętych założeniach oraz potencjalnych wadach modeli ryzyka i jego analizy.

176. KZR powinna zapewnić przegląd transakcji z jednostkami powiązanymi oraz identyfikację i odpowiednią ocenę ryzyka, jakie stwarzają one dla instytucji.

177. KZR powinna zapewnić skuteczne monitorowanie wszystkich zidentyfikowanych rodzajów ryzyka przez jednostki biznesowe.

178. KZR powinna regularnie monitorować rzeczywisty profil ryzyka instytucji oraz oceniać go w kontekście jej celów strategicznych i skłonności do podejmowania ryzyka, aby umożliwić podejmowanie decyzji przez organ zarządzający pełniący funkcję zarządczą i ich kontrolę przez organ zarządzający pełniący funkcję nadzorczą.

179. KZR powinna analizować tendencje oraz rozpoznawać ryzyko nowe lub rosnące wskutek zmian okoliczności i warunków. Powinna również regularnie porównywać rzeczywiste wyniki w zakresie ryzyka z wcześniejszymi szacunkami (tj. dokonywać weryfikacji historycznej), aby ocenić i poprawić dokładność oraz skuteczność procesu zarządzania ryzykiem.

180. KZR powinna oceniać możliwe sposoby minimalizacji ryzyka. Sprawozdawczość dla organu zarządzającego powinna obejmować proponowane odpowiednie działania mające na celu minimalizację ryzyka.

20.4 Rola KZR w odniesieniu do niezatwierdzonych ekspozycji

181. KZR powinna dokonywać niezależnej oceny przypadków naruszeń skłonności do podejmowania ryzyka lub limitów (ustalając ich przyczyny oraz analizując pod kątem prawnym i ekonomicznym rzeczywisty koszt zamknięcia, redukcji lub zabezpieczenia ekspozycji w porównaniu z potencjalnym kosztem jej utrzymywania). KZR powinna informować właściwe jednostki biznesowe oraz organ zarządzający i zalecać możliwe działania naprawcze. W przypadku gdy naruszenie jest istotne, KZR powinna przedstawić sprawozdanie bezpośrednio organowi zarządzającemu pełniącemu funkcję nadzorczą, bez uszczerbku dla sprawozdawczości KZR dla innych wewnętrznych komórek i komitetów.

182. KZR powinna odgrywać kluczową rolę w zapewnieniu, aby decyzje w sprawie jej zaleceń były podejmowane na stosownym poziomie, przestrzegane przez stosowne jednostki biznesowe oraz odpowiednio raportowane organowi zarządzającemu i komitetowi ds. ryzyka, jeżeli został on ustanowiony.

20.5 Kierownik komórki ds. zarządzania ryzykiem

183. Kierownik KZR powinien być odpowiedzialny za dostarczenie kompleksowych i zrozumiałych informacji na temat ryzyka oraz doradztwo dla organu zarządzającego, umożliwiając temu

organowi zrozumienie ogólnego profilu ryzyka instytucji. To samo dotyczy kierownika KZR instytucji dominującej na poziomie skonsolidowanym.

184. Kierownik KZR powinien posiadać wystarczającą wiedzę fachową, niezależność i staż, aby móc kwestionować decyzje mające wpływ na ekspozycję instytucji na ryzyko. W przypadku gdy kierownik KZR nie jest członkiem organu zarządzającego, istotne instytucje powinny wyznaczyć niezależnego kierownika KZR, który nie ponosi odpowiedzialności za inne komórki i podlega bezpośrednio organowi zarządzającemu. W przypadku gdy nie byłoby proporcjonalne mianowanie osoby, która pełniłaby wyłącznie rolę kierownika KZR, z uwzględnieniem zasady proporcjonalności określonej w tytule I, funkcja ta może być połączona z funkcją kierownika komórki ds. nadzoru zgodności z prawem lub też może być wykonywana przez innego wyższego szczeblem pracownika pod warunkiem, że między łączonymi funkcjami nie zachodzi konflikt interesów. W każdym przypadku osoba ta powinna dysponować wystarczającymi uprawnieniami, statusem i niezależnością (np. być dyrektorem działu prawnego).

185. Kierownik KZR powinien mieć możliwość kwestionowania decyzji podejmowanych przez kierownictwo instytucji i jej organ zarządzający, a podstawy takiego sprzeciwu należy formalnie udokumentować. Jeżeli instytucja pragnie przyznać kierownikowi KZR prawo weta wobec decyzji (np. kredytowych lub inwestycyjnych bądź dotyczących ustanowienia limitów) podejmowanych na szczeblach poniżej organu zarządzającego, powinna ona określić zakres takiego prawa weta, procedury przekazywania sprawy na wyższy szczebel lub odwoławcze, a także sposób zaangażowania organu zarządzającego.

186. Instytucje powinny ustanowić cechujące się zaostrzonymi kryteriami procesy zatwierdzania decyzji negatywnie zaopiniowanych przez kierownika KZR. Organ zarządzający pełniący funkcję nadzorczą powinien mieć możliwość bezpośredniego omówienia z kierownikiem KZR najważniejszych zagadnień związanych z ryzykiem, w tym potencjalnych niezgodności ze skłonnością instytucji do podejmowania ryzyka i jej strategią w zakresie ryzyka.

21 Komórka ds. nadzoru zgodności z prawem

187. Instytucje powinny ustanowić stałą, skuteczną komórkę ds. nadzoru zgodności z prawem w celu zarządzania ryzykiem braku zgodności oraz mianować osobę odpowiedzialną za tę komórkę w obrębie całej instytucji (pracownika ds. nadzoru zgodności z prawem lub kierownika ds. nadzoru zgodności z prawem).

188. W przypadku gdy nie byłoby proporcjonalne mianowanie osoby, która pełniłaby wyłącznie rolę kierownika ds. nadzoru zgodności z prawem, z uwzględnieniem zasady proporcjonalności określonej w tytule I, funkcja ta może być połączona z funkcją kierownika KZR lub też może być wykonywana przez innego wyższego szczeblem pracownika (np. dyrektora działu prawnego) pod warunkiem, że między łączonymi funkcjami nie zachodzi konflikt interesów.

189. Komórka ds. nadzoru zgodności z prawem, w tym jej kierownik, powinna być niezależna od linii biznesowych i jednostek wewnętrznych, które kontroluje, oraz dysponować wystarczającymi

uprawnieniami, statusem i zasobami. Z uwzględnieniem kryteriów proporcjonalności określonych w tytule I, komórka ta może być wspomagana przez KZR bądź połączona z KZR lub innymi odpowiednimi komórkami, np. działem prawnym lub kadrowym.

190. Pracownicy komórki ds. nadzoru zgodności z prawem powinni posiadać wystarczającą wiedzę, umiejętności i doświadczenie w odniesieniu do nadzoru zgodności z prawem i odpowiednich procedur, jak też powinni mieć dostęp do regularnych szkoleń.

191. Organ zarządzający pełniący funkcję nadzorczą powinien nadzorować wdrożenie należycie udokumentowanej polityki nadzoru zgodności z prawem, która powinna być komunikowana wszystkim pracownikom. Instytucje powinny ustanowić proces regularnej oceny zmian prawa i regulacji mających zastosowanie do ich działalności.

192. Komórka ds. nadzoru zgodności z prawem powinna doradzać organowi zarządzającemu w sprawie środków, które należy podjąć w celu zapewnienia zgodności z obowiązującymi przepisami, zasadami, regulacjami oraz standardami, a także oceniać możliwy wpływ ewentualnych zmian w otoczeniu prawnym lub regulacyjnym na działalność instytucji i ramy nadzoru zgodności z prawem.

193. Komórka ds. nadzoru zgodności z prawem powinna zapewnić, aby monitorowanie zgodności z prawem było prowadzone w ramach ustrukturyzowanego i należycie określonego programu monitorowania zgodności oraz aby była przestrzegana polityka nadzoru zgodności z prawem. Komórka ds. nadzoru zgodności z prawem powinna podlegać organowi zarządzającemu i w stosownych przypadkach komunikować się z KZR w sprawie ryzyka braku zgodności w instytucji oraz zarządzania nim. Komórka ds. nadzoru zgodności z prawem i KZR powinny w stosownych przypadkach współpracować i wymieniać informacje, aby móc wykonywać swoje zadania. Ustalenia komórki ds. nadzoru zgodności z prawem powinny zostać uwzględnione przez organ zarządzający i KZR w procesach decyzyjnych.

194. Zgodnie z sekcją 18 niniejszych wytycznych komórka ds. nadzoru zgodności z prawem powinna również weryfikować, w ścisłej współpracy z KZR i działem prawnym, czy nowe produkty i procedury są zgodne z obecnym otoczeniem prawnym a także, w stosownych przypadkach, ze wszelkimi znanymi nadchodzącymi zmianami przepisów, regulacji i wymogów nadzorczych.

195. Instytucje powinny podejmować odpowiednie działania przeciw nadużyciom wewnętrznym lub zewnętrznym i naruszeniom dyscypliny (np. naruszeniom procedur wewnętrznych lub limitów).

196. Instytucje powinny zapewnić, aby ich jednostki zależne i oddziały podjęły kroki w celu zapewnienia zgodności swojej działalności z lokalnymi przepisami i regulacjami. Jeżeli lokalne przepisy i regulacje utrudniają stosowanie bardziej rygorystycznych procedur oraz systemów nadzoru zgodności z prawem wdrażanych przez grupę, a zwłaszcza jeżeli uniemożliwiają one ujawnianie i wymianę niezbędnych informacji między podmiotami należącymi do grupy, jednostki zależne i oddziały powinny poinformować o tym pracownika ds. nadzoru zgodności z prawem lub kierownika ds. nadzoru zgodności z prawem instytucji konsolidującej.

22 Komórka audytu wewnętrznego

197. Instytucja powinna ustanowić niezależną skuteczną komórkę audytu wewnętrznego (KAW) z uwzględnieniem kryteriów proporcjonalności określonych w tytule I, oraz mianować osobę odpowiedzialną za tę komórkę w obrębie całej instytucji. KAW powinna być niezależna oraz dysponować wystarczającymi uprawnieniami, statusem i zasobami. W szczególności instytucja powinna zapewnić, aby kwalifikacje pracowników KAW oraz zasoby KAW, a w szczególności jej narzędzia audytu i metody analizy ryzyka były odpowiednie do wielkości i lokalizacji instytucji, a także charakteru, skali i złożoności ryzyka związanego z modelem biznesowym instytucji, jej działalnością, kulturą ryzyka i skłonnością do podejmowania ryzyka.

198. KAW powinna być niezależna od działalności podlegającej audytowi. Dlatego też KAW nie powinna być łączona z żadną inną komórką.

199. KAW powinna, w oparciu o analizę ryzyka, niezależnie oceniać zgodność wszystkich działań i jednostek instytucji (w tym czynności objętych outsourcingiem) z jej polityką i procedurami oraz wymogami zewnętrznymi, a także dostarczyć obiektywnego zapewnienia tej zgodności. Każdy podmiot należący do grupy powinien być objęty zakresem działań KAW.

200. KAW nie powinna uczestniczyć w projektowaniu, wyborze, ustanawianiu i wdrażaniu konkretnej polityki, mechanizmów i procedur kontroli wewnętrznej, a także limitów ryzyka. Nie powinno to jednak uniemożliwiać organowi zarządzającemu pełniącego funkcję zarządczą żądania wkładu ze strony komórki audytu wewnętrznego w sprawach związanych z ryzykiem, kontrolą wewnętrzną i przestrzeganiem obowiązujących zasad.

201. KAW powinna oceniać, czy ramy kontroli wewnętrznej instytucji określone w sekcji 15 są skuteczne i efektywne. W szczególności KAW powinna oceniać:

a. odpowiedniość ram zarządzania instytucją;

b. czy dotychczasowa polityka i procedury są nadal odpowiednie i zgodne z wymogami prawnymi oraz regulacyjnymi, a także ze skłonnością instytucji do podejmowania ryzyka i jej strategią w zakresie ryzyka;

c. zgodność procedur z obowiązującymi przepisami i regulacjami oraz decyzjami organu zarządzającego;

d. czy procedury są prawidłowo i skutecznie wdrażane (np. zgodność transakcji, poziom efektywnie ponoszonego ryzyka itp.); oraz

e. odpowiedniość, jakość i skuteczność wdrażanych mechanizmów kontrolnych oraz sprawozdawczości obronnych jednostek biznesowych, a także komórek ds. zarządzania ryzykiem i ds. nadzoru zgodności z prawem.

202. KAW powinna zwłaszcza weryfikować rzetelność procesów zapewniających wiarygodność metod i technik stosowanych przez instytucję, a także założeń oraz źródeł informacji wykorzystywanych w jej modelach wewnętrznych (np. modelowania ryzyka i wyceny księgowej). Powinna ona także oceniać jakość i sposób wykorzystania narzędzi służących do jakościowej identyfikacji i oceny ryzyka oraz środków wdrożonych w celu minimalizacji ryzyka.

203. KAW powinna mieć swobodny dostęp do wszystkich ewidencji, dokumentów, informacji i budynków w całej instytucji. Powinno to obejmować dostęp do systemów informacji zarządczej oraz protokołów z posiedzeń wszystkich komitetów i organów decyzyjnych.

204. KAW powinna przestrzegać krajowych i międzynarodowych standardów zawodowych. Przykładem standardów zawodowych, o których jest mowa, są standardy ustanowione przez Instytut Audytorów Wewnętrznych.

205. Prace w ramach audytu wewnętrznego powinny być prowadzone zgodnie z planem audytu oraz szczegółowym programem audytu w oparciu o analizę ryzyka.

206. Plan audytu wewnętrznego powinien być sporządzany co najmniej raz w roku na podstawie rocznych celów kontrolnych audytu wewnętrznego. Plan audytu wewnętrznego powinien zostać zatwierdzony przez organ zarządzający.

207. Wszystkie zalecenia z audytu powinny skutkować formalnymi działaniami następczymi podejmowanymi na odpowiednich szczeblach kierownictwa w celu zapewnienia rozwiązania problemów w skuteczny i terminowy sposób i przedłożenia stosownych sprawozdań.

Tytuł VI – Zarządzanie ciągłością działania

208. W celu zapewnienia zdolności do prowadzenia bieżącej działalności i ograniczenia strat w przypadku poważnego zakłócenia działalności instytucje powinny ustanowić prawidłowy plan zarządzania ciągłością działania.

209. Instytucje mogą ustanowić konkretną niezależną komórkę ds. ciągłości działania, np. w ramach KZR[26].

210. Działalność instytucji jest uzależniona od pewnych zasobów o znaczeniu krytycznym (np. systemów informatycznych, w tym usług w chmurze, systemów łączności i budynków). Celem zarządzania ciągłością działania jest zmniejszenie operacyjnych, finansowych, prawnych, reputacyjnych i innych istotnych konsekwencji katastrofy lub długotrwałej przerwy w dostępie do tych zasobów oraz wynikającego z niej zakłócenia zwykłych procedur biznesowych instytucji. Inne środki zarządzania ryzykiem mogą mieć na celu zmniejszenie prawdopodobieństwa takich incydentów lub przeniesienie ich skutków finansowych na osoby trzecie (np. dzięki ubezpieczeniu).

[26] Proszę też zapoznać się z art. 312 rozporządzenia (UE) nr 575/2013.

211. Aby ustanowić prawidłowy plan zarządzania ciągłością działania, instytucja powinna poddać starannej analizie swoje narażenie na poważne zakłócenia działalności oraz ocenić (w ujęciu ilościowym i jakościowym) ich potencjalne skutki, wykorzystując dane wewnętrzne lub zewnętrzne oraz analizę scenariuszy wariantowych. Analiza ta powinna obejmować wszystkie linie biznesowe i jednostki wewnętrzne, w tym KZR, oraz powinna uwzględniać ich wzajemne zależności. Wyniki analizy powinny wnieść wkład w określenie priorytetów i celów instytucji w zakresie przywrócenia działalności.

212. Na podstawie powyższej analizy instytucja powinna ustanowić:

    a. plany awaryjne i plany ciągłości działania zapewniające odpowiednią reakcję instytucji na sytuacje awaryjne oraz jej zdolność do kontynuowania najważniejszej działalności w razie zakłócenia zwykłych procedur biznesowych; oraz

    b. plany przywrócenia zasobów o znaczeniu krytycznym służące wznowieniu zwykłych procedur biznesowych w odpowiednich ramach czasowych. Wszelkie ryzyko szczątkowe wynikające z potencjalnego zakłócenia działalności powinno być zgodne ze skłonnością instytucji do podejmowania ryzyka.

213. Plany awaryjne, ciągłości działania i przywrócenia gotowości do pracy powinny być udokumentowane oraz należycie wdrożone. Dokumentacja powinna być dostępna w liniach biznesowych, jednostkach wewnętrznych i KZR oraz powinna być przechowywana w systemach oddzielonych fizycznie i łatwo dostępnych w razie wystąpienia sytuacji awaryjnej. Należy przeprowadzić odpowiednie szkolenia. Plany należy regularnie testować i aktualizować. Wszelkie trudności lub niepowodzenia ujawnione podczas testów należy udokumentować i przeanalizować, a plany poddać stosownemu przeglądowi.

Tytuł VII – Przejrzystość

214. Wszyscy stosowni pracownicy instytucji powinni być informowani o jej strategiach, polityce i procedurach. Pracownicy instytucji powinni rozumieć politykę i procedury dotyczące ich zakresu obowiązków oraz ich przestrzegać.

215. W związku z tym organ zarządzający powinien na bieżąco informować stosownych pracowników o strategiach i polityce instytucji w jasny i spójny sposób, co najmniej w zakresie niezbędnym dla pełnienia ich obowiązków. Może to następować za pośrednictwem pisemnych wytycznych, podręczników lub w inny sposób.

216. W przypadku gdy na mocy art. 106 ust. 2 dyrektywy 2013/36/UE właściwe organy wymagają od jednostek dominujących corocznego publikowania opisu ich struktury prawnej oraz zarządzania, a także struktury organizacyjnej grupy instytucji, informacje te powinny

obejmować wszystkie podmioty w obrębie struktury grupowej określonej w dyrektywie 2013/34/UE[27], w podziale na kraje.

217. Publikacje takie powinny obejmować co najmniej:

a. przegląd organizacji wewnętrznej instytucji i struktury grupowej określonej w dyrektywie 2013/34/UE i zmiany w niej, w tym dotyczące głównej hierarchii podległości służbowej i obowiązków;

b. wszelkie istotne zmiany od czasu poprzedniej publikacji oraz datę istotnej zmiany;

c. nowe struktury prawne, zarządzania lub organizacyjne;

d. informacje na temat struktury, organizacji i członków organu zarządzającego, w tym na temat liczby jego członków i liczby członków uznawanych za niezależnych, wraz z określeniem płci i okresu trwania mandatu każdego członka organu zarządzającego;

e. najważniejsze obowiązki organu zarządzającego;

f. wykaz komitetów organu zarządzającego pełniącego funkcję nadzorczą oraz ich skład;

g. przegląd polityki przeciwdziałania konfliktom interesów mającej zastosowanie do instytucji i organu zarządzającego;

h. przegląd ram kontroli wewnętrznej; oraz

i. przegląd ram zarządzania ciągłością działalności.

Załącznik I – Aspekty, które należy uwzględnić przy opracowywaniu polityki zarządzania wewnętrznego

Zgodnie z tytułem III podczas dokumentowania polityki i zasad zarządzania wewnętrznego instytucje powinny uwzględnić aspekty, takie jak:

1. Struktura własnościowa
2. W stosownych przypadkach struktura grupy (prawna i funkcjonalna)

[27] Dyrektywa Parlamentu Europejskiego i Rady 2013/34/UE z dnia 26 czerwca 2013 r. w sprawie rocznych sprawozdań finansowych, skonsolidowanych sprawozdań finansowych i powiązanych sprawozdań niektórych rodzajów jednostek, zmieniająca dyrektywę Parlamentu Europejskiego i Rady 2006/43/WE oraz uchylająca dyrektywy Rady 78/660/EWG i 83/349/EWG (Dz.U. L 182 z 29.6.2013, s. 19).

3. Skład i funkcjonowanie organu zarządzającego
   a) kryteria wyboru
   b) liczba członków, długość mandatu, rotacja, wiek
   c) członkowie niezależni organu zarządzającego
   d) członkowie wykonawczy organu zarządzającego
   e) członkowie niewykonawczy organu zarządzającego
   f) w stosownych przypadkach wewnętrzny podział zadań
4. Struktura zarządzania i struktura organizacyjna (wraz z jej wpływem na grupę w stosownych przypadkach)
   a) wyspecjalizowane komitety
      i. skład
      ii. funkcjonowanie
   b) komitet wykonawczy, jeżeli został ustanowiony
      i. skład
      ii. funkcjonowanie
5. Osoby pełniące najważniejsze funkcje
   a) kierownik komórki ds. zarządzania ryzykiem
   b) kierownik komórki ds. nadzoru zgodności z prawem
   c) kierownik komórki audytu wewnętrznego
   d) dyrektor finansowy
   e) inne osoby pełniące najważniejsze funkcje
6. Ramy kontroli wewnętrznej
   a) opis każdej funkcji, w tym jej organizacji, zasobów, statusu i uprawnień
   b) opis ram zarządzania ryzykiem, w tym strategii w zakresie ryzyka
7. Struktura organizacyjna (wraz z jej wpływem na grupę w stosownych przypadkach)
   a) struktura operacyjna, linie biznesowe oraz przydział kompetencji i zadań
   b) outsourcing
   c) oferta produktów i usług
   d) zakres geograficzny działalności
   e) swoboda świadczenia usług
   f) oddziały
   g) jednostki zależne, spółki *joint venture* itp.
   h) korzystanie z centrów zagranicznych
8. Kodeks postępowania i zachowania (wraz z jego wpływem na grupę w stosownych przypadkach)

a) cele strategiczne i wartości spółki
b) wewnętrzne kodeksy i regulacje, polityka prewencyjna
c) polityka przeciwdziałania konfliktom interesów
d) sygnalizowanie nieprawidłowości

9. Status polityki w zakresie zarządzania wewnętrznego wraz z jej datą
   a) opracowanie
   b) ostatnia zmiana
   c) ostatnia ocena
   d) zatwierdzenie przez organ zarządzający.