EBA/GL/2021/05

2 lipca 2021 r.

Projekt wytycznych

w sprawie zarządzania wewnętrznego

1. Zgodność i obowiązki sprawozdawcze

Status niniejszych wytycznych

1. Niniejsze wytyczne opracowano na podstawie art. 16 rozporządzenia (UE) nr 1093/2010[1]. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy i instytucje finansowe muszą dołożyć wszelkich starań, aby zastosować się do niniejszych wytycznych.

2. Wytyczne przedstawiają stanowisko EUNB w sprawie odpowiednich praktyk nadzoru w ramach Europejskiego Systemu Nadzoru Finansowego lub tego, jak należy stosować prawo unijne 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 nadzoru), również jeżeli wytyczne są skierowane przede wszystkim do instytucji.

Wymogi sprawozdawcze

3. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy mają obowiązek powiadomić EUNB do dnia (05.12.2021), czy stosują się lub czy zamierzają zastosować się do niniejszych wytycznych, albo uzasadnić, dlaczego się do nich nie zastosują. W razie braku powiadomienia w wyznaczonym terminie EUNB uzna, że właściwe organy nie stosują się do niniejszych wytycznych. Powiadomienia należy przekazać poprzez wysłanie formularza dostępnego na stronie internetowej EUNB na adres compliance@eba.europa.eu z dopiskiem „EBA/GL/2021/05”. Powiadomienia przekazują osoby odpowiednio upoważnione do informowania o stosowaniu się do wytycznych w imieniu właściwego organu. Do EUNB należy również zgłaszać wszelkie zmiany związane ze stosowaniem się do wytycznych.

4. Powiadomienia zostaną opublikowane na stronie internetowej EUNB zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010.

[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 szczegółowo określa się ustalenia, procesy oraz mechanizmy z zakresu zarządzania wewnętrznego, jakie powinny zostać wdrożone zgodnie z art. 74 ust. 1 dyrektywy 2013/36/UE przez instytucje podlegające przepisom dyrektywy 2013/36/UE[2] oraz firmy inwestycyjne podlegające przepisom tytułu VII dyrektywy 2013/36/UE w ramach zastosowania postanowień art. 1 ust. 2 i ust. 5 rozporządzenia 2019/2033/UE, w celu zapewnienia skutecznego i ostrożnego zarządzania takimi instytucjami i firmami.

Adresaci

Niniejsze wytyczne są skierowane do właściwych organów zdefiniowanych w art. 4 pkt 2 ppkt (i) rozporządzenia (UE) 1093/2010, oraz instytucji finansowych zdefiniowanych w art. 4 pkt 1 rozporządzenia (UE) 1093/2010, które są uznawane albo za instytucje dla celów stosowania dyrektywy 2013/36/UE zgodnie z definicją w art. 3 ust. 1 pkt 3 dyrektywy 2013/36/UE i również uwzględniając art. 3 ust. 3 tej dyrektywy, albo za firmy inwestycyjne podlegające przepisom tytułu VII dyrektywy 2013/36/UE w zastosowaniu art. 1 ust. 2 i ust. 5 rozporządzenia 2019/2033/UE („instytucje”).

Zakres stosowania

6. 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 wszelkim ryzykiem[3], jego monitorowaniu i sprawozdawczości, oraz ram kontroli wewnętrznej.

7. 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].

[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] Odniesienia do ryzyka w niniejszych wytycznych obejmują ryzyko w zakresie prania pieniędzy i finansowania terroryzmu.
[4] Zob. też motyw 56 dyrektywy 2013/36/UE.

8. 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) 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.

9. W państwach członkowskich, w których organ zarządzający przekazuje funkcje wykonawcze w całości lub częściowo osobie lub wewnętrznemu organowi wykonawczemu (np. dyrektorowi generalnemu, zespołowi zarządzającemu lub komitetowi wykonawczemu), przyjmuje się, że osoby pełniące takie funkcje wykonawcze w ramach przekazania funkcji wypełniają funkcje kierownicze 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 lub organów zarządzających instytucji na mocy prawa krajowego.

10. 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.

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

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

Definicje

13. O ile nie określono inaczej, pojęcia stosowane i zdefiniowane w dyrektywie 2013/36/UE i rozporządzeniu (UE) nr 575/2013 mają w niniejszych wytycznych takie samo znaczenie. Ponadto do celów niniejszych wytycznych stosuje się następujące definicje:

Akcjonariusz	oznacza osobę posiadającą akcje instytucji lub, w zależności od formy prawnej instytucji, innych właścicieli lub członków instytucji.
Dyrektor finansowy	oznacza osobę odpowiedzialną za ogólne zarządzanie wszystkimi następującymi działaniami: zarządzaniem zasobami finansowymi, planowaniem finansowym i sprawozdawczością finansową.
Dyrektor generalny	oznacza osobę odpowiedzialną za zarządzanie i kierowanie całą działalnością biznesową instytucji.
Funkcja dyrektorska	oznacza członka organu zarządzającego instytucji lub innego podmiotu prawnego.
Gotowość 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.
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.
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.
Instytucje notowane na giełdzie	oznaczają instytucje, których instrumenty finansowe są dopuszczone do obrotu na rynku regulowanym lub na wielostronnej platformie obrotu określonych w art. 4 ust. 21 i art. 4 ust. 22 dyrektywy 2014/65/UE w co najmniej jednym państwie członkowskim[5].
Kierownicy komórek kontroli wewnętrznej	oznacza osoby będące na najwyższym poziomie hierarchii odpowiedzialne za skuteczne kierowanie bieżącym funkcjonowaniem niezależnych jednostek ds. zarządzania ryzykiem, zgodności z przepisami i audytu wewnętrznego.
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 częścią 1, tytułem 2, rozdziałem 2 rozporządzenia (UE) nr 575/2013.[6]
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

[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).

[6] Zob. również regulacyjne standardy techniczne dotyczące konsolidacji ostrożnościowej pod adresem: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2021/973355/Final%20Report%20Draft%20RTS%20methods%20of%20consolidation.pdf.

	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.
Osoby pełniące najważniejsze funkcje	oznacza osoby mające znaczący wpływ na kierowanie instytucją, 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.
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.
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.
Zróżnicowanie wynagrodzenia ze względu na płeć	oznacza różnicę pomiędzy średnim wynagrodzeniem brutto za jedną godzinę pracy mężczyzn i kobiet, wyrażoną jako wartość procentowa średniego wynagrodzenia brutto za jedną godzinę pracy mężczyzn.

3. Wdrożenie

Data rozpoczęcia stosowania

14. Niniejsze wytyczne mają zastosowanie od dnia 31 grudnia 2021 r.

Uchylenie

15. Uchyla się wytyczne EUNB w sprawie zarządzania wewnętrznego (EBA/GL/2017/11) z dnia 26 września 2017 r. ze skutkiem od dnia 31 grudnia 2021 r.

4. Wytyczne

Tytuł I – Proporcjonalność

16. 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 i przepisów.

17. 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 stosować bardziej wyrafinowane zasady zarządzania, natomiast mniejsze i mniej złożone instytucje mogą wdrożyć prostsze zasady zarządzania. Instytucje powinny jednak wziąć pod uwagę, że wielkość i znaczenie systemowe danej instytucji nie może samo w sobie wskazywać na zakres, w jakim jest ona narażona na ryzyko.

18. Do celów zastosowania zasady proporcjonalności oraz zapewnienia odpowiedniego wdrożenia wymogów regulacyjnych oraz niniejszych wytycznych instytucje i właściwe organy powinny wziąć pod uwagę wszystkie następujące aspekty:

    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;

    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, gotowość do podejmowania ryzyka i rzeczywisty profil ryzyka instytucji, również z uwzględnieniem wyników BION dotyczących kapitału i płynności;

i. strukturę własnościową i strukturę 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;

l. stosowane systemy informatyczne (IT), w tym systemy służące utrzymaniu ciągłości działania i czynności objęte outsourcingiem w tym obszarze;

m. czy instytucja jest objęta definicją przedstawioną w art. 4 ust. 1 pkt 145 rozporządzenia (UE) 575/2013 dotyczącą małej i niezłożonej instytucji, czy definicją przedstawioną w art. 4 ust. 1 pkt 146 rozporządzenia (UE) 575/2013 dotyczącą dużej instytucji.

Tytuł II – Rola i skład organu zarządzającego oraz komitetów

1 Rola i obowiązki organu zarządzającego

19. 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.

20. 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. 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.

21. 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 wykonywać swoje role. W celu zapewnienia odpowiednich mechanizmów kontroli i równowagi proces decyzyjny w ramach organu zarządzającego nie powinien być zdominowany przez jednego członka lub niewielką grupę członków.

22. 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, gotowości 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 i zarządzaniem ryzykiem;

c. odpowiednich i skutecznych ram zarządzania wewnętrznego oraz kontroli wewnętrznej, zgodnie z definicją w tytule V, które:

    i. obejmują jasną strukturę organizacyjną i dobrze funkcjonujące, niezależne wewnętrzne komórki ds. zarządzania ryzykiem, ds. zgodności z przepisami i audytu, dysponujące wystarczającymi uprawnieniami, statusem i zasobami, aby móc wykonywać swoje funkcje;

    ii. zapewniają zgodność z obowiązującymi wymogami regulacyjnymi w zakresie zapobiegania praniu pieniędzy i finansowaniu terroryzmu;

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

e. celów w zakresie 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[7];

g. zasad mających na celu zapewnienie skutecznego przeprowadzenia indywidualnych i zbiorowych ocen odpowiedniości organu zarządzającego, odpowiedniego składu organu zarządzającego i planowania sukcesji w jego obrębie oraz skutecznego pełnienia funkcji przez organ zarządzający[8];

h. procesu wyboru i oceny odpowiedniości osób pełniących najważniejsze funkcje[9];

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

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

[7] Wytyczne EUNB dotyczące prawidłowej polityki wynagrodzeń.
[8] Zob. także wspólne wytyczne ESMA i EUNB w sprawie oceny odpowiedniości członków organu zarządzającego i osób pełniących najważniejsze funkcje.
[9] Zob. także wspólne wytyczne ESMA i EUNB w sprawie oceny odpowiedniości członków organu zarządzającego i osób pełniących najważniejsze funkcje.

ii. odpowiedniego przepływu informacji, w tym dokumentacji zaleceń i wniosków, oraz zasad raportowania 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;

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.

23. Podczas ustanawiania, zatwierdzania i nadzorowania wdrożenia kwestii, o których mowa w pkt 22, organ zarządzający powinien zapewnić wprowadzenie takiego modelu biznesowego i zasad zarządzania wewnętrznego, w tym ram zarządzania ryzykiem, które uwzględniają wszystkie rodzaje ryzyka. Analizując wszystkie rodzaje ryzyka, na jakie instytucje mogą być narażone, instytucje powinny wziąć pod uwagę wszystkie mające zastosowanie czynniki ryzyka, w tym dotyczące ryzyka środowiskowego, społecznego i związanego z zarządzaniem. Instytucje powinny uwzględnić fakt, że wymienione na końcu poprzedniego zdania czynniki ryzyka mogą wpływać na ich ryzyka ostrożnościowe, w tym ryzyko kredytowe np. w związku z występowaniem czynników ryzyka związanego z przejściem na gospodarkę zrównoważoną lub czynników zewnętrznych związanych z klimatem, które mogą wpłynąć na dłużników, rynek, płynność, ryzyko operacyjne a także ryzyko utraty reputacji – np. w związku z obecnością czynników ryzyka społecznego i związanego z zarządzaniem w kontekście outsourcingu [10]. Takie rodzaje ryzyka obejmują, na przykład, ryzyko prawne związane z prawem umów lub prawem pracy, ryzyko związane z potencjalnym naruszeniem praw człowieka, czy inne czynniki ryzyka środowiskowego, społecznego i związanego z zarządzaniem, które mogą wpłynąć na kraj, w którym zlokalizowany jest usługodawca, oraz na jego zdolność do świadczenia usług na ustalonym poziomie.

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

[10] Zob. raport EUNB w sprawie zarządzania i nadzoru nad ryzykiem środowiskowym, społecznym i związanym z zarządzaniem, opublikowany na podstawie dyrektywy o wymogach kapitałowych (CRD), art. 98 ust. 8, który zawiera opis przedstawiający definicje wg EUNB dotyczące ryzyka środowiskowego, społecznego i związanego z zarządzaniem, kanałów transmisji, a także zalecenia odnośnie do ustaleń, procesów, mechanizmów i strategii, jakie instytucje powinny wdrożyć w celu identyfikacji i oceny ryzyka środowiskowego, społecznego i związanego z zarządzaniem oraz zarządzania tym ryzykiem.

25. Wszyscy członkowie organu zarządzającego powinni być informowani o pełnej działalności instytucji oraz jej sytuacji finansowej i sytuacji pod względem ryzyka, z uwzględnieniem środowiska gospodarczego, a także o podejmowanych decyzjach mających znaczący 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 na niezależność komórki kontroli wewnętrznej.

27. Organ zarządzający powinien monitorować wszelkie uchybienia zidentyfikowane w odniesieniu do wdrażania procesów, strategii i polityki wymienionych w pkt 22 i 23, dokonywać ich okresowego przeglądu oraz podejmować działania naprawcze. 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 szczegółowy 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 oceny 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 regularnie, w razie potrzeby bez zbędnej zwłoki, informować organ zarządzający pełniący funkcję nadzorczą o istotnych elementach oceny sytuacji, ryzyku i zmianach mających wpływ lub mogących mieć wpływ na instytucję, np. istotnych decyzjach dotyczących działań biznesowych i ponoszonego ryzyka, ocenie otoczenia gospodarczego i biznesowego instytucji, płynności oraz solidnej bazie kapitałowej, a także ocenie istotnych ekspozycji na ryzyko.

31. Bez uszczerbku dla transpozycji dyrektywy 2015/849/UE do prawa krajowego, organ zarządzający powinien wyznaczyć jednego ze swoich członków, zgodnie z wymogami na mocy art. 46 ust. 4 dyrektywy 2015/849/UE w sprawie przeciwdziałania praniu pieniędzy (AMLD), który będzie odpowiedzialny za wdrożenie przepisów, regulacji i postanowień niezbędnych do realizacji celu dyrektywy, w tym stosownych procedur w instytucji dotyczących

przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, na poziomie organu zarządzającego[11].

3 Funkcja nadzorcza organu zarządzającego

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

33. 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 odpowiedniości członków organu zarządzającego i osób pełniących najważniejsze funkcje, wydanych na mocy dyrektywy 2013/36/UE i dyrektywy 2014/65/UE.

34. Bez uszczerbku dla zadań przydzielonych na mocy obowiązujących przepisów krajowego prawa spółek, organ zarządzający pełniący funkcję nadzorczą powinien:

    a. nadzorować i monitorować proces podejmowania decyzji przez kierownictwo oraz jego działania, zapewnić skuteczny nadzór nad organem zarządzającym pełniącym funkcję zarządczą, w tym monitorowanie oraz kontrolę jego indywidualnych i zbiorowych wyników a także 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. nominacji 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 gotowości 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;

[11] Organ zarządzający, jako ciało kolegialne, ponosi odpowiedzialność solidarną.

g. nadzorować wdrażanie i stosowanie 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

35. 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, o ile zostały one ustanowione, oraz powinien być odpowiedzialny za jego ogólne, skuteczne funkcjonowanie.

36. Przewodniczący powinien zachęcać do otwartej i krytycznej dyskusji, propagować taką dyskusję oraz zapewnić możliwość wyrażania i omawiania odmiennych poglądów w ramach procesu decyzyjnego.

37. 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 w instytucji (np. przez wyznaczenie głównego członka rady lub najstarszego stażem niezależnego członka rady lub 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 generalnego w tej samej instytucji, chyba że zostało to uzasadnione przez instytucję a właściwe organy wydały na to zezwolenie.

38. 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 członków tego organu z wystarczającym wyprzedzeniem przed posiedzeniami.

39. 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

40. 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, nominacji[12] oraz wynagrodzeń[13], 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.

41. W przypadku gdy komitet ds. ryzyka lub nominacji 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.

42. Z uwzględnieniem kryteriów określonych w tytule I niniejszych wytycznych instytucje mogą ustanawiać inne komitety (np. do spraw zapobiegania praniu pieniędzy/finansowaniu terroryzmu, etyki, kodeksu postępowania oraz zgodności z prawem).

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

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

45. 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.

[12] Zob. też wspólne wytyczne ESMA i EUNB w sprawie oceny odpowiedniości członków organu zarządzającego i osób pełniących najważniejsze funkcje wydane na mocy dyrektywy 2013/36/UE i dyrektywy 2014/65/UE.
[13] W odniesieniu do komitetu ds. wynagrodzeń zob. też wytyczne EUNB dotyczące prawidłowej polityki wynagrodzeń.

5.2 Skład komitetów[14]

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

47. Członkowie niezależni[15] organu zarządzającego pełniącego funkcję nadzorczą powinni być aktywnie zaangażowani w pracę komitetów.

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

49. Z uwzględnieniem wielkości organu zarządzającego oraz liczby członków niezależnych organu zarządzającego pełniącego funkcję nadzorczą, instytucje powinny zapewnić, aby poszczególne komitety nie składały się z tej samej grupy członków.

50. 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.

51. Komitety ds. ryzyka i nominacji 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[16]. Skład komitetu ds. wynagrodzeń powinien być zgodny z sekcją 2.4.1 wytycznych EUNB dotyczących prawidłowej polityki wynagrodzeń[17].

52. W przypadku globalnych instytucji o znaczeniu systemowym i innych instytucji o znaczeniu systemowym komitet ds. nominacji 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. nominacji powinna wchodzić wystarczająca liczba członków niezależnych; instytucje takie mogą również uznać za dobrą praktykę taką, zgodnie z którą przewodniczącym komitetu ds. nominacji jest członek niezależny.

53. Członkowie komitetu ds. nominacji powinni posiadać indywidualnie i zbiorowo odpowiednią wiedzę, w tym wiedzę fachową, oraz umiejętności w odniesieniu do procesu selekcji i wymagań dotyczących odpowiedniości, jak określono w dyrektywie 2013/36/UE.

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

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

[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] 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).

54. 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 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.

55. 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

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

57. Komitety powinny w stosownych przypadkach współdziałać ze sobą. Bez uszczerbku dla pkt 49, współdziałanie takie może przyjąć formę łączenia udziału polegającego na tym, że przewodniczący lub członek komitetu może być zarazem członkiem innego komitetu.

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

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

60. Komitety ds. ryzyka i nominacji powinny co najmniej:

    a. mieć dostęp do wszystkich istotnych informacji i danych niezbędnych w celu pełnienia ich funkcji, w tym informacji i danych ze stosownych komórek korporacyjnych i kontrolnych (np. ds. prawnych, finansowych, kadrowych, informatycznych, audytu wewnętrznego, ryzyka, zgodności z przepisami, jak również informacji dotyczących zgodności z przepisami dotyczącymi przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, a także zagregowanych informacji o podejrzanych transakcjach oraz o czynnikach ryzyka prania pieniędzy i finansowania terroryzmu);

    b. otrzymywać regularne sprawozdania, informacje doraźne, komunikaty i opinie od kierowników komórek kontroli wewnętrznej dotyczące aktualnego profilu ryzyka instytucji, kultury ryzyka i limitów ryzyka, a także wszelkich istotnych naruszeń[18], do

[18] W odniesieniu do poważnych naruszeń w obszarze przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Zob. również wytyczne, które zostaną wydane na podstawie art. 117 ust. 6 dyrektywy 2013/36/UE, określające metody współpracy i wymiany informacji pomiędzy organami, o których mowa w ust. 5 powyższego artykułu, w szczególności w odniesieniu do grup działających w skali transgranicznej oraz w kontekście identyfikacji poważnych naruszeń zasad w zakresie przeciwdziałania praniu pieniędzy.

których mogło dojść, ze szczegółowymi informacjami i zaleceniami dotyczącymi podjętych, planowanych lub sugerowanych środków naprawczych służących ich usunięciu; okresowo dokonywać weryfikacji i decydować w zakresie treści, formatu i częstotliwości informacji dotyczących ryzyka, które mają być im przekazywane; oraz

c. 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

61. 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 gotowości instytucji do podejmowania ryzyka oraz strategii w zakresie ryzyka, z uwzględnieniem wszystkich rodzajów ryzyka, w celu zapewnienia, aby były one zgodne ze 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 strategii w zakresie ryzyka i gotowości do podejmowania 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 [19]. Komitet ds. ryzyka powinien ocenić ryzyko związane z oferowanymi

[19] Zob. również 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.

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.

62. Komitet ds. ryzyka powinien współpracować z innymi komitetami, których działalność może mieć wpływ na strategię w zakresie ryzyka (np. komitetami ds. audytu i nominacji), oraz regularnie komunikować się z komórkami kontroli wewnętrznej instytucji, zwłaszcza z komórką ds. zarządzania ryzykiem.

63. Jeżeli ustanowiony został komitet ds. ryzyka, komitet ten musi zbadać, bez uszczerbku dla zadań komitetu ds. wynagrodzeń, czy zachęty przewidziane w polityce i praktykach w zakresie wynagrodzeń uwzględniają ryzyko, kapitał i płynność instytucji oraz prawdopodobieństwo i perspektywę czasową uzyskania przez nią zysków.

5.5 Rola komitetu ds. audytu

64. Zgodnie z dyrektywą 2006/43/WE[20], 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[21], w szczególności odpowiedniości świadczenia usług niebędących badaniem sprawozdań finansowych zgodnie z art. 5 tego rozporządzenia;

e. monitorować badanie ustawowe rocznych i skonsolidowanych sprawozdań finansowych, w szczególności jego wykonanie, z uwzględnieniem wszelkich ustaleń i

[20] 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.

[21] 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).

wniosków właściwego organu zgodnie z art. 26 ust. 6 rozporządzenia (UE) nr 537/2014;

f. ponosić odpowiedzialność za procedurę wyboru zewnętrznego biegłego rewidenta lub rewidentów lub 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;

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

65. 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.

66. Jeżeli w instytucji nieistotnej zostały ustanowione komitety ds. ryzyka i nominacji, 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.

67. 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[22].

Tytuł III – Ramy zarządzania

6 Ramy i struktura organizacyjna

6.1 Ramy organizacyjne

68. 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

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

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 funkcji. 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.

69. 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.

70. 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 lub wydarzenia zewnętrzne) wpływają na stabilność ram organizacyjnych. W przypadku stwierdzenia uchybień organ zarządzający powinien niezwłocznie dokonywać wszelkich niezbędnych korekt.

6.2 „Poznaj swoją strukturę”

71. Organ zarządzający powinien w pełni znać i rozumieć strukturę prawną, organizacyjną i operacyjną instytucji (zasada „Poznaj swoją strukturę”) oraz zapewnić jej zgodność z zatwierdzoną strategią biznesową i strategią w zakresie ryzyka, jak też gotowością do podejmowania ryzyka, a także objęcie tej struktury ramami zarządzania ryzykiem.

72. 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.

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

74. 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.

75. 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 dotyczących kwestii, 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

76. 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, finansowaniem terroryzmu lub innymi przestępstwami finansowymi, a także ustanowione mechanizmy kontrolne i ramy prawne[23]. W tym celu instytucje powinny uwzględniać co najmniej:

[23] Aby uzyskać bardziej szczegółowe informacje na temat oceny ryzyka dla danego kraju oraz ryzyka związanego z poszczególnymi produktami i klientami, instytucje powinny zapoznać się również ze wspólnymi wytycznymi dotyczącymi ryzyka w zakresie prania pieniędzy i finansowania terroryzmu (EBA GL JC/2017/37), które są aktualnie w trakcie weryfikacji.

a. stopień, w jakim jurysdykcja, w której zostanie ustanowiona struktura, skutecznie spełnia unijne i międzynarodowe standardy w zakresie przejrzystości podatkowej oraz przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu[24];

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;

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.

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

78. 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, oraz że 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.

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

80. 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, metod przepływu informacji)

[24] Zob. też: https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/rts-on-the-implementation-of-group-wide-aml/cft-policies-in-third-countries.

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.

81. 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.

82. Instytucje powinny stosować 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 ryzyko utraty reputacji. W szczególności instytucje powinny analizować przyczyny, dla których klient chce utworzyć konkretną strukturę.

7 Ramy organizacyjne w kontekście grupowym

83. Zgodnie z art. 109 ust. 2 dyrektywy 2013/36/UE jednostki dominujące i jednostki zależne objęte tą 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, w tym jednostki ustanowione w innych państwach, w tym centrach offshore, aby zapewnić solidne zasady zarządzania w ujęciu skonsolidowanym i subskonsolidowanym. Odnośnie do wymogów związanych z wynagrodzeniami zastosowanie mają określone wyjątki przewidziane w art. 109 ust. 4 i 5[25] ww. dyrektywy. 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 w sekcji 6.2.

[25] Zob. również wytyczne EUNB dotyczące prawidłowej polityki wynagrodzeń.

84. 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.

85. Na poziomie skonsolidowanym i subskonsolidowanym, instytucja konsolidująca powinna zapewnić przestrzeganie ogólnogrupowej polityki w zakresie zarządzania oraz wewnętrznych ram kontroli, o których mowa w tytule V, 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.

86. Instytucja konsolidująca powinna rozważyć interesy wszystkich swoich jednostek zależnych oraz ustalić, w jaki sposób strategie i polityka sprzyjają realizacji interesów każdej jednostki zależnej oraz interesów całej grupy w perspektywie długookresowej.

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

88. 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.

89. Wymogi dotyczące zarządzania określone w dyrektywie 2013/36/UE i postanowienia 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 szczegółowych wyjaśnieniach w niniejszych wytycznych.

90. 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[26]

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

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

93. 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.

Tytuł IV – Kultura ryzyka i prowadzenie działalności

9 Kultura ryzyka

94. Prawidłowa, staranna 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 sposobie zarządzania nim, uwzględniając swoją gotowość 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.

[26] Zob. też wytyczne EUNB dotyczące outsourcingu, dostępne pod adresem: https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements.

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 gotowości 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 gotowość do podejmowania ryzyka i zdolność do jego ponoszenia. Powinni 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[27].

10 Wartości instytucji i kodeks postępowania

99. Organ zarządzający powinien opracować i przyjąć wysokie standardy etyczne i zawodowe, a następnie ich przestrzegać i je upowszechniać, uwzględniając szczególne potrzeby oraz cechy

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

instytucji, oraz 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, lub wspólne standardy wydane przez stowarzyszenia lub inne stosowne organizacje.

100. Instytucje powinny zapewnić brak dyskryminacji pracowników ze względu na płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub wiarę, opinie polityczne lub wszelkie inne opinie, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną.

101. Polityki instytucji powinny być neutralne pod względem płci. Obejmuje to, między innymi, kwestie dotyczące wynagrodzenia, procedur rekrutacji, rozwoju kariery i planów sukcesji, dostępu do szkoleń oraz możliwości zgłaszania się na wolne stanowiska w ramach rekrutacji wewnętrznej. Instytucje powinny zapewnić równe szanse [28] dla wszystkich członków personelu, niezależnie od ich płci, jeśli chodzi o perspektywy rozwoju kariery, a także czynić starania w kierunku polepszenia wskaźnika reprezentacji mniejszościowej płci na stanowiskach w organie zarządzającym, a także w grupie personelu posiadającej kompetencje kierownicze, zgodnie z rozporządzeniem delegowanym Komisji (regulacyjne standardy techniczne w zakresie ustalania kategorii pracowników)[29]. Instytucje powinny monitorować rozwój sytuacji w zakresie zróżnicowania wynagrodzenia ze względu na płeć, oddzielnie dla zidentyfikowanych członków personelu (z wyłączeniem członków organu zarządzającego), członków organu zarządzającego sprawującego funkcję zarządczą, członków organu zarządzającego sprawującego funkcję nadzorczą oraz pozostałych pracowników. Instytucje powinny wdrożyć procedury umożliwiające reintegrację pracowników powracających z urlopów macierzyńskich, ojcowskich lub wychowawczych.

102. Wdrożone standardy powinny mieć na celu rozwój zasad dotyczących zarządzania w instytucji oraz zmniejszenie ryzyka, na jakie narażona jest instytucja, w szczególności ryzyka operacyjnego i ryzyka 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.

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

a. uświadamiać pracowników, 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

[28] Zob. też dyrektywę 2006/54/WE Parlamentu Europejskiego i Rady z dnia 5 lipca 2006 r. w sprawie wprowadzenia w życie zasady równości szans oraz równego traktowania kobiet i mężczyzn w dziedzinie zatrudnienia i pracy.
[29] Zob. też wytyczne EUNB w sprawie neutralnej płciowo polityki wynagrodzeń.

działalność nie może wykraczać poza określony poziom gotowości 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, między innymi, nadużyciami, praniem pieniędzy i finansowaniem terroryzmu, praktykami monopolistycznymi, omijaniem sankcji finansowych, przekupstwem i korupcją, manipulacjami rynkowymi, nieprawidłowościami związanymi ze sprzedażą, innymi naruszeniami przepisów dotyczących ochrony konsumentów, przestępstwami podatkowymi, niezależnie od tego, czy zostały popełnione w sposób bezpośredni, czy pośredni, w tym w sposób niezgodny z prawem lub przy wykorzystaniu zakazanych systemów arbitrażu dywidendowego;

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 niewłaściwe postępowanie oraz niedopuszczalne zachowania.

104. 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

105. 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. w związku z różnymi działaniami i rolami danej instytucji lub różnych instytucji objętych zakresem konsolidacji ostrożnościowej lub różnych linii biznesowych lub też jednostek w obrębie instytucji, lub też mogą odnosić się do zewnętrznych zainteresowanych stron.

106. Instytucje powinny w ramach swoich zasad organizacyjnych i administracyjnych podjąć odpowiednie kroki w celu zapobiegania niekorzystnemu wpływowi konfliktów interesów na interesy ich klientów.

107. 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 lub 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.

12 Polityka przeciwdziałania konfliktom interesów dla pracowników[30]

108. 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.

109. 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 wcześniejszych relacji osobistych lub zawodowych. W przypadku wystąpienia konfliktów interesów, instytucje powinny ocenić ich istotność, podjąć decyzję i w stosownych przypadkach wdrożyć środki w celu ich minimalizacji.

110. W odniesieniu do konfliktów interesów wynikających z wcześniejszych relacji, instytucje powinny ustalić odpowiednie ramy czasowe, co do których pracownicy powinni zgłaszać takie konflikty interesów, z uwagi na to, że mogą one nadal mieć wpływ na zachowanie pracowników i ich udział w podejmowaniu decyzji.

111. 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,

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

członkostwo w organie lub prawo własności organu lub podmiotu mającego sprzeczne interesy);

b. osobiste lub zawodowe powiązania z właścicielami znacznych pakietów akcji 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. wpływ polityczny lub powiązania polityczne.

112. Niezależnie od powyższego instytucje powinny uwzględnić fakt, że bycie akcjonariuszem instytucji lub 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*.

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

114. 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 którymi wystarczy zazwyczaj zastosować jednorazowy środek. We wszystkich przypadkach w podejmowanych decyzjach należy uwzględniać przede wszystkim interes instytucji.

115. 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 wywołujących konflikt 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 lub jego obiektywność lub też zdolność do należytego wypełniania obowiązków wobec instytucji może ulec zmniejszeniu w inny sposób;

d. 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.

116. 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[31].

117. Podczas ograniczania skutków zidentyfikowanych konfliktów interesów członków organu zarządzającego instytucje powinny dokumentować zastosowane środki, w tym uzasadnienie co do skuteczności zastosowanych środków, aby zapewnić obiektywność w procesie podejmowania decyzji.

118. Rzeczywiste lub potencjalne konflikty interesów, które zostały ujawnione odpowiedzialnej komórce w obrębie instytucji, należy odpowiednio ocenić i odpowiednio nimi zarządzać. Jeżeli stwierdzono konflikt interesów u 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.

119. 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.

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

12.1 Polityka dotycząca konfliktu interesów w kontekście pożyczek oraz innych transakcji z członkami organu zarządzającego i stronami z nimi powiązanymi

120. W ramach polityki przeciwdziałania konfliktom interesów dla pracowników (sekcja 12) i zarządzania konfliktami interesów na szczeblu członków organu zarządzającego, jak opisano w pkt 117, organ zarządzający powinien ustalić ramy identyfikacji konfliktów interesów i zarządzania konfliktami interesów w kontekście udzielania pożyczek i zawierania innych transakcji (np. faktoring, leasing, transakcje dotyczące nieruchomości itp.) z członkami organu zarządzającego i stronami z nimi powiązanymi.

121. Bez uszczerbku dla transpozycji dyrektywy 2013/36/EU[32] do prawa krajowego, instytucje mogą wziąć pod uwagę dodatkowe kategorie stron powiązanych, do których będą miały zastosowanie, w całości lub w części, ramy dotyczące pożyczek i innych transakcji.

122. Ramy dotyczące konfliktu interesów powinny zapewniać, aby decyzje dotyczące pożyczek i zawierania innych transakcji z członkami organu zarządzającego i powiązanymi z nimi osobami były podejmowane w sposób obiektywny, bez zezwalania na niewłaściwy wpływ ewentualnego konfliktu interesów, oraz aby transakcje takie były, co do zasady, zawierane na warunkach rynkowych.

123. Organ zarządzający powinien opracować procesy decyzyjne dotyczące udzielania pożyczek oraz zawierania innych transakcji z członkami organu zarządzającego oraz osobami z nimi powiązanymi. Ramy te mogą przewidywać rozróżnienie pomiędzy standardowymi transakcjami biznesowymi[33], zawieranymi w ramach zwykłej działalności i na zwyczajowych warunkach rynkowych, oraz pożyczkami dla pracowników i transakcjami zawieranymi na warunkach dostępnych dla wszystkich pracowników. Dodatkowo ramy dotyczące konfliktu interesów i procesu decyzyjnego mogą rozróżniać pożyczki istotne i nieistotne, różne rodzaje pożyczek i innych transakcji, a także różne poziomy konfliktów interesów, jakie takie transakcje mogą wywołać.

124. Jako część ram dotyczących konfliktu interesów organ zarządzający powinien ustalić odpowiednie progi (np. dotyczące rodzaju produktu lub warunków transakcji), po przekroczeniu których pożyczka lub inna transakcja z członkami organu zarządzającego lub powiązanymi z nimi osobami będzie zawsze wymagać zatwierdzenia organu zarządzającego. Decyzje w odniesieniu do istotnych pożyczek lub innych istotnych transakcji z członkami organu zarządzającego, które nie są zawierane na zwykłych warunkach rynkowych, lecz na warunkach oferowanych wszystkim pracownikom powinny być zawsze podejmowane przez organ zarządzający.

[32] Zob. też Podstawowa Zasada Bazylejska nr 20.
[33] Transakcje biznesowe obejmują pożyczki i inne transakcje (np. leasing, faktoring, usługi w ramach tzw. pierwszej oferty publicznej (IPO), fuzje i przejęcia, sprzedaż i zakup aktywów).

125. Członek organu zarządzającego, który odnosi korzyści z istotnej pożyczki lub innej istotnej transakcji, lub członek powiązany z drugą stroną transakcji, nie powinien być zaangażowany w proces decyzyjny.

126. Przed podjęciem decyzji odnośnie pożyczki lub innej transakcji z członkiem organu zarządzającego lub powiązaną z nim osobą, instytucje powinny ocenić ryzyko, na jakie instytucja może zostać narażona w związku z transakcją.

127. Jeśli pożyczka jest udzielana w ramach linii kredytowej (np. kredyt w rachunku bieżącym), wstępną decyzję oraz wszelkie zmiany decyzji należy udokumentować. Wykorzystanie takich udogodnień kredytowych w ramach ustalonych limitów nie powinno być uznawane za dokonane na podstawie nowej decyzji o pożyczce dla członka organu zarządzającego lub powiązanej z nim osoby. Jeśli zmiana wysokości linii kredytowej jest istotna, w świetle procedur obowiązujących w instytucji, należy przeprowadzić nową ocenę oraz podjąć nową decyzję.

128. Aby zapewnić zgodność z procedurami dotyczącymi konfliktu interesów, instytucje powinny zapewnić, aby wszystkie obowiązujące procedury kontrolne miały bezpośrednie zastosowanie do pożyczek i innych transakcji z członkami organu zarządzającego lub powiązanymi z nimi osobami, oraz aby obowiązywały odpowiednie procedury nadzoru na poziomie organu zarządzającego w ramach sprawowanej przez niego funkcji nadzorczej.

12.2 Dokumentacja dotycząca pożyczek dla członków organu zarządzającego i powiązanych z nimi osób oraz informacje dodatkowe

129. W kontekście art. 88 ust. 1 dyrektywy 2013/36/UE, instytucje powinny dokumentować informacje dotyczące pożyczek[34] dla członków organu zarządzającego i powiązanych z nimi osób, która to dokumentacja powinna zawierać co najmniej następujące elementy:

a. imię i nazwisko dłużnika i jego status (tj. członek organu zarządzającego lub osoba powiązana) oraz, w odniesieniu do pożyczek dla osoby powiązanej, dane członka organu zarządzającego, z którym taka osoba jest powiązana, oraz rodzaj powiązania;

b. rodzaj/charakter i kwota pożyczki;

c. warunki mające zastosowanie do pożyczki;

d. data zatwierdzenia pożyczki;

e. imię i nazwisko osoby, lub nazwa i skład organu, podejmujących decyzję o zatwierdzeniu pożyczki i warunków jej udzielenia;

[34] Zob. też wytyczne EUNB dotyczące udzielania kredytów, dostępne pod adresem: https://eba.europa.eu/regulation-and-policy/credit-risk/guidelines-on-loan-origination-and-monitoring.

f. czy pożyczka została udzielona na warunkach rynkowych (tak/nie); oraz

g. czy pożyczka została udzielona na warunkach dostępnych dla wszystkich pracowników (tak/nie).

130. Instytucje powinny zapewnić, aby dokumentacja dotycząca wszystkich pożyczek dla członków organu zarządzającego i powiązanych z nimi osób była kompletna i aktualizowana w taki sposób, aby instytucja mogła udostępnić właściwym organom pełną dokumentację w odpowiednim formacie, na żądanie i bez zbędnej zwłoki.

131. W przypadku pożyczki dla członka organu zarządzającego lub powiązanej z nim osoby w wysokości powyżej 200 000 euro, instytucje powinny być w stanie przedstawić właściwemu organowi, na jego żądanie, następujące informacje dodatkowe:

a. wartość procentowa pożyczki oraz wartość procentowa sumy wszystkich należnych kwot od tego samego dłużnika, w porównaniu ze:

i. wskaźnikiem kapitału Tier 1 oraz wskaźnikiem kapitału Tier 2, oraz

ii. wskaźnikiem kapitału podstawowego Tier-1 instytucji;

b. czy pożyczka stanowi część dużej ekspozycji kredytowej[35]; oraz

c. relatywnej wagi zagregowanej sumy wszystkich należnych kwot z tytułu pożyczki od tego samego dłużnika, obliczonej jako wartość procentowa poprzez podzielenie kwoty należnej przez łączną kwotę należną z tytułu wszystkich pożyczek dla członków organu zarządzającego i powiązanych z nimi osób.

13 Wewnętrzne procedury ostrzegania

132. 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 wystąpienie naruszenia; powinni oni jednak mieć wystarczającą pewność, aby uzasadnione było wszczęcie dochodzenia. Instytucje powinny również wdrożyć odpowiednie procesy i procedury zapewniające przestrzeganie przez instytucje nałożonych obowiązków związanych z wdrożeniem do porządku krajowego dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii.

133. Aby uniknąć konfliktów interesów, powinna istnieć możliwość zgłaszania przez pracowników naruszeń poza normalną hierarchią służbową (np. za pośrednictwem komórki ds. zgodności z przepisami, komórki audytu wewnętrznego lub niezależnej wewnętrznej

[35] Zob. też część IV rozporządzenia (UE) nr 575/2013, w szczególności art. 392.

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 rozporządzeniem 2016/679/UE[36] (RODO).

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

135. Informacje dostarczone przez pracowników za pośrednictwem procedur ostrzegania należy udostępnić organowi zarządzającemu oraz innym odpowiedzialnym komórkom określonym w polityce wewnętrznego ostrzegania. Na żądanie pracownika zgłaszającego 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.

136. 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 podjąć odpowiednie środki przeciw osobom odpowiedzialnym za jakiekolwiek tego rodzaju represje.

137. 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 zastosowania określonych środków instytucja powinna podjąć je w taki sposób, aby chronić daną osobę przed niezamierzonymi negatywnymi skutkami wykraczającymi poza cel podjętych środków.

138. 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 rozporządzeniem (UE) 2016/679, 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;

[36] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

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

139. 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 rozporządzeniem (UE) 2016/679 (RODO); oraz

d. jasne procedury określone w sekcji 13.

140. 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

141. Instytucje powinny wypracować oraz utrzymywać kulturę zachęcającą do pozytywnego nastawienia do kontroli ryzyka i zgodności z przepisami w instytucji, a także solidne i kompleksowe ramy kontroli wewnętrznej. W tych ramach linie biznesowe instytucji powinny być odpowiedzialne 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 ustanowić komórki kontroli wewnętrznej dysponujące wystarczającymi

uprawnieniami, statusem i dostępem do organu zarządzającego, aby móc wypełniać swoją funkcję, oraz ustanowić ramy zarządzania ryzykiem.

142. Ramy kontroli wewnętrznej instytucji powinny być dostosowane do specyfiki jej działalności, jej złożoności i związanego z nią ryzyka, z uwzględnieniem kontekstu grupy. Instytucje powinny 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. zgodności z przepisami i komórką ds. zgodności z przepisami w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, w przypadkach kiedy jest to osobna komórka kontrolna, na poziomie grupy oraz między kierownikami komórek kontroli wewnętrznej na szczeblu grupy oraz organem zarządzającym instytucji.

143. Instytucje powinny wdrożyć odpowiednie procesy i procedury zapewniające przestrzeganie obowiązków instytucji w kontekście przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Instytucje powinny ocenić swoją ekspozycję na ryzyko związane z wykorzystaniem instytucji do celów prania pieniędzy i finansowania terroryzmu oraz, jeśli to konieczne, podjąć kroki ograniczające takie ryzyko, a także powiązane z nim ryzyko operacyjne i ryzyko utraty reputacji. Instytucje powinny podjąć kroki w celu zapewnienia, aby ich personel był świadomy ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu oraz wpływu ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu na instytucję i na rzetelność systemu finansowego.

144. 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.

145. 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

146. 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. zgodności z przepisami o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu – jeśli funkcjonują oddzielnie od komórki ds. zgodności z przepisami, oraz komórki audytu wewnętrznego). Instytucje powinny ustanowić, utrzymywać i regularnie aktualizować odpowiednią pisemną politykę, mechanizmy i procedury kontroli wewnętrznej, które powinny zostać zatwierdzone przez organ zarządzający.

147. Instytucja powinna wdrożyć 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.

148. Instytucje powinny poinformować o polityce, mechanizmach i procedurach wszystkich pracowników za każdym razem, gdy zostają w nich wprowadzone istotne zmiany.

149. Wdrażając ramy kontroli wewnętrznej, instytucje powinny ustanowić odpowiedni podział obowiązków, np. powierzenie sprzecznych czynności w zakresie przetwarzania transakcji lub świadczenia usług różnym osobom lub 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.

150. Komórki kontroli wewnętrznej powinny sprawdzać, czy polityka, mechanizmy i procedury określone w ramach kontroli wewnętrznej są prawidłowo wdrażane w poszczególnych obszarach, za które komórki te odpowiadają.

151. Komórki kontroli wewnętrznej powinny regularnie przedkładać organowi zarządzającemu sprawozdania dotyczące zidentyfikowanych poważnych uchybień. W przypadku każdego nowego wykrytego poważnego uchybienia sprawozdania te powinny zawierać informację o związanych z tym zagrożeniach, ocenę wpływu, zalecenia i działania naprawcze, które należy podjąć. Organ zarządzający powinien odpowiednio szybko i skutecznie reagować na ustalenia funkcji kontroli wewnętrznej oraz żądać adekwatnych działań naprawczych. Należy opracować formalną procedurę reagowania na dokonane ustalenia i podejmowania działań naprawczych.

17 Ramy zarządzania ryzykiem

152. W ramach ogólnych ram kontroli wewnętrznej instytucje powinny posiadać kompleksowe 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 ryzyko pozabilansowe, a także rzeczywiste i przyszłe ryzyko, na jakie może być narażona instytucja. Ocena ryzyka powinna mieć charakter oddolny i odgórny oraz być przeprowadzana 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. Ramy zarządzania ryzykiem powinny obejmować wszystkie istotne rodzaje ryzyka, z należytym uwzględnieniem ryzyka zarówno finansowego, jak i niefinansowego, w tym ryzyka kredytowego, rynkowego, ryzyka płynności, koncentracji, ryzyka operacyjnego, informatycznego, ryzyka utraty reputacji, ryzyka prawnego, ryzyka związanego z kodeksem postępowania, ryzyka związanego ze zgodnością z przepisami o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu oraz innymi przestępstwami finansowymi, ryzyka środowiskowego, społecznego i związanego z zarządzaniem oraz ryzyka strategicznego.

153. 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.

154. Ramy zarządzania ryzykiem instytucji powinny dostarczać konkretnych wskazówek na temat wdrażania jej strategii. W stosownych przypadkach we wskazówkach tych należy zawrzeć i monitorować limity wewnętrzne zgodne z gotowością instytucji do podejmowania ryzyka oraz dostosowane do potrzeb jej prawidłowego działania, kondycji 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.

155. Ramy zarządzania ryzykiem powinny podlegać niezależnemu przeglądowi wewnętrznemu, np. dokonywanemu przez komórkę audytu wewnętrznego, oraz regularnej ocenie pod kątem gotowości 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.

156. W odniesieniu do identyfikacji oraz pomiaru lub oceny ryzyka, instytucja powinna opracować odpowiednie metodologie obejmujące zarówno narzędzia prognostyczne, jak i retrospektywne. Metodologie 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 z gotowością

instytucji do podejmowania ryzyka, a także określenie i ocenę potencjalnych ekspozycji na ryzyko, także w warunkach skrajnych, w różnych zakładanych niekorzystnych okolicznościach w porównaniu ze zdolnością 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.

157. 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.

158. 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.

159. 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).

160. Oprócz własnych ocen instytucje mogą 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.

161. 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.

162. 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 procesów 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[37]

163. 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 transakcje wyjątkowe. 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 gotowością instytucji do podejmowania ryzyka oraz z odpowiednimi limitami obowiązującymi w instytucji, lub też zapewnić wprowadzenie niezbędnych zmian.

164. 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 lub ram lub procedur zarządzania ryzykiem; oraz zmiany organizacji instytucji.

165. Instytucja powinna stosować konkretne procedury oceny zgodności z postanowieniami takiej polityki, uwzględniając wkład komórki ds. zarządzania ryzykiem. Powinno to obejmować systematyczną uprzednią ocenę i udokumentowaną opinię wydaną przez komórkę ds. zgodności z przepisami w odniesieniu do nowych produktów lub znaczących zmian dotychczasowych produktów.

166. 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.

167. 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. Dodatkowo w celu wypełnienia obowiązków wynikających z dyrektywy (UE) 2015/849, instytucje powinny

[37] 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.

zidentyfikować i ocenić ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu powiązane z nowym produktem lub praktyką biznesową, oraz wdrożyć środki ograniczające takie 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 do zrozumienia związanego z nią ryzyka i zarządzania nim.

168. W zatwierdzaniu nowych produktów lub znaczących zmian dotychczasowych produktów, procesów i systemów powinny uczestniczyć komórka ds. zarządzania ryzykiem i komórka ds. zgodności z przepisami. 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 również mieć jasny zarys 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

169. Wśród komórek kontroli wewnętrznej powinna znaleźć się komórka ds. zarządzania ryzykiem (zob. sekcję 20), komórka ds. zgodności z przepisami (zob. sekcję 21) oraz komórka audytu wewnętrznego (zob. sekcję 22). Komórki ds. zarządzania ryzykiem i ds. zgodności z przepisami powinny podlegać przeglądowi ze strony komórki audytu wewnętrznego. Zadania funkcji kontrolnych obejmują również zapewnienie zgodności z wymogami dotyczącymi przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

170. 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 lub 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.

171. Bez uszczerbku dla transpozycji dyrektywy 2015/849/UE do prawa krajowego, instytucje powinny przypisać odpowiedzialność za zapewnienie przestrzegania przez instytucję wymogów tej dyrektywy oraz za realizację polityk i procedur w instytucji w tym zakresie, określonemu pracownikowi (np. kierownikowi działu zgodności z przepisami). Instytucje mogą wyznaczyć oddzielną komórkę ds. zgodności z przepisami w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, jako niezależną komórkę kontrolną[38]. Osoba odpowiedzialna za przestrzeganie regulacji dotyczących przeciwdziałania praniu pieniędzy i

[38] Zob. też wytyczne EUNB dotyczące komórki ds. przestrzegania przepisów w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (aktualnie w opracowaniu).

finansowaniu terroryzmu powinna bezpośrednio podlegać, o ile to możliwe, organowi zarządzającemu zarówno w ramach jego funkcji zarządczej, jak i nadzorczej.

19.1 Kierownicy komórek kontroli wewnętrznej

172. 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. zgodności z przepisami i audytu wewnętrznego powinni podlegać organowi zarządzającemu oraz ponosić bezpośrednią odpowiedzialność przed tym organem, a oceny ich wyników powinien dokonywać organ zarządzający.

173. W razie konieczności kierownicy komórek kontroli wewnętrznej powinni mieć dostęp do organu zarządzającego pełniącego funkcję nadzorczą i bezpośrednio go informować, aby zwrócić uwagę na zagrożenia i ostrzec, gdy jest to wskazane, jeśli konkretne czynniki wpływają albo mogą wpłynąć na instytucję. Nie powinno to uniemożliwiać kierownikom komórek kontroli wewnętrznej sprawozdawczości w obrębie ich regularnej hierarchii podległości służbowej.

174. Instytucje powinny ustanowić udokumentowane procesy mianowania kierownika komórki kontroli wewnętrznej oraz cofania jego uprawnień. W każdym przypadku kierownicy komórek kontroli wewnętrznej nie powinni być usuwani ze stanowiska bez uprzedniej zgody organu zarządzającego pełniącego funkcję nadzorczą; nie wolno również na mocy art. 76 ust. 5 dyrektywy 2013/36/UE usuwać ze stanowiska kierownika komórki ds. zarządzania ryzykiem 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

175. 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[39].

19.3 Łączenie komórek kontroli wewnętrznej

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

19.4 Zasoby komórek kontroli wewnętrznej

177. 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 monitorowany na bieżąco i powinni oni odbywać niezbędne szkolenia.

178. 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

179. 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.

180. 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.

[39] 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.

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

182. 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.

183. 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.

184. 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.

185. 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.

186. 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 strategią instytucji w zakresie ryzyka oraz gotowością instytucji do podejmowania 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

187. 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 gotowości instytucji do podejmowania ryzyka. KZR powinna ocenić solidność i trwałość strategii w zakresie ryzyka oraz gotowości do jego podejmowania. Powinna ona zapewnić, aby gotowość do podejmowania ryzyka przekładała się na konkretne limity ryzyka. KZR powinna również ocenić strategie jednostek biznesowych w zakresie ryzyka i gotowość jednostek biznesowych do

podejmowania ryzyka oraz zaangażować się w podejmowanie decyzji dotyczących strategii w zakresie ryzyka i gotowości do podejmowania ryzyka przez organ zarządzający. Cele powinny być wiarygodne i spójne ze strategią instytucji w zakresie ryzyka.

188. 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

189. 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.

190. 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

191. KZR powinna zapewnić, aby wdrożono odpowiednie ramy zarządzania ryzykiem oraz aby wszystkie rodzaje ryzyka były identyfikowane, oceniane, mierzone, monitorowane, zarządzane i odpowiednio raportowane przez odpowiednie jednostki w instytucji.

192. 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.

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

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

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

196. 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.

197. 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

198. KZR powinna dokonywać niezależnej oceny przypadków naruszeń gotowości 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.

199. 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

200. Kierownik KZR powinien być odpowiedzialny za dostarczenie kompleksowych i zrozumiałych informacji na temat ryzyka oraz doradztwo dla organu zarządzającego, aby umożliwić temu organowi zrozumienie ogólnego profilu ryzyka instytucji. To samo dotyczy kierownika KZR instytucji dominującej na poziomie skonsolidowanym.

201. 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 funkcję kierownika KZR, z uwzględnieniem zasady proporcjonalności określonej w tytule I, funkcja ta może być połączona z funkcją kierownika komórki ds. zgodności z przepisami lub też może być wykonywana przez innego pracownika wyższego szczebla 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).

202. 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 dotyczących ustanowienia limitów) podejmowanych na szczeblach poniżej organu zarządzającego, powinna ona określić zakres takiego prawa weta, procedury przekazywania sprawy na wyższy szczebel lub procedury odwoławcze, a także sposób zaangażowania organu zarządzającego.

203. 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 strategią instytucji w zakresie ryzyka oraz gotowością instytucji do podejmowania ryzyka.

21 Funkcja zapewnienia zgodności z przepisami

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

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

206. Komórka ds. zgodności z przepisami, 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 lub połączona z KZR lub innymi odpowiednimi komórkami, np. działem prawnym lub kadrowym.

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

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

209. Komórka ds. zgodności z przepisami 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 zgodności z przepisami.

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

211. Zgodnie z sekcją 18 niniejszych wytycznych komórka ds. zgodności z przepisami 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.

212. Instytucje powinny podjąć odpowiednie działania odnośnie do zachowań praktykowanych w relacjach wewnętrznych lub zewnętrznych, które mogą umożliwić popełnienie oszustwa, pranie pieniędzy lub finansowanie terroryzmu, lub popełnienie innego przestępstwa finansowego i naruszenie dyscypliny (np. naruszenie procedur wewnętrznych, naruszenie limitów).

213. 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 zgodności z przepisami 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. zgodności z przepisami lub kierownika ds. zgodności z przepisami instytucji konsolidującej.

22 Komórka audytu wewnętrznego

214. 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 gotowością do podejmowania ryzyka.

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

216. 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.

217. 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.

218. 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 strategią instytucji w zakresie ryzyka i gotowością instytucji do podejmowania 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. zgodności z przepisami.

219. 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.

220. 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.

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

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

223. 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.

224. 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[40]

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

226. Instytucje mogą ustanowić konkretną niezależną komórkę ds. ciągłości działania, np. w ramach KZR[41].

227. Działalność instytucji jest uzależniona od pewnych zasobów o znaczeniu krytycznym (np. systemów informatycznych, w tym usług w chmurze, systemów łączności, personelu podstawowego 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).

228. Aby ustanowić prawidłowy plan zarządzania ciągłością działania, instytucja powinna poddać starannej analizie czynniki ryzyka i własną ekspozycję 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.

[40] Instytucje powinny zapoznać się również z wytycznymi EUNB w zakresie ryzyka ICT, dostępnymi pod adresem: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management.
[41] Zob. też art. 312 rozporządzenia (UE) nr 575/2013.

229. 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 z gotowością instytucji do podejmowania ryzyka.

230. Plany awaryjne, plany ciągłości działania i plany 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

231. 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.

232. 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.

233. 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[42], w podziale na kraje.

234. 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;

[42] 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).

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

c. nowe struktury prawne, struktury zarządzania lub struktury 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 działania.

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)
3. skład i funkcjonowanie organu zarządzającego
   a) kryteria selekcji, w tym sposób uwzględniania kwestii różnorodności
   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. zgodności z przepisami
   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
7. opis strategii dotyczącej ryzyka oraz ram zarządzania ryzykiem

8. 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) świadczenie usług w ramach swobody świadczenia usług
    f) oddziały
    g) jednostki zależne, spółki joint venture itp.
    h) korzystanie z centrów offshore
9. 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
10. status polityki w zakresie zarządzania wewnętrznego wraz z jej datą
    a) opracowanie
    b) ostatnia zmiana
    c) ostatnia ocena
    d) zatwierdzenie przez organ zarządzający.