EBA/GL/2017/11

21/03/2018

Obecné pokyny

k vnitřnímu systému správy a řízení

1. Dodržování předpisů a oznamovací povinnost

Status těchto obecných pokynů

1. Tento dokument obsahuje obecné pokyny vydané podle článku 16 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 [1]. V souladu s čl. 16 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 příslušné orgány a finanční instituce vynaloží veškeré úsilí, aby se těmito obecnými pokyny řídily.

2. Obecné pokyny formulují názor orgánu EBA na náležité postupy dohledu v rámci Evropského systému dohledu nad finančním trhem nebo na to, jak by unijní právní předpisy měly být uplatňovány v konkrétní oblasti. Příslušné orgány ve smyslu čl. 4 odst. 2 nařízení (EU) č. 1093/2010, na které se tyto obecné pokyny vztahují, by s nimi měly být v souladu a začlenit je do svých postupů (např. pozměněním právního rámce nebo dohledových postupů), včetně případů, kdy jsou obecné pokyny zaměřeny v prvé řadě na instituce.

Oznamovací povinnost

3. V souladu s čl. 16 odst. 3 nařízení (EU) č. 1093/2010 musí příslušné orgány do 21/05/2018 orgánu EBA oznámit, zda se těmito obecnými pokyny řídí nebo hodlají řídit, a v opačném případě uvést do tohoto data důvody, proč se jimi neřídí či nehodlají řídit. Neposkytnou-li příslušné orgány oznámení v této lhůtě, bude mít orgán EBA za to, že se těmito obecnými pokyny neřídí nebo nehodlají řídit. Oznámení by měla být zasílána na formuláři, který je k dispozici na internetových stránkách orgánu EBA, na adresu compliance@eba.europa.eu s označením „EBA/GL/2017/11“. Oznámení by měly předkládat osoby s příslušným oprávněním oznamovat, zda se jejich příslušné orgány těmito obecnými pokyny řídí nebo hodlají řídit. Jakoukoli změnu stavu dodržování pokynů je rovněž nutno oznámit orgánu EBA.

4. Oznámení budou zveřejněna na internetových stránkách orgánu EBA v souladu s čl. 16 odst. 3.

[1] Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331, 15.12.2010, s. 12).

2. Předmět, oblast působnosti a definice

Předmět

5. Tyto obecné pokyny upřesňují systém, procesy a mechanismy vnitřní správy a řízení, které musí úvěrové instituce a investiční podniky zavést v souladu s čl. 74 odst. 1 směrnice 2013/36/EU[2] s cílem zajistit účinné a obezřetné řízení instituce.

Adresáti

6. Tyto obecné pokyny jsou určeny příslušným orgánům vymezeným v čl. 4 odst. 1 bodě 40 nařízení (EU) č. 575/2013[3], mezi něž patří i Evropská centrální banka, pokud jde o záležitosti vztahující se k úkolům, které jí byly svěřeny nařízením (EU) č. 1024/2013, a institucím vymezeným v čl. 4 odst. 1 bodě 3 nařízení (EU) č. 575/2013.

Oblast působnosti

7. Tyto obecné pokyny se uplatňují v souvislosti se systémy správy a řízení institucí, včetně jejich organizační struktury a odpovídající odpovědnosti, procesů sloužících k identifikaci, řízení, sledování a vykazování rizik, jimž jsou nebo mohou být vystaveny, a rámce vnitřní kontroly.

8. Cílem obecných pokynů je, aby zahrnovaly všechny stávající struktury orgánů a neobhajovaly žádnou konkrétní strukturu. Obecné pokyny nezasahují do obecného rozdělení pravomocí podle vnitrostátního práva obchodních společností. Měly by být proto uplatňovány bez ohledu na strukturu orgánů (unitární a/nebo duální struktura orgánů a/nebo jiná struktura) používanou v členských státech. Vedoucí orgán, který je definován v čl. 3 odst. 1 bodech 7 a 8 směrnice 2013/36/EU, by měl být chápán jako orgán mající řídící (výkonnou) a kontrolní (nevýkonnou) funkci[4].

9. Pojmy „vedoucí orgán v řídící funkci“ a „vedoucí orgán v kontrolní funkci“ jsou v těchto obecných pokynech používány, aniž by odkazovaly na konkrétní strukturu správy a řízení, a odkazy na řídící (výkonnou) nebo kontrolní (nevýkonnou) funkci by se měly vykládat tak, že se vztahují k orgánům nebo členům vedoucího orgánu odpovědným za danou funkci v souladu s vnitrostátním právem. Při provádění těchto obecných pokynů by měly příslušné orgány

[2] Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (Úř. věst. L 176, 27.6.2013, s. 338).

[3] Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012 (Úř. věst. L 176, 27.6.2013, s. 1–337).

[4] Viz též 56. bod odůvodnění směrnice 2013/36/EU.

přihlížet k vnitrostátnímu právu obchodních společností a v případě potřeby stanovit, na jaký orgán nebo členy vedoucího orgánu by se uvedené funkce měly vztahovat.

10. V členských státech, kde vedoucí orgán částečně nebo plně pověřuje výkonnými funkcemi osobu nebo vnitřní výkonný orgán (např. výkonného ředitele (CEO), tým vedoucích pracovníků nebo výkonný výbor), by měly být osoby, které tyto výkonné funkce na základě pověření vykonávají, považovány za součást řídící funkce vedoucího orgánu. Pro účely těchto obecných pokynů se jakýkoliv odkaz na vedoucí orgán v jeho řídící funkci vykládá tak, že zahrnuje rovněž členy výkonného orgánu nebo výkonného ředitele (CEO) v souladu s definicí v těchto obecných pokynech, a to i v případě, že nebyli navrženi či jmenováni formálními členy řídícího orgánu nebo orgánů instituce podle vnitrostátního práva.

11. V členských státech, kde jsou určité povinnosti vykonávány přímo akcionáři, společníky nebo vlastníky instituce namísto vedoucího orgánu, by instituce měly zajistit, aby tyto povinnosti a související rozhodnutí byly v maximálním možném rozsahu v souladu s obecnými pokyny, které se vztahují na vedoucí orgán.

12. Definice výkonného ředitele (CEO), finančního ředitele (CFO) a držitele klíčových funkcí používané v těchto obecných pokynech jsou čistě funkční a nemají ukládat jmenování těchto vedoucích pracovníků nebo vytvoření těchto pozic, pokud tak nestanovuje příslušné právo EU nebo vnitrostátní právní předpisy.

13. Instituce by měly dodržovat a příslušné orgány by měly zajistit, aby instituce dodržovaly tyto obecné pokyny na individuálním, subkonsolidovaném a konsolidovaném základě v souladu s úrovní použití stanovenou v článku 109 směrnice 2013/36/EU.

Definice

14. Není-li uvedeno jinak, mají pojmy použité a vymezené směrnicí 2013/36/EU v těchto obecných pokynech stejný význam. Kromě toho pro účely těchto obecných pokynů platí tyto definice:

Ochota podstupovat riziko	znamená souhrnnou míru a druhy rizik, které je instituce ochotná podstupovat v rámci své schopnosti nést riziko v souladu se svým obchodním modelem, aby dosáhla svých strategických cílů.
Schopnost nést riziko	je maximální míra rizika, kterou je instituce schopna podstoupit vzhledem ke své kapitálové základně, schopnosti řídit a kontrolovat riziko a vzhledem k regulačním omezením.
Kultura řízení rizik	jsou normy, přístupy a chování instituce vztahující se k informovanosti o rizicích a k řízení rizik a kontroly, které utvářejí rozhodnutí týkající se rizik. Kultura řízení rizik ovlivňuje rozhodnutí vedoucích pracovníků a zaměstnanců při výkonu běžné činnosti a má dopad na rizika, která podstupují.

Instituce	jsou úvěrové instituce a investiční podniky definované v čl. 4 odst. 1 bodě 1 a 2 nařízení (EU) č. 575/2013.
Zaměstnanci	jsou všichni zaměstnanci instituce a jejích dceřiných podniků, které spadají do rozsahu její konsolidace, včetně dceřiných podniků, na které se nevztahuje směrnice 2013/36/EU, a všichni členové vedoucího orgánu v jeho řídící funkci a v jeho kontrolní funkci.
Výkonný ředitel (CEO)	je osoba, která je odpovědná za řízení a vedení celkové podnikatelské činnosti instituce.
Finanční ředitel (CFO)	je osoba, která nese celkovou odpovědnost za řízení všech následujících činností: řízení finančních zdrojů, finanční plánování a finanční výkaznictví.
Vedoucí funkcí vnitřní kontroly	jsou osoby na nejvyšší hierarchické úrovni pověřené účinným řízením každodenního výkonu nezávislého řízení rizik, zajišťování shody s předpisy a vnitřního auditu.
Držitelé klíčových funkcí	jsou osoby, které mají výrazný vliv na směřování instituce, ale které nejsou členy vedoucího orgánu ani výkonným ředitelem (CEO). Jedná se o osoby zastávající místa vedoucích funkcí vnitřní kontroly a finančního ředitele, pokud nejsou členy vedoucího orgánu, a další držitele klíčových funkcí, pokud jsou institucemi na základě posouzení rizik identifikováni. K dalším držitelům klíčových funkcí mohou patřit vedoucí významných linií podnikání, poboček v Evropském hospodářském prostoru či Evropském sdružení volného obchodu, dceřiných podniků v třetích zemích a dalších interních funkcí.
Obezřetnostní konsolidace	je uplatnění obezřetnostních pravidel stanovených ve směrnici 2013/36/EU a nařízení (EU) č. 575/2013 na konsolidovaném nebo subkonsolidovaném základě v souladu s částí první hlavou II kapitolou 2 nařízení (EU) č. 575/2013. Obezřetnostní konsolidace zahrnuje všechny dceřiné podniky, které jsou institucemi nebo finančními institucemi podle definice v čl. 4 odst. 3 a 26 nařízení (EU) č. 575/2013, a může rovněž zahrnovat podniky pomocných služeb podle definice v čl. 2 odst. 18 uvedeného nařízení zřízené v EU i mimo EU.
Konsolidující instituce	je instituce, která musí dodržovat obezřetnostní požadavky na základě konsolidované situace v souladu s částí první hlavou II kapitolou 2 nařízení (EU) č. 575/2013.
Významné instituce	jsou instituce uvedené v článku 131 směrnice 2013/36/EU (globální systémově významné instituce, tj. „G-SVI“ a jiné systémově významné instituce, tj. „J-SVI“) a podle potřeby jiné instituce určené příslušným orgánem nebo vnitrostátním právem

	na základě posouzení velikosti a interní organizace institucí a povahy, rozsahu a složitosti jejich činností.
Kótovaná instituce podle směrnice o kapitálových požadavcích	jsou instituce, jejichž finanční nástroje jsou v jednom nebo několika členských státech připuštěny k obchodování na regulovaném trhu nebo v mnohostranném obchodním systému podle definice v čl. 4 odst. 21 a 22 směrnice 2014/65/EU[5].
Akcionář	je osoba, která vlastní akcie instituce, nebo v závislosti na právní formě instituce jiní vlastníci instituce nebo společníci v instituci.
Funkce člena ve vedoucím orgánu	je pozice člena vedoucího orgánu instituce nebo jiné právnické osoby.

3. Provádění

Datum použití

15. Tyto obecné pokyny se použijí od 30. června 2018.

Zrušení

16. S účinností od 30. června 2018 se zrušují obecné pokyny Evropského orgánu pro bankovnictví k internal governance (řídicí a kontrolní systém) (GL 44) ze dne 27. září 2011.

[5] Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU (Úř. věst. L 173, 12.6.2014, s. 349).

4. Obecné pokyny

Hlava I – Proporcionalita

17. Zásada proporcionality zakotvená v čl. 74 odst. 2 směrnice 2013/36/EU má zajistit, aby systém správy a řízení odpovídal individuálnímu rizikovému profilu a obchodnímu modelu instituce tak, aby byly skutečně naplněny cíle regulačních požadavků.

18. Při vytváření a provádění vnitřního řídicího a kontrolního systému by instituce měly zohledňovat svoji velikost a vnitřní organizaci a povahu, rozsah a složitost svých činností. Významné instituce by měly mít sofistikovanější systém správy a řízení, zatímco malé a méně složité instituce mohou používat jednodušší systém správy a řízení.

19. Za účelem uplatňování zásady proporcionality a s cílem zajistit vhodné provádění požadavků by instituce a příslušné orgány měly brát v potaz následující kritéria:

    a. velikost z hlediska bilanční sumy instituce a jejích dceřiných podniků v rámci obezřetnostní konsolidace;

    b. geografickou přítomnost instituce a rozsah jejích operací v každé jurisdikci;

    c. právní formu instituce, včetně toho, zda je instituce součástí skupiny, a v takovém případě pak hodnocení proporcionality za příslušnou skupinu;

    d. zda se jedná nebo nejedná o kótovanou instituci;

    e. zda je instituce oprávněna používat interní modely k měření kapitálových požadavků (např. přístup založený na interním ratingu);

    f. druh povolené činnosti a služeb vykonávaných institucí (např. viz rovněž příloha 1 směrnice 2013/36/EU a příloha 1 směrnice 2014/65/EU);

    g. základní obchodní model a strategii; povahu a složitost obchodní činnosti a organizační strukturu instituce;

    h. strategii v oblasti rizik, ochotu podstupovat riziko a skutečný rizikový profil instituce se současným přihlédnutím k výsledku hodnocení kapitálu a likvidity v procesu dohledu a hodnocení (SREP);

    i. vlastnickou strukturu a strukturu financování instituce;

j. druh klientů (např. retailoví, korporátní, institucionální, malé podniky, veřejné subjekty) a složitost produktů nebo smluv;

k. externě zajišťovanou činnost a distribuční kanály; a

l. existující informační (IT) systémy, včetně systémů zajišťování kontinuity a outsourcingu v této oblasti.

Hlava II – Úloha a složení vedoucího orgánu a výborů

1 Úloha a odpovědnosti vedoucího orgánu

20. Podle čl. 88 odst. 1 směrnice 2013/36/EU musí nést vedoucí orgán za instituci konečnou a celkovou odpovědnost a vymezuje a kontroluje systém správy a řízení a je odpovědný za provádění systému správy a řízení zajišťujícího účinné a obezřetné řízení instituce v dané instituci.

21. Povinnosti vedoucího orgánu by měly být jasně vymezeny, přičemž by měly být odlišeny povinnosti řídící (výkonné) funkce a kontrolní (nevýkonné) funkce. Odpovědnosti a povinnosti vedoucího orgánu by měly být popsány v písemném dokumentu a řádně schváleny vedoucím orgánem.

22. Všichni členové vedoucího orgánu by měli být plně seznámeni se strukturou a povinnostmi vedoucího orgánu a s rozdělením úkolů mezi různé funkce vedoucího orgánu a jeho výbory. Kvůli zajištění odpovídající kontroly a vyváženosti působností by při rozhodování neměl dominovat jediný člen nebo malá skupina členů. Vedoucí orgán by měl v kontrolní funkci a v řídící funkci účinně spolupracovat. Obě funkce by si měly navzájem poskytovat dostatečné informace umožňující jim vykonávat jejich příslušnou úlohu.

23. K povinnostem vedoucího orgánu by mělo patřit stanovování, schvalování a kontrola provádění:

a. celkové obchodní strategie a hlavních politik instituce v mezích platného právního a regulačního rámce s ohledem na dlouhodobé finanční zájmy a solventnost instituce;

b. celkové strategie v oblasti rizik, včetně ochoty instituce podstupovat riziko a jejího rámce řízení rizik a opatření s cílem zajistit, aby vedoucí orgán věnoval otázkám rizika dostatek času;

c. přiměřeného a účinného systému správy a řízení a rámce vnitřní kontroly, který zahrnuje jasnou organizační strukturu a dobře fungující nezávislé interní funkce řízení rizik, zajišťování shody s předpisy a vnitřního auditu, jež mají dostatečnou pravomoc, váhu a zdroje potřebné k vykonávání těchto funkcí;

d. hodnoty, typy a rozdělení vnitřně stanoveného i regulatorního kapitálu k přiměřenému pokrytí rizik instituce;

e. cílů řízení likvidity instituce;

f. zásad odměňování, které jsou v souladu se zásadami odměňování stanovenými v článcích 92 až 95 směrnice 2013/36/EU a v obecných pokynech EBA k řádným zásadám odměňování podle čl. 74 odst. 3 a čl. 75 odst. 2 směrnice 2013/36/EU[6];

g. opatření, jejichž cílem je zajistit účinné provádění individuálního a kolektivního posouzení vhodnosti vedoucího orgánu, vhodné složení a plánování nástupnictví vedoucího orgánu a účinné provádění funkcí vedoucího orgánu[7];

h. procesu výběru a posouzení vhodnosti držitelů klíčových funkcí[8];

i. opatření, jejichž cílem je zajistit vnitřní fungování každého případně zřízeného výboru vedoucího orgánu, přičemž je potřeba blíže určit:

    i. úlohu, složení a úkoly každého z nich;

    ii. vhodný tok informací, včetně dokumentace doporučení a závěrů, a hierarchické vztahy mezi každým výborem a vedoucím orgánem, příslušnými orgány a dalšími stranami;

j. kulturu řízení rizik v souladu s oddílem 9 těchto obecných pokynů, která se zabývá informovaností instituce o rizicích a rizikovým chováním;

k. korporátní kulturu a hodnoty v souladu s oddílem 10, která podporuje odpovědné a etické chování, včetně kodexu chování nebo srovnatelného nástroje;

l. zásady týkající se střetu zájmů na institucionální úrovni v souladu s oddílem 11 a zaměstnanců v souladu s oddílem 12; a

m. opatření, jejichž cílem je zajistit integritu účetních systémů a systémů finančního výkaznictví, včetně finančních a provozních kontrol a dodržování zákonů a příslušných standardů.

24. Vedoucí orgán musí dohlížet na proces zveřejňování informací a na komunikaci s externími zúčastněnými osobami a příslušnými orgány.

[6] Obecné pokyny EBA k řádným zásadám odměňování podle čl. 74 odst. 3 a čl. 75 odst. 2 směrnice 2013/36/EU a k informacím zveřejňovaným podle článku 450 nařízení (EU) č. 575/2013 (EBA/GL/2015/22).

[7] Viz rovněž společné pokyny ESMA a EBA k posouzení vhodnosti členů vedoucího orgánu a držitelů klíčových funkcí podle směrnice 2013/36/EU a směrnice 2014/65/EU.

[8] Viz rovněž společné pokyny ESMA a EBA k posouzení vhodnosti členů vedoucího orgánu a držitelů klíčových funkcí podle směrnice 2013/36/EU a směrnice 2014/65/EU.

25. Všichni členové vedoucího orgánu by měli být s přihlédnutím k hospodářskému prostředí informováni o celkové činnosti instituce, její finanční situaci a situaci související s riziky a o přijatých rozhodnutích, která mají významný dopad na podnikání instituce.

26. Člen vedoucího orgánu může nést odpovědnost za funkci vnitřní kontroly zmíněnou v hlavě V bodě 19.1 za předpokladu, že dotyčný člen nemá jiné mandáty, které by narušily činnost vnitřní kontroly a nezávislost funkce vnitřní kontroly.

27. Vedoucí orgán by měl sledovat, pravidelně přezkoumávat a řešit případné nedostatky zjištěné ve vztahu k provádění procesů, strategií a politik souvisejících s povinnostmi uvedenými v odstavcích 23 a 24. Vnitřní rámec správy a řízení a jeho provádění je potřeba pravidelně přezkoumávat a aktualizovat s přihlédnutím k zásadě proporcionality, jak je dále vysvětleno v hlavě I. V případě podstatných změn ovlivňujících instituci by měl být proveden hlubší přezkum.

2 Řídící funkce vedoucího orgánu

28. Vedoucí orgán v řídící funkci by se měl aktivně podílet na podnikání instituce a měl by činit řádná a informovaná rozhodnutí.

29. Vedoucí orgán v řídící funkci by měl nést odpovědnost za provádění strategií stanovených vedoucím orgánem a pravidelně projednávat provádění a vhodnost těchto strategií s vedoucím orgánem v kontrolní funkci. Provozní provádění může zajišťovat vedení instituce.

30. Vedoucí orgán v řídící funkci by měl konstruktivně a kriticky přezkoumávat návrhy, vysvětlení a informace obdržené při posuzování a rozhodování. Vedoucí orgán v řídící funkci by měl podávat komplexní zprávy a informovat pravidelně a v případě potřeby bez zbytečného prodlení vedoucí orgán v kontrolní funkci o aspektech relevantních pro posouzení situace, rizik a vývoje, které instituci ovlivňují nebo mohou ovlivnit, např. o podstatných rozhodnutích týkajících se obchodní činnosti a podstupovaných rizik, hodnocení hospodářského a obchodního prostředí instituce, likvidity a řádné kapitálové základny a posouzení významných expozic vůči riziku.

3 Kontrolní funkce vedoucího orgánu

31. Úloha členů vedoucího orgánu v kontrolní funkci by měla zahrnovat sledování a konstruktivní kritiku strategie instituce.

32. Aniž by bylo dotčeno vnitrostátní právo, vedoucí orgán v kontrolní funkci by měl mít nezávislé členy v souladu s ustanoveními bodu 9.3 společných obecných pokynů ESMA a EBA k posouzení vhodnosti členů vedoucího orgánu a držitelů klíčových funkcí podle směrnice 2013/36/EU a směrnice 2014/65/EU.

33. Aniž by byly dotčeny povinnosti stanovené podle platného vnitrostátního práva obchodních společností, vedoucí orgán v kontrolní funkci by měl:

a. kontrolovat a sledovat rozhodování a opatření vedení a zajišťovat účinný dohled nad vedoucím orgánem v řídící funkci, včetně sledování a kontroly individuálního a kolektivního výkonu a provádění strategie a cílů instituce;

b. konstruktivně připomínkovat a kriticky přezkoumávat návrhy a informace poskytované členy vedoucího orgánu v řídící funkci i jeho rozhodnutí;

c. s ohledem na zásadu proporcionality uvedenou v hlavě I odpovídajícím způsobem plnit povinnosti a úlohu výboru pro rizika, výboru pro odměňování a výboru pro jmenování, jestliže tyto výbory nebyly zřízeny;

d. zajistit a pravidelně posuzovat účinnost vnitřního rámce správy a řízení a přijímat vhodná opatření k řešení případných zjištěných nedostatků;

e. kontrolovat a sledovat, zda jsou důsledně prováděny strategické cíle instituce, organizační struktura a strategie v oblasti rizik, včetně ochoty podstupovat riziko a rámce řízení rizik, ale i další postupy (např. zásady odměňování) a rámec pro zveřejňování informací;

f. sledovat, zda je kultura řízení rizik instituce důsledně prováděna;

g. kontrolovat provádění a udržování kodexu chování nebo obdobných zásad a účinných postupů za účelem identifikace, řízení a zmírňování skutečných a potenciálních střetů zájmů;

h. kontrolovat integritu finančních informací a výkaznictví a rámec vnitřní kontroly, včetně účinného a řádného rámce řízení rizik;

i. zajistit, aby vedoucí funkcí vnitřní kontroly byli schopní jednat nezávisle a bez ohledu na povinnost podávat zprávy jiným vnitřním orgánům, liniím podnikání nebo útvarům mohli v případě potřeby vyjádřit obavy a přímo varovat vedoucí orgán v kontrolní funkci, jestliže nepříznivý vývoj v oblasti rizik ovlivňuje nebo může ovlivnit instituci; a

j. sledovat provádění plánu vnitřního auditu po předchozím zapojení výboru pro rizika a výboru pro audit, jestliže jsou tyto výbory zřízeny.

4 Úloha předsedy vedoucího orgánu

34. Předseda vedoucího orgánu by měl vést vedoucí orgán, měl by přispívat k účinnému toku informací v rámci vedoucího orgánu a mezi vedoucím orgánem a jeho případně zřízenými výbory a měl by nést odpovědnost za jeho celkové účinné fungování.

35. Předseda by měl podporovat a prosazovat otevřenou a kritickou diskusi a zajišťovat možnost vyjádření a projednání nesouhlasných názorů v rámci rozhodovacího procesu.

36. Obecně platí, že by měl mít předseda vedoucího orgánu funkci nevýkonného člena. Je-li povoleno, aby předseda vykonával výkonné povinnosti, instituce by měla zavést opatření omezující případný nepříznivý dopad na kontroly a vyváženost působností v instituci (např. stanovením vedoucího člena rady nebo nezávislého člena rady ve vyšší pozici nebo tím, že je ve vedoucím orgánu v kontrolní funkci větší počet členů zastávajících nevýkonné funkce). Předseda vedoucího orgánu v kontrolní funkci v instituci podle čl. 88 odst. 1 písm. e) směrnice 2013/36/EU zejména nesmí současně vykonávat funkci výkonného ředitele v téže instituci, ledaže k tomu má oprávnění vydané institucí a povolení příslušných orgánů.

37. Předseda by měl stanovovat program jednání a zajišťovat, aby byly prioritně projednávány strategické otázky. Měl by zajistit, aby rozhodnutí vedoucího orgánu byla přijímána řádně a informovaně a aby dokumenty a informace byly obdrženy v dostatečném předstihu před jednáním.

38. Předseda vedoucího orgánu by měl přispívat k jasnému rozdělení povinností členů vedoucího orgánu a k vytvoření účinného toku informací mezi nimi tak, aby členové vedoucího orgánu v kontrolní funkci mohli konstruktivně přispívat do diskusí a řádně a informovaně hlasovat.

5 Výbory vedoucího orgánu v kontrolní funkci

5.1 Zřízení výborů

39. Podle čl. 109 odst. 1 směrnice 2013/36/EU ve spojení s čl. 76 odst. 3, čl. 88 odst. 2 a čl. 95 odst. 1 směrnice 2013/36/EU musí všechny instituce, jež jsou s ohledem na individuální, subkonsolidovanou a konsolidovanou úroveň samy významné, zřídit výbor pro rizika, výbor pro jmenování[9] a výbor pro odměňování[10], které budou vedoucímu orgánu v kontrolní funkci radit a budou připravovat rozhodnutí přijímaná tímto orgánem. Nevýznamné instituce, včetně těch, jež v subkonsolidované nebo konsolidované situaci spadají do rámce obezřetnostní konsolidace instituce, která je významná, nejsou povinny tyto výbory zřídit.

40. Není-li výbor pro rizika nebo odměňování zřízen, odkazy v těchto obecných pokynech na tyto výbory se vykládají tak, že se vztahují k vedoucímu orgánu v kontrolní funkci, a to s přihlédnutím k zásadě proporcionality stanovené v hlavě I.

41. Instituce mohou s přihlédnutím ke kritériím uvedeným v hlavě I těchto obecných pokynů zřídit jiné výbory (např. etický výbor, výbor pro chování a výbor pro dodržování předpisů).

42. Instituce by měly zajistit jasné přidělení a rozdělení povinností a úkolů specializovaných výborů vedoucího orgánu.

[9] Viz rovněž společné pokyny ESMA a EBA k posouzení vhodnosti členů vedoucího orgánu a držitelů klíčových funkcí podle směrnice 2013/36/EU a směrnice 2014/65/EU.

[10] Pokud jde o výbor pro odměňování, odkazujeme na obecné pokyny EBA k řádným zásadám odměňování.

43. Každý výbor by měl mít od vedoucího orgánu v kontrolní funkci dokumentované pověření, včetně oblasti své působnosti, a měl by zavést vhodné pracovní postupy.

44. Výbory by měly podporovat kontrolní funkci v konkrétních oblastech a umožňovat rozvoj a provádění řádného vnitřního rámce správy a řízení. Skutečnost, že výbory byly pověřeny plněním úkolů, nikterak nezbavuje vedoucí orgán v kontrolní funkci kolektivního plnění jeho povinností a odpovědností.

5.2 Složení výborů[11]

45. Všem výborům by měl předsedat člen vedoucího orgánu zastávající nevýkonnou funkci, který je schopen objektivního posuzování.

46. Do výborů by měli být aktivně zapojeni nezávislí členové[12] vedoucího orgánu v kontrolní funkci.

47. Jestliže mají být podle směrnice 2013/36/EU nebo vnitrostátních právních předpisů zřízeny výbory, tyto výbory by měly mít nejméně tři členy.

48. Instituce by měly s přihlédnutím k velikosti vedoucího orgánu a počtu nezávislých členů vedoucího orgánu v kontrolní funkci zajistit, aby se výbory neskládaly ze stejné skupiny členů, která tvoří jiný výbor.

49. Instituce by měly zvážit občasnou rotaci předsedů a členů výborů, a to s přihlédnutím ke konkrétním zkušenostem, znalostem a dovednostem potřebným individuálně nebo kolektivně v těchto výborech.

50. Výbor pro rizika a výbor pro jmenování by se měly skládat z členů vedoucího orgánu v kontrolní funkci v dotyčné instituci, kteří zastávají nevýkonné funkce. Složení výboru pro audit by mělo odpovídat článku 41 směrnice 2006/43/ES[13]. Složení výboru pro odměňování by mělo být v souladu s bodem 2.4.1 obecných pokynů EBA k řádným zásadám odměňování[14].

51. V globálně systémově významných institucích a v jiných systémově významných institucích by měl mít výbor pro jmenování většinu členů, kteří jsou nezávislí, a měl by mu předsedat nezávislý člen. V jiných významných institucích určených příslušnými orgány nebo stanovených vnitrostátními právními předpisy by měl mít výbor pro jmenování dostatečný počet členů, kteří

[11] Tento oddíl by měl být vykládán ve spojení se společnými pokyny ESMA a EBA k posouzení vhodnosti členů vedoucího orgánu a držitelů klíčových funkcí podle směrnice 2013/36/EU a směrnice 2014/65/EU.

[12] Podle definice v bodě 9.3 společných pokynů ESMA a EBA k posouzení vhodnosti členů vedoucího orgánu a držitelů klíčových funkcí podle směrnice 2013/36/EU a směrnice 2014/65/EU.

[13] Směrnice Evropského parlamentu a Rady 2006/43/ES ze dne 17. května 2006 o povinném auditu ročních a konsolidovaných účetních závěrek, o změně směrnic Rady 78/660/EHS a 83/349/EHS a o zrušení směrnice Rady 84/253/EHS (Úř. věst. L 157, 9.6.2006, s. 87), naposledy pozměněná směrnicí Evropského parlamentu a Rady 2014/56/EU ze dne 16. dubna 2014.

[14] Obecné pokyny EBA k řádným zásadám odměňování podle čl. 74 odst. 3 a čl. 75 odst. 2 směrnice 2013/36/EU a k informacím zveřejňovaným podle článku 450 nařízení (EU) č. 575/2013 (EBA/GL/2015/22).

jsou nezávislí; tyto instituce mohou rovněž jako osvědčený postup zvážit existenci nezávislého předsedy výboru pro jmenování.

52. Členové výboru pro jmenování by měli mít individuálně a kolektivně přiměřené znalosti, dovednosti a odbornost, pokud jde o proces výběru a požadavky z hlediska vhodnosti.

53. V globálně systémově významných institucích a v jiných systémově významných institucích by měl mít výbor pro rizika většinu členů, kteří jsou nezávislí. V globálně systémově významných institucích a v jiných systémově významných institucích by měl být předseda výboru pro rizika nezávislým členem. V jiných významných institucích určených příslušnými orgány nebo stanovených vnitrostátními právními předpisy by měl mít výbor pro rizika dostatečný počet členů, kteří jsou nezávislí; a výboru pro rizika by měl, je-li to možné, předsedat nezávislý člen. Ve všech institucích platí, že by předseda výboru pro rizika neměl být předsedou vedoucího orgánu ani předsedou jiného výboru.

54. Členové výboru pro rizika by měli mít individuálně a kolektivně přiměřené znalosti, dovednosti a odbornost, pokud jde o řízení rizik a kontrolní postupy.

5.3 Jednání výborů

55. Výbory by měly podávat pravidelné zprávy vedoucímu orgánu v kontrolní funkci.

56. Výbory by spolu měly navzájem podle potřeby spolupracovat. Aniž by byl dotčen odstavec 48, tato spolupráce může mít formu účasti v různých výborech, takže předseda nebo člen jednoho výboru může být rovněž členem jiného výboru.

57. Členové výborů by měli vést otevřené a kritické diskuse, během kterých se konstruktivním způsobem projednají nesouhlasné názory.

58. Výbory by měly zdokumentovat program jednání výboru a hlavní výsledky a závěry.

59. Výbor pro rizika a výbor pro jmenování by měly alespoň:

    a. mít přístup k veškerým relevantním informacím a údajům nezbytným k výkonu své úlohy, včetně informací a údajů od relevantních podnikových a kontrolních funkcí (např. právní, finanční, lidské zdroje, IT, řízení rizik, zajišťování shody s předpisy, audit atd.);

    b. dostávat pravidelné zprávy, ad hoc informace, sdělení a stanoviska od vedoucích funkcí vnitřní kontroly týkající se aktuálního rizikového profilu instituce, její kultury řízení rizik a omezení rizik i o případném podstatném porušení stanovených předpisů a zásad, k němuž mohlo dojít, spolu s podrobnými informacemi a doporučeními ohledně nápravných opatření, která byla přijata, budou přijata nebo byla navržena s cílem tato porušení vyřešit;

c. pravidelně přezkoumávat obsah, formát a četnost informací o riziku, které jim mají být předkládány, a přijímat rozhodnutí o obsahu, formátu a četnosti takových informací; a

d. v případě potřeby zajistit řádné zapojení funkcí vnitřní kontroly a dalších relevantních funkcí (lidské zdroje, právní, finanční) v jejich příslušné oblasti odbornosti a/nebo si vyžádat externí odborné poradenství.

5.4 Úloha výboru pro rizika

60. Je-li zřízen, výbor pro rizika by měl alespoň:

a. poskytovat vedoucímu orgánu v kontrolní funkci poradenství a podporu týkající se sledování celkové skutečné a budoucí ochoty instituce podstupovat riziko a strategie v oblasti rizik s přihlédnutím ke všem druhům rizik, aby bylo zajištěno, že jsou v souladu s obchodní strategií, cíli, korporátní kulturou a hodnotami instituce;

b. pomáhat vedoucímu orgánu v kontrolní funkci při kontrole provádění strategie instituce v oblasti rizik a souvisejících stanovených omezení;

c. dohlížet na provádění strategií v oblasti řízení kapitálu a likvidity i strategií týkajících se všech ostatních relevantních rizik instituce, jako je riziko tržní, úvěrové, operační (včetně právních rizik a rizik v oblasti informačních technologií) a riziko ztráty dobré pověsti, aby bylo možné posoudit jejich přiměřenost s ohledem na schválenou ochotu podstupovat riziko a strategii v oblasti rizik;

d. poskytovat vedoucímu orgánu v kontrolní funkci doporučení ohledně úpravy strategie v oblasti rizik nezbytné mimo jiné v důsledku změn obchodního modelu instituce, vývoje na trhu nebo doporučení, která učinila funkce řízení rizik;

e. poskytovat poradenství ohledně jmenování externích konzultantů, které se může vedoucí orgán v kontrolní funkci rozhodnout zapojit za účelem poradenství nebo podpory;

f. přezkoumat řadu možných scénářů, včetně zátěžových scénářů, s cílem posoudit reakci rizikového profilu instituce na externí a interní události;

g. dohlížet na soulad veškerých významných finančních produktů a služeb nabízených klientům s obchodním modelem a strategií instituce v oblasti rizik[15]. Výbor pro rizika by měl posuzovat rizika související s nabízenými finančními produkty a službami a přihlížet k souladu mezi cenami přiřazenými takovým produktům a službám a ziskem plynoucím z takových produktů a služeb; a

[15] Viz rovněž obecné pokyny EBA k dohledu a mechanismům pro správu a řízení retailových bankovních produktů, dostupné na adrese http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products.

h. posuzovat doporučení interních nebo externích auditorů a následně sledovat vhodné provádění přijatých opatření.

61. Výbor pro rizika by měl spolupracovat s jinými výbory, jejichž činnost může ovlivnit strategii v oblasti rizik (např. výbor pro audit a výbor pro odměňování), a pravidelně komunikovat s odděleními vnitřní kontroly instituce, zejména pak s oddělením řízení rizik.

62. Je-li zřízen výbor pro rizika, musí přezkoumávat, a to aniž by byly dotčeny úkoly výboru pro odměňování, zda pobídky stanovené v zásadách a postupech odměňování zohledňují rizika, kapitál a likviditu instituce a pravděpodobnost a načasování jejího zisku.

5.5 Úloha výboru pro audit

63. Je-li zřízen, výbor pro audit by podle směrnice 2006/43/ES[16] měl mimo jiné:

a. sledovat účinnost interních systémů instituce pro kontrolu kvality a řízení rizik a případně funkce vnitřního auditu, pokud jde o finanční výkaznictví auditované instituce, aniž by došlo k porušení její nezávislosti;

b. dohlížet na vytvoření účetních pravidel instituce;

c. sledovat proces finančního výkaznictví a předkládat doporučení s cílem zajistit jeho integritu;

d. přezkoumat a sledovat nezávislost statutárních auditorů nebo auditorských firem v souladu s články 22, 22a, 22b, 24a a 24b směrnice 2006/43/EU a s článkem 6 nařízení (EU) č. 537/2014[17] a zejména vhodnost poskytování neauditorských služeb auditované instituci podle článku 5 uvedeného nařízení;

e. sledovat povinný audit roční a konsolidované účetní závěrky, zejména pak jeho provedení, a to s přihlédnutím k případným zjištěním a závěrům příslušného orgánu podle čl. 26 odst. 6 nařízení (EU) č. 537/2014;

f. nést odpovědnost za postup při výběru externích statutárních auditorů nebo auditorských firem a doporučit jejich jmenování, odměňování a odvolání ke schválení kompetentním orgánem instituce (podle článku 16 nařízení (EU) č. 537/2014, s výjimkou případů, kdy je uplatňován čl. 16 odst. 8 nařízení (EU) č. 537/2014);

[16] Směrnice Evropského parlamentu a Rady 2006/43/ES ze dne 17. května 2006 o povinném auditu ročních a konsolidovaných účetních závěrek, o změně směrnic Rady 78/660/EHS a 83/349/EHS a o zrušení směrnice Rady 84/253/EHS (Úř. věst. L 157, 9.6.2006, s. 87), naposledy pozměněná směrnicí Evropského parlamentu a Rady 214/56/EU ze dne 16. dubna 2014.

[17] Nařízení Evropského parlamentu a Rady (EU) č. 537/2014 ze dne 16. dubna 2014 o specifických požadavcích na povinný audit subjektů veřejného zájmu a o zrušení rozhodnutí Komise 2005/909/ES (Úř. věst. L 158, 27.5.2014, s. 77).

g. přezkoumat rozsah auditu a četnost povinného auditu roční nebo konsolidované účetní závěrky;

h. v souladu s čl. 39 odst. 6 písm. a) směrnice 2006/43/EU informovat správní nebo kontrolní orgán auditovaného subjektu o výsledku povinného auditu a vysvětlit, jak povinný audit přispěl k integritě finančních výkazů a jakou úlohu v tomto procesu sehrál výbor pro audit; a

i. dostávat a zohledňovat zprávy auditora.

5.6 Smíšené výbory

64. V souladu s čl. 76 odst. 3 směrnice 2013/36/EU mohou příslušné orgány povolit institucím, které nejsou považovány za významné, aby sloučily výbor pro rizika a případně zřízený výbor pro audit, jak se uvádí v článku 39 směrnice 2006/43/ES.

65. Jsou-li výbor pro rizika a výbor pro jmenování zřízeny v nevýznamných institucích, lze tyto výbory sloučit. Pokud tak učiní, tyto instituce by měly zdokumentovat důvody, proč se rozhodly pro sloučení výborů a jak zvolený přístup naplňuje cíle výborů.

66. Instituce by měly vždy zajišťovat, aby členové smíšených výborů měli individuálně a kolektivně potřebné znalosti, dovednosti a odborné zkušenosti, které jim umožní plně porozumět povinnostem, jež smíšený výbor plní[18].

Hlava III – Rámec správy a řízení

6 Organizační rámec a struktura

6.1 Organizační rámec

67. Vedoucí orgán instituce by měl zajistit vhodnou a transparentní organizační a provozní strukturu pro danou instituci a měl by mít její písemný popis. Struktura by měla podporovat a prokazovat účinné a obezřetné řízení instituce na individuální, subkonsolidované a konsolidované úrovni. Vedoucí orgán by měl zajistit, aby byly funkce vnitřní kontroly nezávislé na liniích podnikání, které kontrolují, včetně toho, že je zajištěno řádné oddělení povinností a tyto funkce mají odpovídající finanční a lidské zdroje i pravomoci umožňující jim účinně vykonávat jejich úlohu. Vymezení podřízenosti a rozdělení povinností v instituci, zejména v případě držitelů klíčových funkcí, by mělo být jasné, dobře definované, ucelené, vymahatelné a řádně zdokumentované. Dokumentace by měla být podle potřeby aktualizována.

[18] Viz rovněž společné pokyny ESMA a EBA k posouzení vhodnosti členů vedoucího orgánu a držitelů klíčových funkcí podle směrnice 2013/36/EU a směrnice 2014/65/EU.

68. Struktura instituce by neměla omezovat schopnost vedoucího orgánu účinně kontrolovat a řídit rizika, jimž instituce nebo skupina čelí, ani schopnost příslušného orgánu vykonávat nad institucí účinný dohled.

69. Vedoucí orgán by měl posoudit, zda a jak podstatné změny struktury skupiny (např. založení nových dceřiných podniků, fúze a akvizice, prodej nebo likvidace částí skupiny či vnější vývoj) ovlivní přiměřenost organizačního rámce instituce. Jsou-li zjištěny nedostatky, vedoucí orgán by měl urychleně provést případné nezbytné úpravy.

6.2 Důkladná znalost vlastní struktury

70. Vedoucí orgán by měl v plné šíři znát a chápat právní, organizační a provozní strukturu instituce a zajistit, aby byla v souladu se schválenou strategií podnikání, strategií v oblasti rizik a ochotou podstupovat riziko.

71. Vedoucí orgán by měl nést odpovědnost za schválení řádných strategií a zásad pro budování nových struktur. Pokud instituce vytváří v rámci své skupiny řadu právních subjektů, jejich počet a zvláště pak jejich vzájemná propojení a transakce by neměly představovat problém pro navrhování vnitřního systému správy a řízení dané instituce a pro účinné řízení rizik a dohled nad riziky skupiny jako celku. Vedoucí orgán by měl s přihlédnutím ke kritériím uvedeným v oddíle 7 zajistit, aby struktura instituce a případné struktury v rámci skupiny byly jasné, účinné a transparentní, a to pro zaměstnance instituce, akcionáře a jiné zúčastněné osoby i pro příslušný orgán.

72. Vedoucí orgán by měl řídit strukturu instituce, její vývoj a omezení a měl by zajistit, aby struktura byla odůvodněná a účinná a nebyla zbytečně nebo nevhodně složitá.

73. Vedoucí orgán konsolidující instituce by měl chápat nejen právní, organizační a provozní strukturu skupiny, ale také účel a činnost různých subjektů skupiny a jejich vzájemné propojení a vztahy mezi nimi. To znamená také porozumět operačním rizikům specifickým pro skupinu, expozicím v rámci skupiny i tomu, jak by mohly být financování skupiny, kapitál, likvidita a rizikový profil dotčeny za obvyklých a za nepříznivých okolností. Vedoucí orgán by měl zajistit, aby byla instituce schopna včas poskytovat informace o typu, charakteristice, organizačním diagramu, vlastnické struktuře a podnikatelských aktivitách každého právního subjektu a aby instituce ve skupině dodržovaly všechny požadavky na oznamování orgánům dohledu na individuálním, subkonsolidovaném a konsolidovaném základě.

74. Vedoucí orgán konsolidující instituce by měl zajistit, aby jednotlivé subjekty ve skupině (včetně samotné konsolidující instituce) dostávaly informace dostatečné k tomu, aby mohly získat jasný obraz o obecných cílech, strategiích a rizikovém profilu skupiny a o tom, jak je dotyčný subjekt ze skupiny začleněn do struktury a provozního působení skupiny. Tyto informace a jejich revize by měly být zdokumentovány a zpřístupněny relevantním dotčeným funkcím, včetně vedoucího orgánu, linií podnikání a funkcí vnitřní kontroly. Členové vedoucího orgánu

konsolidující instituce by měli být s přihlédnutím ke kritériím uvedeným v oddílu 7 obecných pokynů průběžně informováni o rizicích vyplývajících ze struktury skupiny. To zahrnuje:

a. informace o zásadních rizikových faktorech;

b. pravidelné zprávy posuzující celkovou strukturu instituce a hodnotící soulad činnosti jednotlivých subjektů se schválenou strategií celé skupiny; a

c. pravidelné zprávy o tématech, kde je potřeba dodržovat regulační rámec na individuální, subkonsolidované a konsolidované úrovni.

6.3 Složité struktury a nestandardní nebo netransparentní činnosti

75. Instituce by neměly vytvářet složité a potenciálně netransparentní struktury. Instituce by měly při rozhodování zohledňovat výsledky posouzení rizik provedeného ve snaze zjistit, zda by bylo možné tyto struktury využít pro účel, který souvisí s praním peněz nebo jinou finanční trestnou činností a s příslušnými zavedenými kontrolami a právním rámcem[19]. Za tímto účelem by instituce měly zohlednit alespoň:

a. do jaké míry jurisdikce, ve které bude struktura zřízena, účinně splňuje standardy Evropské unie a mezinárodní standardy pro daňovou transparentnost a o boji proti praní peněz a financování terorismu;

b. do jaké míry struktura slouží očividnému hospodářskému a zákonnému účelu;

c. do jaké míry by bylo možné strukturu použít k zatajení totožnosti konečného skutečného vlastníka;

d. do jaké míry požadavek zákazníka vedoucí k možnému zřízení struktury vyvolává obavy;

e. zda může struktura ohrozit řádnou kontrolu prováděnou vedoucím orgánem instituce nebo schopnost instituce řídit související riziko; a

f. zda struktura představuje překážku bránící řádnému dohledu vykonávanému příslušnými orgány.

[19] Pokud jde o podrobnější údaje o posouzení rizika země a rizika souvisejícího s jednotlivými produkty a zákazníky instituce, měl by být učiněn odkaz také na konečnou verzi (až bude vydaná) společných obecných pokynů k rizikovým faktorům: https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence/-/regulatory-activity/consultation-paper.

76. Instituce by v žádném případě neměly vytvářet neprůhledné nebo zbytečné složité struktury, které nemají jasný ekonomický důvod nebo právní účel nebo u nichž se instituce obávají, že lze tyto struktury využít k účelu souvisejícímu s finanční trestnou činností.

77. Při vytváření struktur by měl vedoucí orgán rozumět těmto strukturám a jejich účelu a souvisejícím konkrétním rizikům a zajistit, aby se na vytváření těchto struktur řádně podílely funkce vnitřní kontroly. Tyto struktury by měly být schváleny a udržovány pouze v případě, kdy byl jasně definován a pochopen jejich účel a kdy se vedoucí orgán přesvědčil, že byla zjištěna veškerá významná rizika, včetně rizik ztráty dobré pověsti, že lze veškerá rizika účinně řídit a řádně vykazovat a že byla zajištěna účinná kontrola. Čím složitější a neprůhlednější organizační a provozní struktura a čím větší rizika, tím intenzivnější by měla být kontrola struktury.

78. Instituce by měly dokumentovat svá rozhodnutí a měly by být schopné odůvodnit svá rozhodnutí příslušným orgánům.

79. Vedoucí orgán by měl zajistit přijetí vhodných opatření, aby se vyhnul rizikům souvisejícím s činností v rámci takových struktur nebo aby tato rizika zmírnil. To znamená zajistit, aby:

    a. instituce měla zavedeny odpovídající zásady a postupy a zdokumentované procesy (např. platné limity, požadavky na informace) pro posuzování, dodržování, schvalování takových činností a řízení jejich rizik, a to s přihlédnutím k důsledkům pro organizační a provozní strukturu skupiny, její rizikový profil a riziko ztráty dobré pověsti;

    b. informace týkající se těchto činností a souvisejících rizik byly přístupné konsolidující instituci interním a externím auditorům a aby byly předávány vedoucímu orgánu v kontrolní funkci a příslušnému orgánu, který udělil povolení; a

    c. instituce pravidelně posuzovala potřebu nadále zachovávat tyto struktury.

80. Tyto struktury a činnosti, včetně jejich souladu s právními předpisy a profesními standardy, by měly podrobeny pravidelnému přezkumu vykonávanému vnitřním auditem na základě posouzení rizik.

81. Při provádění nestandardních nebo netransparentních činností pro klienty (např. pomáhají-li klientům zřídit nástroje v zahraničních jurisdikcích, vytvářejí-li složité struktury, financují-li pro ně transakce nebo poskytují-li správcovské služby), které představují podobné problémy z hlediska vnitřního systému správy a řízení a přinášejí významná operační rizika a rizika ztráty dobré pověsti, by instituce měly přijmout stejná opatření v oblasti řízení rizik jako v případě vlastní obchodní činnosti instituce. Instituce by zejména měly analyzovat důvod, proč chce klient určitou strukturu vytvořit.

7 Organizační rámec v kontextu skupiny

82. Podle čl. 109 odst. 2 směrnice 2013/36/EU by měly mateřské a dceřiné podniky, na něž se vztahuje tato směrnice, zajistit, aby jejich systémy, postupy a mechanismy správy a řízení byly konzistentní a řádně integrované na konsolidovaném a subkonsolidovaném základě. Za tímto účelem by mateřské a dceřiné podniky v rámci obezřetnostní konsolidace měly ve svých dceřiných podnicích, na něž se směrnice 2013/36/EU nevztahuje, zavést takové systémy, procesy a mechanismy, které zajišťují spolehlivé systémy správy a řízení na konsolidovaném a subkonsolidovaném základě. Příslušné funkce v rámci konsolidující instituce a jejích dceřiných podnicích by měly podle potřeby spolupracovat a poskytovat si navzájem údaje a informace. Systémy, postupy a mechanismy správy a řízení by měly zajistit, aby konsolidující instituce měla dostatečné údaje a informace a byla schopná posoudit rizikový profil celé skupiny v souladu s ustanoveními v bodě 6.2.

83. Vedoucí orgán dceřiného podniku, na který se vztahuje směrnice 2013/36/EU, by měl přijmout a provádět na individuální úrovni zásady správy a řízení celé skupiny stanovené na konsolidované nebo nekonsolidované úrovni způsobem, který splňuje všechny konkrétní požadavky vyplývající z práva Evropské unie a vnitrostátních právních předpisů.

84. Na konsolidované a subkonsolidované úrovni by konsolidující instituce měla zajistit dodržování zásad správy a řízení celé skupiny všemi institucemi a dalšími subjekty v rámci obezřetnostní konsolidace, včetně jejich dceřiných podniků, na které se samostatně nevztahuje směrnice 2013/36/EU. Při provádění zásad správy a řízení by konsolidující instituce měla zajistit, aby byly zavedeny spolehlivé systémy správy a řízení pro každý dceřiný podnik, a zvážit zvláštní systémy, postupy a mechanismy v případě, že obchodní činnost není organizována v samostatných právních subjektech, ale v matici linií podnikání, které zahrnují více právních subjektů.

85. Konsolidující instituce by měla zohlednit zájmy všech svých dceřiných podniků i to, jak strategie a zásady dlouhodobě přispívají k naplňování zájmu jednotlivých dceřiných podniků a zájmu skupiny jako celku.

86. Mateřské podniky a jejich dceřiné společnosti by měly zajistit, aby instituce a subjekty ve skupině dodržovaly všechny konkrétní požadavky v každé příslušné jurisdikci.

87. Konsolidující instituce by měla zajistit, aby dceřiné podniky zřízené v třetích zemích a zahrnuté do obezřetnostní konsolidace zavedly systémy, postupy a mechanismy správy a řízení, které jsou v souladu se zásadami správy a řízení celé skupiny a splňují požadavky článků 74 až 96 směrnice 2013/36/EU a těchto obecných pokynů, pokud to není v rozporu se zákony dotyčné třetí země.

88. Požadavky v oblasti správy a řízení vyplývající ze směrnice 2013/36/EU a z těchto obecných pokynů se vztahují na instituce bez ohledu na to, zda se případně jedná o dceřiné podniky mateřského podniku v třetí zemi. Je-li dceřiný podnik v EU, který je dceřiným podnikem mateřského podniku v třetí zemi, konsolidující institucí, nezahrnuje obezřetnostní konsolidace úroveň mateřského podniku nacházejícího se v třetí zemi ani další přímé dceřiné podniky

dotyčného mateřského podniku. Konsolidující instituce by měla zajistit, aby její vlastní zásady správy a řízení zohledňovaly zásady správy a řízení mateřského podniku v třetí zemi vztahující se na celou skupinu, pokud to není v rozporu s požadavky stanovenými na základě příslušných právních předpisů EU, včetně směrnice 2013/36/EU a těchto obecných pokynů.

89. Při vytváření zásad a dokumentování systémů správy a řízení by instituce měly zohlednit faktory uvedené v příloze I obecných pokynů. Přestože zásady a dokumentace mohou být obsaženy v samostatných dokumentech, instituce by měly zvážit jejich spojení nebo odkaz na ně v jediném rámcovém dokumentu týkajícím se systému správy a řízení.

8 Zásady pro outsourcing[20]

90. Vedoucí orgán by měl schválit a pravidelně přezkoumávat a aktualizovat zásady instituce pro outsourcing a zajistit včasné provedení odpovídajících změn.

91. Zásady pro outsourcing by měly brát v úvahu dopad outsourcingu na podnikání instituce a na rizika, jimž instituce čelí (například operační rizika, včetně právních rizik a rizik v oblasti informačních technologií; rizika ztráty dobré pověsti; a rizika koncentrace). Zásady by měly zahrnovat režimy pro podávání zpráv a sledování, které by měly být uplatňovány od počátku ujednání o outsourcingu až do jeho konce (včetně vypracování obchodního případu pro outsourcing, uzavření smlouvy o outsourcingu, plnění této smlouvy až do konce její platnosti, plánů pro nepředvídané události a strategií pro ukončení smluvního vztahu). Instituce je i nadále plně odpovědná za všechny externě zajišťované služby a činnosti a za manažerská rozhodnutí, která z nich vyplynou. V souladu s tím by měly zásady pro outsourcing jasně uvádět, že outsourcing nezbavuje instituci jejích regulačních povinností a její odpovědnosti vůči jejím zákazníkům.

92. Zásady by měly uvádět, že ujednání o outsourcingu by neměla narušovat efektivní dohled nad institucí vykonávaný na místě i na dálku a neměla by porušovat žádná dohledová omezení pro služby a činnosti. Zásady by rovněž měly zahrnovat externí zajištění služeb nebo činností v rámci skupiny (tj. služby poskytované samostatným právním subjektem v rámci skupiny dané instituce) a zohledňovat případné zvláštní okolnosti v dané skupině.

93. Zásady by měly vyžadovat, že při výběru důležitých externích poskytovatelů služeb nebo při externím zajišťování činností musí instituce zohlednit, zda má poskytovatel služeb vhodné etické standardy nebo kodex chování.

Hlava IV – Kultura řízení rizik a obchodní chování

9 Kultura řízení rizik

[20] Tyto obecné pokyny se omezují na obecné zásady pro outsourcing, přičemž konkrétní aspekty outsourcingu upravují obecné pokyny CEBS k outsourcingu, které mají být revidovány. Uvedené obecné pokyny jsou k dispozici na adrese https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing.

94. Řádná a důsledná kultura řízení rizik by měla být klíčovým prvkem účinného řízení rizik institucí a měla by umožňovat institucím přijímat řádná a informovaná rozhodnutí.

95. Instituce by měly vypracovat integrovanou kulturu řízení rizik zahrnující celou instituci, a to na základě úplného pochopení a uceleného pojetí rizik, jimž čelí, a způsobu jejich řízení, s ohledem na ochotu instituce podstupovat riziko.

96. Instituce by měly rozvíjet kulturu řízení rizik prostřednictvím zásad, komunikace a odborné přípravy zaměstnanců týkající se činnosti, strategie a rizikového profilu institucí a měly by přizpůsobit komunikaci a odbornou přípravu zaměstnanců s přihlédnutím k povinnostem zaměstnanců, pokud jde o podstupování rizik a jejich řízení.

97. Zaměstnanci by měli být plně seznámeni se svými povinnostmi vztahujícími se k řízení rizik. Řízení rizik by se nemělo omezovat na specialisty na rizika nebo na funkce vnitřní kontroly. Obchodní útvary by měly pod dohledem vedoucího orgánu nést v první řadě odpovědnost za každodenní řízení rizik v souladu se zásadami, postupy a kontrolami instituce a s přihlédnutím k ochotě instituce podstupovat riziko a schopnosti nést riziko.

98. Účinná kultura řízení rizik by měla mimo jiné zahrnovat:

    a. Tón udávaný shora: vedoucí orgán by měl nést odpovědnost za stanovení a šíření základních hodnot a očekávání instituce. Chování jeho členů by mělo vyjadřovat zastávané hodnoty. Vedení instituce, včetně držitelů klíčových funkcí, by se mělo podílet na interním šíření základních hodnot a očekávání ve vztahu k zaměstnancům. Zaměstnanci by měli jednat v souladu se všemi platnými zákony a právními předpisy a v instituci nebo mimo ni ihned upozornit na zjištěné nedodržování předpisů (např. příslušný orgán prostřednictvím postupu oznamování porušení). Vedoucí orgán by měl průběžně podporovat, sledovat a posuzovat kulturu řízení rizik instituce; zvažovat dopad kultury řízení rizik na finanční stabilitu, rizikový profil a spolehlivou správu a řízení instituce; a případně provádět potřebné změny.

    b. Odpovědnost: příslušní zaměstnanci na všech úrovních by měli znát základní hodnoty instituce a rozumět jim a v rozsahu nezbytném pro jejich úlohu by měli být seznámeni s její ochotou podstupovat riziko a schopností nést riziko. Měli by být schopni vykonávat svoji úlohu a uvědomovat si, že ponesou odpovědnost za svoji činnost v souvislosti s rizikovým chováním instituce.

    c. Účinnou komunikaci a kritické zhodnocení: řádná kultura řízení rizik by měla přispívat k vytváření prostředí otevřené komunikace a účinného kritického zhodnocení, ve kterém rozhodovací procesy podporují širokou škálu názorů, umožňují testovat stávající postupy, stimulovat konstruktivní kritický přístup zaměstnanců a podporovat prostředí otevřeného a konstruktivního zapojení v celé organizaci.

d. Pobídky: vhodné pobídky by měly hrát důležitou úlohu při slaďování rizikového chování s rizikovým profilem instituce a jejími dlouhodobými zájmy[21].

10 Firemní hodnoty a kodex chování

99. Vedoucí orgán by měl vypracovat, zavést, dodržovat a prosazovat přísné etické a profesní standardy zohledňující konkrétní potřeby a charakteristiku instituce a měl by zajistit provádění těchto standardů (prostřednictvím kodexu chování nebo obdobného nástroje). Měl by rovněž dohlížet na dodržování těchto standardů zaměstnanci. Vedoucí orgán může případně v instituci přijmout a zavést standardy platné v celé skupině nebo společné standardy vydané sdruženími nebo jinými příslušnými organizacemi.

100. Zavedené standardy by měly usilovat o snížení rizik, jimž je instituce vystavena, zejména pak operačních rizik a rizik ztráty dobré pověsti, které mohou mít značný negativní dopad na ziskovost instituce a udržitelnost prostřednictvím pokut, nákladů na vedení soudních sporů, omezení stanovených příslušnými orgány, jiných finančních a trestních postihů a ztráty hodnoty značky a důvěry spotřebitelů.

101. Vedoucí orgán by měl mít jasné a zdokumentované zásady, pokud jde o způsoby, jakými by tyto standardy měly být naplňovány. Tyto zásady by měly:

a. připomínat čtenářům, že by veškeré činnosti instituce měly být vykonávány v souladu s platnými zákony a s firemními hodnotami instituce;

b. podporovat informovanost o rizicích prostřednictvím důsledné kultury řízení rizik v souladu s oddílem 9 obecných pokynů a vyjadřovat očekávání vedoucího orgánu, že při výkonu činnosti nedojde k překročení stanovené ochoty podstupovat riziko, omezení stanovených institucí a příslušných povinností zaměstnanců;

c. vymezit zásady a poskytnout příklady týkající se přijatelného a nepřijatelného chování, zejména pak v souvislosti s nepravdivým finančním výkaznictvím a porušením povinností, hospodářskou a finanční trestnou činností (včetně podvodu, praní peněz a postupů porušujících antimonopolní předpisy, finančních sankcí, úplatkářství a korupce, manipulace s trhem, zprostředkování nevhodných produktů, nesprávného prodeje a jiných porušení zákonů na ochranu spotřebitelů);

d. vyjasnit, že se kromě dodržování požadavků vyplývajících z právních, regulačních a interních předpisů očekává, že zaměstnanci budou jednat čestně a bezúhonně a budou plnit svoje povinnosti s patřičnou dovedností, péčí a opatrností; a

[21] Viz rovněž obecné pokyny EBA k řádným zásadám odměňování podle čl. 74 odst. 3 a čl. 75 odst. 2 směrnice 2013/36/EU a k informacím zveřejňovaným podle článku 450 nařízení (EU) č. 575/2013 (EBA/GL/2015/22), dostupné na adrese https://www.eba.europa.eu/regulation-and-policy/remuneration.

e. zajistit, aby zaměstnanci byli seznámeni s možnými interními a externími kázeňskými postihy, právními kroky a sankcemi, které mohou následovat v případě porušení povinností a nepřijatelného chování.

102. Instituce by měly sledovat dodržování těchto standardů a zajišťovat, aby o nich zaměstnanci byli informováni, např. prostřednictvím odborné přípravy. Instituce by měly určit funkci odpovědnou za sledování dodržování kodexu chování nebo obdobného nástroje a za vyhodnocení případného porušení kodexu chování nebo obdobného nástroje a měly by stanovit postup pro účely řešení případů nedodržení. Vedoucí orgán by měl být pravidelně informován o výsledcích.

11 Střet zájmů na úrovni instituce

103. Vedoucí orgán by měl nést odpovědnost za stanovení, schválení a kontrolu provádění a udržování účinných zásad pro určení, posouzení, řízení a zmírnění či prevenci skutečných a potenciálních střetů zájmů na úrovni instituce, např. v důsledku různých činností a úloh instituce, různých institucí v rámci obezřetnostní konsolidace nebo různých linií podnikání nebo organizačních útvarů v dané instituci či s ohledem na externí zúčastněné osoby.

104. Instituce by měly v rámci svých organizačních a administrativních opatření přijmout odpovídající opatření s cílem předcházet tomu, aby střety zájmů negativně ovlivňovaly zájmy jejich klientů.

105. Opatření institucí za účelem řízení a případně zmírňování střetu zájmů by měla být zdokumentována a měla by mimo jiné zahrnovat:

a. odpovídající oddělení povinností, např. svěření činností, u nichž dochází ke střetu při zpracování transakcí nebo poskytování služeb, různým osobám nebo svěření odpovědností za dohled a podávání zpráv o činnostech, u nichž dochází ke střetu, různým osobám;

b. vybudování informačních překážek, např. prostřednictvím fyzického oddělení určitých linií podnikání nebo útvarů; a

c. stanovení vhodných postupů pro transakce se spřízněnými stranami, např. požadavku, aby byly transakce prováděny za obvyklých tržních podmínek.

12 Zásady týkající se střetu zájmů pro zaměstnance[22]

106. Vedoucí orgán by měl nést odpovědnost za stanovení, schválení a kontrolu provádění a zachovávání účinných zásad pro určení, posouzení, řízení a zmírnění nebo prevenci skutečných a potenciálních střetů mezi zájmy instituce a soukromými zájmy zaměstnanců, včetně členů vedoucího orgánu, které by mohly negativně ovlivnit plnění jejich povinností

[22] Tento oddíl by měl být vykládán ve spojení se společnými pokyny ESMA a EBA k posouzení vhodnosti členů vedoucího orgánu a držitelů klíčových funkcí podle směrnice 2013/36/EU a směrnice 2014/65/EU.

a odpovědností. Konsolidující instituce by měla zohlednit zájmy v rámci zásad týkajících se střetů zájmů a platných v celé skupině na konsolidovaném či nekonsolidovaném základě.

107. Cílem zásad by mělo být určit střety zájmů zaměstnanců, včetně zájmů nejbližších rodinných příslušníků. Instituce by měly přihlížet k tomu, že střety zájmů mohou vznikat nejen v důsledku současných, ale také dřívějších osobních nebo pracovních vztahů. Dojde-li ke střetu zájmů, instituce by měly posoudit jeho významnost a rozhodnout o vhodných zmírňujících opatřeních a tato vhodná zmírňující opatření zavést.

108. Pokud jde o střety zájmů, které mohou vzniknout v důsledku dřívějších vztahů, instituce by měly stanovit odpovídající časový rámec, za který mají zaměstnanci střety zájmů nahlašovat, jestliže takové vztahy mohou mít i nadále vliv na chování zaměstnanců a na jejich účast na rozhodování.

109. Zásady by měly zahrnovat alespoň následující situace nebo vztahy, kdy může střet zájmů vznikat:

    a. hospodářské zájmy (např. akcie, jiná vlastnická práva a podíly, finanční účasti a jiné hospodářské zájmy týkající se komerčních klientů, práva duševního vlastnictví, úvěry poskytnuté dotyčnou institucí společnosti, kterou vlastní zaměstnanci, členství v orgánu nebo vlastnictví orgánu nebo subjektu se zájmy ve střetu);

    b. osobní nebo pracovní vztahy s vlastníky kvalifikovaných účastí v instituci;

    c. osobní nebo pracovní vztahy se zaměstnanci instituce nebo subjekty zahrnutými do obezřetnostní konsolidace (např. rodinné vztahy);

    d. jiné zaměstnání nebo předchozí zaměstnání v nedávné minulosti (např. během pěti let);

    e. osobní nebo pracovní vztahy s relevantními externími zúčastněnými osobami (např. spojení s důležitými dodavateli, poradenskými firmami nebo jinými poskytovateli služeb); a

    f. politický vliv nebo politické vztahy.

110. Nehledě na výše uvedené by instituce měly přihlížet k tomu, že by skutečnost, že je zaměstnanec akcionářem jakékoliv instituce nebo má soukromé účty či úvěry u určité instituce nebo používá jiné služby určité instituce, neměla vést k situaci, kdy se předpokládá, že u zaměstnanců dochází ke střetu zájmů, jestliže je dodržen odpovídající limit malého rozsahu.

111. Zásady by měly stanovovat postupy pro oznamování a komunikaci s funkcí odpovědnou podle těchto zásad. Zaměstnanci by měli mít povinnost neprodleně interně oznámit jakoukoliv záležitost, která může vést nebo již vedla ke střetu zájmů.

112. Zásady by měly rozlišovat střety zájmů, které trvají a je potřeba je řešit neustále, a střety zájmů, které nastanou neočekávaně v souvislosti s jedinou událostí (např. transakcí, výběrem poskytovatele služeb atd.) a lze je obvykle řešit pomocí jednorázového opatření. Zájem instituce by měl být při rozhodování za všech okolností ústředním prvkem.

113. Zásady by měly stanovovat postupy, opatření, požadavky týkající se dokumentace a odpovědnosti za účelem identifikace a prevence střetů zájmů, posouzení jejich významnosti a přijetí zmírňujících opatření. Tyto postupy, požadavky, odpovědnosti a opatření by měly zahrnovat:

    a. svěření činností nebo transakcí ve střetu různým osobám;

    b. bránění tomu, aby zaměstnanci aktivní i mimo instituci měli v oblasti takových jiných činností nepřiměřený vliv v rámci instituce;

    c. stanovení povinnosti členů vedoucího orgánu zdržet se hlasování v záležitostech, u kterých dochází nebo může dojít ke střetu zájmů u daného člena nebo u kterých může být jiným způsobem narušena objektivita člena nebo jeho schopnost řádně vykonávat povinnosti vůči instituci;

    d. stanovení vhodných postupů pro transakce se spřízněnými stranami (instituce mohou mimo jiné zvážit požadavek, aby byly transakce prováděny za obvyklých tržních podmínek, požadavek, aby se u takových transakcí v plném rozsahu uplatnily všechny relevantní postupy vnitřní kontroly, požadavek vyžádat si závaznou radu od nezávislých členů vedoucího orgánu, požadavek, aby nejdůležitější transakce schválili akcionáři, a omezení expozice vůči takovým transakcím); a

    e. předcházení tomu, aby členové vedoucího orgánu zastávali funkci člena ve vedoucím orgánu v konkurenčních institucích, pokud se nejedná o instituce, které patří do stejného institucionálního systému ochrany podle čl. 113 odst. 7 nařízení (EU) č. 575/2013, úvěrové instituce trvale přidružené k ústřednímu subjektu podle článku 10 nařízení (EU) č. 575/2013 nebo instituce v rámci obezřetnostní konsolidace.

114. Zásady by měly konkrétně upravovat riziko střetu zájmů na úrovni vedoucího orgánu a poskytovat dostatečný návod, jak určit a řídit střety zájmů, které mohou ohrozit schopnost členů vedoucího orgánu přijímat objektivní a nestranná rozhodnutí, jejichž účelem je přispívat k naplnění nejlepších zájmů dotyčné instituce. Instituce by rovněž měly zohlednit, že střet zájmů může mít dopad na nezávislost uvažování členů vedoucího orgánu[23].

115. Skutečné nebo potenciální střety zájmů oznámené odpovědné funkci v dané instituci by měly být řádně posouzeny a řešeny. Je-li zjištěn střet zájmů zaměstnanců, instituce by měla zdokumentovat přijaté rozhodnutí, zejména pak tehdy, když dojde k přijetí střetu zájmů

[23] Viz rovněž společné pokyny ESMA a EBA k posouzení vhodnosti členů vedoucího orgánu a držitelů klíčových funkcí podle směrnice 2013/36/EU a směrnice 2014/65/EU.

a souvisejících rizik, a v případě, že byl střet zájmů přijat, by instituce měla zdokumentovat, jak byl tento střet zájmů uspokojivě zmírněn nebo napraven.

116. Všechny skutečné a potenciální střety zájmů by měly být individuálně nebo kolektivně na úrovni vedoucího orgánu odpovídajícím způsobem zdokumentovány, oznámeny vedoucímu orgánu a projednány vedoucím orgánem, který o nich rozhodne a bude je řádně řešit.

13 Vnitřní postupy pro oznamování problémů

117. Instituce by měly zavést a udržovat vhodné vnitřní zásady a postupy pro oznamování problémů, které mohou pracovníci využívat k tomu, aby prostřednictvím konkrétního, nezávislého a autonomního kanálu oznámili možné nebo skutečné porušení požadavků vyplývajících z regulačních nebo interních předpisů, včetně předpisů uvedených v nařízení (EU) č. 575/2013 a ve vnitrostátních předpisech provádějících směrnici 2013/36/EU, nebo porušení vnitřního systému správy a řízení. Nemělo by být nutné, aby zaměstnanci provádějící oznámení měli důkaz o porušení, měli by si však být dostatečně jistí tím, že existuje dostatečný důvod pro zahájení vyšetřování.

118. Aby se předešlo střetům zájmů, měli by mít zaměstnanci možnost oznamovat taková porušení mimo obvyklé linie podávání zpráv (např. prostřednictvím funkce zajišťování shody s předpisy, funkce vnitřního auditu či nezávislého vnitřního postupu oznamování podezření na protiprávní jednání). Postupy pro oznamování problémů by měly v souladu se směrnicí 95/46/ES zajišťovat ochranu osobních údajů osoby, která porušení oznámila, i fyzické osoby, která se porušení údajně dopustila.

119. Postupy pro oznamování problémů by měly být dostupné všem zaměstnancům instituce.

120. Informace poskytované ze strany zaměstnanců prostřednictvím postupů pro oznamování problémů by měly být případně zpřístupněny vedoucímu orgánu a jiným odpovědným funkcím stanoveným ve vnitřních zásadách pro oznamování problémů. Jestliže to zaměstnanec oznamující porušení vyžaduje, informace by měly být poskytnuty vedoucímu orgánu a jiným odpovědným funkcím v anonymizované podobě. Instituce mohou rovněž stanovit postup oznamování podezření na protiprávní jednání, který umožňuje anonymní předkládání informací.

121. Instituce by měly zajistit, aby osoba oznamující porušení byla řádně chráněna před negativním dopadem, např. odplatou, diskriminací nebo jinými druhy nespravedlivého zacházení. Instituce by měly zajistit, aby se žádná osoba pod kontrolou instituce nepodílela na pronásledování osoby, která oznámila porušení, a měly by učinit odpovídající opatření proti osobám odpovědným za takové případné pronásledování.

122. Instituce by rovněž měly chránit osoby, které jsou předmětem oznámení, před negativními dopady pro případ, že během vyšetřování nebudou zjištěny žádné důkazy, které přijetí opatření proti takové osobě odůvodňují. Jsou-li přijata opatření, instituce by je měla učinit tak,

aby byla dotyčná osoba chráněna před nezamýšlenými negativními dopady, které přesahují cíl přijatého opatření.

123. Vnitřní postupy pro oznamování problémů by měly zejména:

a. být zdokumentovány (např. v příručce pro zaměstnance);

b. poskytovat jasná pravidla, která zajistí, aby informace o osobě, která oznámení učiní, o osobě, která je předmětem oznámení, a o předmětném porušení byly považované za důvěrné v souladu se směrnicí 95/46/ES, pokud podle vnitrostátních právních předpisů není vyžadováno zveřejnění informací v souvislosti s dalším vyšetřováním nebo následným soudním řízením;

c. chránit zaměstnance, kteří oznámí problémy, před pronásledováním za to, že oznámili porušení, které je potřeba oznámit;

d. zajistit, aby potenciální nebo skutečná porušení byla posouzena a předána k vyřešení na vyšší úroveň, a to podle potřeby i relevantnímu příslušnému orgánu nebo donucovacím orgánům;

e. zajistit, je-li to možné, aby zaměstnanci, kteří oznámili potenciální nebo skutečná porušení, obdrželi potvrzení o přijetí informací;

f. zajistit sledování výsledku vyšetřování oznámeného porušení; a

g. zajistit řádnou evidenci.

14 Oznamování porušení příslušným orgánům

124. Příslušné orgány by měly stanovit účinné a spolehlivé mechanismy umožňující zaměstnancům institucí oznamovat příslušným orgánům relevantní potenciální nebo skutečná porušení regulačních požadavků, včetně požadavků plynoucích z nařízení (EU) č. 575/2013 a z vnitrostátních předpisů provádějících směrnici 2013/36/EU. Tyto mechanismy by měly zahrnovat alespoň:

a. konkrétní postupy pro přijímání oznámení o porušení a následných opatření, například oddělení, útvar nebo funkci pro oznamování porušení;

b. odpovídající ochranu podle oddílu 13;

c. v souladu se směrnicí 95/46/ES ochranu osobních údajů fyzické osoby, která porušení oznámila, i fyzické osoby, která se porušení údajně dopustila; a

d. jasné postupy podle ustanovení bodu 123.

125. Aniž by byla dotčena možnost oznamování porušení prostřednictvím mechanismů příslušných orgánů, příslušné orgány mohou vyzvat zaměstnance, aby se nejprve pokusili využít vnitřní postupy svých institucí pro oznamování problémů.

Hlava V – Rámec a mechanismy vnitřní kontroly

15 Rámec vnitřní kontroly

126. Instituce by měly vypracovat a zachovávat kulturu, která podporuje pozitivní přístup k řízení rizik a zajišťování shody s předpisy v rámci instituce, a spolehlivý a komplexní rámec vnitřní kontroly. Na základě tohoto rámce by linie podnikání institucí měly nést odpovědnost za řízení rizik, s nimiž se setkají při výkonu své činnosti, a měly by zavést kontroly, jejichž účelem je zajistit dodržování interních a externích požadavků. Jako součást tohoto rámce by instituce měly mít funkce vnitřní kontroly s odpovídající a dostatečnou pravomocí, váhou a přístupem k vedoucímu orgánu tak, aby mohly plnit svoje poslání, a měly by mít rámec řízení rizik.

127. Rámec vnitřní kontroly dotyčné instituce by měl být individuálně přizpůsoben specifikům její obchodní činnosti, její složitosti a souvisejícím rizikům, s přihlédnutím k situaci v celé skupině. Dotyčné instituce musí zajistit výměnu nezbytných informací tak, aby každý vedoucí orgán, linie podnikání a interní útvar, včetně každé funkce vnitřní kontroly, mohly vykonávat svoje povinnosti. To například znamená nezbytnou výměnu přiměřených informací mezi liniemi podnikání a funkcí zajišťování shody s předpisy na úrovni skupiny a dále mezi vedoucími funkcí vnitřní kontroly na úrovni skupiny a vedoucím orgánem instituce.

128. Rámec vnitřní kontroly by měl zahrnovat celou organizaci, včetně povinností a úkolů vedoucího orgánu, a činnosti všech linií podnikání a interních útvarů, včetně funkcí vnitřní kontroly, externě zajišťovaných činností a distribučních kanálů.

129. Rámec vnitřní kontroly instituce by měl zajišťovat:

a. účinný a efektivní provoz;

b. obezřetné vykonávání činnosti;

c. vhodnou identifikaci, měření a zmírňování rizik;

d. spolehlivost finančních a nefinančních informací vykazovaných interně i externě;

e. řádné administrativní a účetní postupy; a

f. dodržování zákonů, právních předpisů, požadavků dohledu a interních zásad, procesů, pravidel a rozhodnutí instituce.

16 Provádění rámce vnitřní kontroly

130. Vedoucí orgán by měl nést odpovědnost za stanovení a sledování vhodnosti a účinnosti rámce, procesů a mechanismů vnitřní kontroly a za kontrolu všech linií podnikání a interních útvarů, včetně funkcí vnitřní kontroly (například funkcí řízení rizik, zajišťování shody s předpisy a vnitřního auditu). Instituce by měly stanovit, zachovávat a pravidelně aktualizovat odpovídající písemné zásady, mechanismy a postupy vnitřní kontroly, které by měl schválit vedoucí orgán.

131. Instituce by měla mít ve svém rámci vnitřní kontroly jasný, transparentní a zdokumentovaný rozhodovací proces a jasné rozdělení odpovědností a pravomocí, včetně svých linií podnikání, interních útvarů a funkcí vnitřní kontroly.

132. Instituce by o těchto zásadách, mechanismech a postupech měly informovat všechny zaměstnance vždy, když jsou provedeny podstatné změny.

133. Při provádění rámce vnitřní kontroly by instituce měly zavést odpovídající oddělení povinností, např. svěřit činnosti, u kterých dochází ke střetu při zpracování transakcí nebo při poskytování služeb, různým osobám nebo svěřit různým osobám odpovědnosti za dohled a podávání zpráv v souvislosti s činnostmi, u kterých dochází ke střetu, a měly by vytvořit informační překážky, např. fyzickým oddělením určitých útvarů.

134. Funkce vnitřní kontroly by měly ve svých příslušných oblastech působnosti ověřit, zda jsou zásady, mechanismy a postupy stanovené v rámci vnitřní kontroly správně prováděné.

135. Funkce vnitřní kontroly by měly pravidelně předkládat vedoucímu orgánu písemné zprávy o zásadních zjištěných nedostatcích. Tyto zprávy by měly u každého nového zásadního nedostatku uvádět příslušná související rizika, posouzení dopadů, doporučení a nápravná opatření, která mají být učiněna. Vedoucí orgán by měl na základě zjištění funkcí vnitřní kontroly včas a účinně jednat a měl by vyžadovat odpovídající nápravná opatření. Měl by být zaveden formální postup pro následnou kontrolu a monitorování zjištění a nápravných opatření.

17 Rámec řízení rizik

136. Součástí celkového rámce vnitřní kontroly by mělo být zavedení uceleného rámce řízení rizik v celé instituci ze strany institucí, který zahrnuje všechny její linie podnikání a interní útvary, včetně funkcí vnitřní kontroly, a plně uznává ekonomickou podstatu všech expozic vůči rizikům. Rámec řízení rizik by měl instituci umožňovat, aby činila plně informovaná rozhodnutí o podstupování rizik. Rámec řízení rizik by měl zahrnovat rozvahová a podrozvahová rizika i aktuální rizika a budoucí rizika, jimž instituce může být vystavena. Rizika by měla být hodnocena zdola nahoru a shora dolů, v rámci linií podnikání i napříč liniemi podnikání, s použitím důsledné terminologie a kompatibilní metodiky v celé instituci a na konsolidované nebo subkonsolidované úrovni. Do rámce řízení rizik by měla být zahrnuta veškerá relevantní

rizika s příslušným zohledněním finančních i nefinančních rizik, včetně úvěrového rizika, tržního rizika, rizika likvidity, rizika koncentrace, operačního rizika, rizika v oblasti informačních technologií, rizika ztráty dobré pověsti, právního rizika, rizika chování, rizika nedodržení předpisů a strategických rizik.

137. Rámec řízení rizik instituce by měl obsahovat zásady, postupy, omezení rizik a kontroly rizik zajišťující vhodné, včasné a průběžné určení, měření nebo posouzení, sledování, řízení, zmírnění a vykazování rizik na úrovni linie podnikání, na úrovni instituce a na konsolidované nebo subkonsolidované úrovni.

138. Rámec řízení rizik instituce by měl stanovovat konkrétní pokyny k provádění jejích strategií. Stanovené pokyny by měly podle potřeby stanovit a udržovat vnitřní limity v souladu s ochotou instituce podstupovat riziko a úměrně k její řádné činnosti, finanční síle, kapitálové základně a strategickým záměrům. Rizikový profil instituce by měl být udržován v rámci těchto stanovených omezení. Rámec řízení rizik by měl zajistit, aby pro každý případ porušení omezení rizik existoval stanovený postup, pokud jde o předání k vyřešení na vyšší úroveň a jeho vyřešení, spolu s odpovídajícím postupem pro následnou kontrolu a monitorování.

139. Rámec řízení rizik by měl podléhat nezávislému internímu přezkumu, prováděnému například funkcí vnitřního auditu, a měl by být pravidelně přehodnocován podle ochoty instituce podstupovat riziko, a to při zohlednění informací od funkce řízení rizik a případně zřízeného výboru pro rizika. K faktorům, které je třeba zvážit, patří interní a externí vývoj včetně změn rozvahy a příjmů; zvýšení složitosti podnikání instituce, rizikového profilu nebo provozní struktury; geografická expanze; fúze a akvizice; a zavedení nových produktů nebo linií podnikání.

140. Pro účely zjišťování a měření nebo posuzování rizik by instituce měla vypracovat vhodné metody, včetně nástrojů zaměřených na budoucnost a na vývoj v minulosti. Metody by měly umožnit agregování expozic vůči riziku napříč liniemi podnikání a podporovat určování koncentrací rizik. Nástroje by měly zahrnovat posouzení skutečného rizikového profilu podle ochoty instituce podstupovat riziko, ale i určování a posouzení potenciálních a zátěžových expozic vůči riziku v celé řadě předpokládaných nepříznivých situací s ohledem na schopnost instituce nést riziko. Nástroje by měly poskytovat informace o případné změně rizikového profilu, kterou může být potřebné provést. Při vytváření zátěžových scénářů by instituce měly vycházet z vhodných konzervativních předpokladů.

141. Instituce by měly zohlednit, že výsledky kvantitativních metod hodnocení, včetně zátěžových testů, jsou do velké míry závislé na omezeních a předpokladech modelů (včetně závažnosti a doby trvání šoku a souvisejících rizik). Například modely, které vykazují velmi vysokou návratnost ekonomického kapitálu, mohou být výsledkem nedostatků daných modelů (např. vyloučení některých relevantních rizik) a nikoli vynikající strategie nebo skvělého provádění strategie na straně instituce. Určování úrovně podstupovaného rizika by tudíž nemělo vycházet pouze z kvantitativních informací nebo výstupů modelů; mělo by rovněž zahrnovat kvalitativní přístup (včetně odborného posouzení a kritické analýzy). Výslovně by měly být řešeny

příslušné trendy a údaje týkající se makroekonomického prostředí tak, aby byl určen jejich potenciální dopad na expozice a portfolia.

142. Konečná odpovědnost za posouzení rizik spočívá výhradně na instituci, která by v souladu s tím měla hodnotit svá rizika kriticky a neměla by se spoléhat výhradně na externí posouzení. Například by instituce měla ověřovat zakoupený model rizika a kalibrovat jej podle svých vlastních individuálních okolností, aby zajistila přesné a komplexní zachycení a analýzu rizika v příslušném modelu.

143. Instituce by si měly být plně vědomy omezení modelů a metriky a měly by využívat nástroje sloužící nejen ke kvantitativnímu, ale i kvalitativnímu posouzení rizik (včetně odborného posouzení a kritické analýzy).

144. Kromě vlastního posouzení prováděného institucí mohou instituce využívat externí posouzení rizik (včetně externího úvěrového ratingu nebo externě pořízených modelů rizik). Instituce by si měly být plně vědomy skutečného rozsahu takových posouzení a jejich omezení.

145. Měly by být zavedeny mechanismy pravidelného a transparentního podávání zpráv, aby vedoucí orgán, jeho případně zřízený výbor pro rizika a všechny příslušné útvary v instituci dostávaly včasné, přesné, stručné, srozumitelné a smysluplné zprávy a mohly sdílet relevantní informace o určení, měření nebo posuzování, sledování a řízení rizik. Rámec podávání zpráv by měl být dobře vymezen a zdokumentován.

146. Efektivní sdělování informací a povědomí o rizicích a strategii v oblasti rizik má zásadní význam pro celý proces řízení rizik, včetně přezkumu a rozhodovacích procesů, a pomáhá předcházet rozhodnutím, kterými by mohlo být nevědomky zvýšeno riziko. Účinné oznamování rizik zahrnuje řádné interní posuzování a sdělování strategie v oblasti rizik a příslušných údajů o rizicích (např. expozic a klíčových ukazatelů rizika), a to jak horizontálně napříč institucí, tak vertikálně v obou směrech řetězce řízení.

18 Nové produkty a významné změny[24]

147. Instituce by měla mít zavedeny dobře dokumentované zásady schvalování nových produktů, které schválil vedoucí orgán a které se zabývají rozvojem nových trhů, produktů a služeb a významnými změnami trhů, produktů a služeb stávajících i mimořádnými transakcemi. Zásady by měly kromě toho zahrnovat podstatné změny souvisejících procesů (např. nová ujednání o outsourcingu) a systémů (např. procesy týkající se změn v oblasti IT). Zásady schvalování nových produktů by měly zajistit, aby schválené produkty a změny byly v souladu se strategií v oblasti rizik, ochotou instituce podstupovat riziko a příslušnými limity, nebo aby byly provedeny nezbytné revize.

[24] Viz rovněž obecné pokyny EBA k dohledu a mechanismům pro správu a řízení retailových bankovních produktů, dostupné na adrese https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products.

148. Podstatnými změnami nebo mimořádnými transakcemi mohou být fúze a akvizice, včetně potenciálních důsledků provedení nedostatečné hloubkové kontroly (due diligence), která neidentifikuje rizika a závazky vzniklé po provedení fúze; vytváření struktur (např. nových dceřiných podniků nebo jednoúčelových společností); nové produkty; změny systémů nebo rámce řízení rizik či postupů; a změny v organizaci dané instituce.

149. Instituce by měla mít konkrétní postupy pro posuzování dodržování těchto zásad s přihlédnutím k údajům poskytnutým funkcí řízení rizik. Uvedené by mělo v případě nových produktů nebo významných změn stávajících produktů zahrnovat systematické předběžné posouzení a zdokumentované stanovisko funkce zajišťování shody s předpisy.

150. Zásady schvalování nových produktů instituce by měly zahrnovat všechny aspekty, které je třeba zohlednit před rozhodnutím o vstupu na nové trhy, o obchodování s novými produkty, uvedení nové služby na trh nebo o provedení významných změn stávajících produktů nebo služeb. Zásady schvalování nových produktů by také měly obsahovat definice pojmů „nový produkt/trh/podnikání“ a „významné změny“, které by měly být používány v rámci organizace a v rámci interních útvarů, jež se mají podílet na rozhodovacím procesu.

151. Zásady schvalování nových produktů by měly uvádět hlavní otázky, které je třeba před přijetím rozhodnutí řešit. K těm by měly patřit dodržování regulačních předpisů; účetnictví; cenové modely; dopady na rizikový profil, kapitálovou přiměřenost a rentabilitu; dostupnost dostatečných zdrojů v úseku sjednávání, vypořádání a zpracování obchodů; a dostupnost odpovídajících interních nástrojů a odborných zkušeností pro pochopení a sledování souvisejících rizik. Rozhodnutí zahájit novou činnost by mělo jasně uvádět obchodní útvar a jednotlivce odpovědné za tuto činnost. Nová činnost by neměla být prováděna, dokud nebudou k dispozici přiměřené zdroje pro pochopení a řízení souvisejících rizik.

152. Na schvalování nových produktů nebo významných změn stávajících produktů, procesů a systémů by se měly podílet funkce řízení rizik a funkce zajišťování shody s předpisy. Jejich přínos by měl zahrnovat úplné a objektivní posouzení rizik vyplývajících z nových činností podle různých scénářů, jakýchkoli případných nedostatků řízení rizik a rámců vnitřní kontroly v instituci a schopnosti instituce řídit veškerá nová rizika účinně. Funkce řízení rizik by měla mít rovněž jasný přehled o uvádění nových produktů (nebo významných změn stávajících produktů, procesů a systémů) napříč jednotlivými liniemi podnikání a portfolii a měla by mít pravomoc požadovat, aby změny stávajících produktů prošly formálním procesem stanoveným pro schvalování nových produktů.

19 Funkce vnitřní kontroly

153. Funkce vnitřní kontroly by měly zahrnovat funkci řízení rizik (viz oddíl 20), funkci zajišťování shody s předpisy (viz oddíl 21) a funkci vnitřního auditu (viz oddíl 22). Funkce řízení rizik a funkce zajišťování shody s předpisy by měly být předmětem přezkumu, který provádí funkce vnitřního auditu.

154. Provozní úkoly funkcí vnitřní kontroly lze s ohledem na kritéria proporcionality uvedená v hlavě I a se souhlasem vedoucích orgánů dotčených institucí zajišťovat externě prostřednictvím konsolidující instituce nebo jiného subjektu v rámci skupiny i mimo ni. Vedoucí dotyčné funkce vnitřní kontroly a vedoucí orgán nesou i v případě, že jsou provozní úkoly vnitřní kontroly zajišťovány zčásti nebo zcela externě, nadále odpovědnost za tyto činnosti a za zachovávání funkce vnitřní kontroly v dané instituci.

19.1 Vedoucí funkcí vnitřní kontroly

155. Vedoucí funkcí vnitřní kontroly by měli být ustanoveni na vhodné hierarchické úrovni, která vedoucímu kontrolní funkce zajišťuje odpovídající pravomoc a váhu potřebnou k výkonu jeho povinností. Nehledě na celkovou odpovědnost vedoucího orgánu by vedoucí funkcí vnitřní kontroly měli být nezávislí na liniích podnikání nebo útvarech, které kontrolují. Za tímto účelem by vedoucí funkce řízení rizik, zajišťování shody s předpisy a vnitřního auditu měli podávat zprávy a být přímo podřízení vedoucímu orgánu a jejich činnost by měla být posuzována vedoucím orgánem.

156. V případě potřeby by vedoucí funkcí vnitřní kontroly měli mít přístup k vedoucímu orgánu v kontrolní funkci a měli by mít možnost mu přímo oznámit případné problémy a vedoucí orgán v kontrolní funkci podle potřeby varovat, pokud určitý vývoj instituci ovlivňuje nebo může ovlivnit. To by nemělo vedoucím funkcí vnitřní kontroly bránit v tom, aby rovněž podávali zprávy prostřednictvím běžných cest pro podávání zpráv v dané hierarchii.

157. Instituce by měly mít zdokumentované procesy pro přidělení pozice vedoucího funkce vnitřní kontroly a pro jeho odvolání z funkce. Vedoucí funkcí vnitřní kontroly by v žádném případě neměli být odvoláni bez předchozího souhlasu vedoucího orgánu v kontrolní funkci, přičemž vedoucí funkce řízení rizik podle čl. 76 odst. 5 směrnice 2013/36/EU nelze odvolat bez předchozího souhlasu vedoucího orgánu v kontrolní funkci. Ve významných institucích by měly být příslušné orgány neprodleně informovány o schválení a hlavních důvodech odvolání vedoucího funkce vnitřní kontroly.

19.2 Nezávislost funkcí vnitřní kontroly

158. Aby bylo možné funkce vnitřní kontroly považovat za nezávislé, měly by být splněny následující podmínky:

a. její zaměstnanci neplní žádné provozní úkoly spadající do působnosti činností, které mají dané funkce vnitřní kontroly sledovat a kontrolovat;

b. jsou organizačně oddělené od činností, které mají sledovat a kontrolovat;

c. nehledě na celkovou odpovědnost členů vedoucího orgánu za instituci by vedoucí funkce vnitřní kontroly neměl být podřízen osobě, která nese odpovědnost za řízení činností, jež funkce vnitřní kontroly sleduje a kontroluje; a

d. odměňování zaměstnanců funkcí vnitřní kontroly by nemělo být vázáno na provádění činností, které daná funkce vnitřní kontroly sleduje a kontroluje, a neměla by existovat žádná jiná možnost, že toto odměňování naruší objektivitu zaměstnanců kontrolní funkce[25].

19.3 Spojení funkcí vnitřní kontroly

159. S přihlédnutím ke kritériím proporcionality uvedeným v hlavě I lze sloučit funkci řízení rizik a funkci zajišťování shody s předpisy. Funkce vnitřního auditu by neměla být slučována s jinou funkcí vnitřní kontroly.

19.4 Zdroje funkcí vnitřní kontroly

160. Funkce vnitřní kontroly by měly mít dostatečné zdroje. Měly by mít odpovídající počet kvalifikovaných zaměstnanců (na úrovni mateřského podniku i na úrovni dceřiného podniku). Zaměstnanci by si měli průběžně udržovat kvalifikaci a měla by pro ně být podle potřeby zajišťována odborná příprava.

161. Funkce vnitřní kontroly by měly mít k dispozici vhodné informační systémy i podporu a přístup k interním a externím informacím nutným pro plnění jejich povinností. Měly by mít přístup ke všem nezbytným informacím o všech liniích podnikání a relevantních dceřiných podnicích nesoucích rizika, zejména pak o těch, které mohou pro instituce potenciálně vytvářet významná rizika.

20 Funkce řízení rizik

162. Instituce by měly zřídit funkci řízení rizik zahrnující celou instituci. Funkce řízení rizik by měla mít s ohledem na kritéria proporcionality uvedená v hlavě I dostatečnou pravomoc, váhu a zdroje k provádění zásad řízení rizik a rámce řízení rizik podle ustanovení oddílu 17.

163. Funkce řízení rizik by měla mít v případě potřeby přímý přístup k vedoucímu orgánu v kontrolní funkci a k jeho případně zřízeným výborům, a to zejména včetně výboru pro rizika.

164. Funkce řízení rizik by měla mít přístup ke všem liniím podnikání a dalším interním útvarům, které mohou potenciálně představovat riziko, i k relevantním dceřiným a přidruženým podnikům.

165. Zaměstnanci v rámci funkce řízení rizik by měli mít dostatečné znalosti, dovednosti a zkušenosti týkající se metod a postupů řízení rizik, trhů a produktů a měli by mít přístup k pravidelné odborné přípravě.

166. Funkce řízení rizik by měla být nezávislá na liniích podnikání a na útvarech, jejichž rizika kontroluje, ale nemělo by jí být znemožněno s nimi spolupracovat. Vzájemná spolupráce mezi

[25] Viz rovněž obecné pokyny EBA k řádným zásadám odměňování, které jsou dostupné na adrese https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

provozními funkcemi a funkcí řízení rizik by mělo přispět k dosažení cíle všech zaměstnanců instituce, kteří nesou odpovědnost za řízení rizika.

167. Funkce řízení rizik by měla být ústředním organizačním prvkem instituce strukturovaným tak, aby mohla uplatňovat zásady řízení rizik a kontrolovat rámec řízení rizik. Funkce řízení rizik by měla hrát klíčovou úlohu při zajišťování toho, aby instituce měla zavedeny účinné procesy řízení rizik. Funkce řízení rizik by se měla aktivně podílet na veškerých podstatných rozhodnutích o řízení rizik.

168. Významné instituce mohou zvážit zřízení specializovaných funkcí řízení rizik pro každou podstatnou linii podnikání. Měla by však existovat centrální funkce řízení rizik (včetně funkce řízení rizik v konsolidující instituci s působností v celé skupině), která by poskytovala ucelený pohled na všechna rizika v celé instituci a skupině a zajišťovala dodržování strategie v oblasti rizik.

169. Funkce řízení rizik by měla poskytovat relevantní nezávislé informace, analýzy a odborné posouzení týkající se expozic vůči riziku a poradenství ve věci návrhů a rozhodnutí o rizicích přijatých liniemi podnikání nebo interními útvary a měla by informovat vedoucí orgán o tom, zda jsou v souladu s ochotou instituce podstupovat riziko a se strategií instituce v oblasti rizik. Funkce řízení rizik může doporučovat zlepšení rámce řízení rizik a nápravná opatření při porušení zásad a postupů týkajících se řízení rizik a omezení rizik.

20.1 Úloha funkce řízení rizik ve strategii a rozhodnutích v oblasti rizik

170. Funkce řízení rizik by se měla v rané fázi aktivně podílet na vypracování strategie instituce v oblasti rizik a na zajištění toho, aby instituce měla zavedeny účinné postupy řízení rizik. Funkce řízení rizik by měla vedoucímu orgánu poskytovat všechny relevantní informace týkající se rizik, aby mu umožnila stanovit míru ochoty instituce podstupovat riziko. Funkce řízení rizik by měla posuzovat spolehlivost a udržitelnost strategie v oblasti rizik a ochoty podstupovat riziko. Měla by zajistit, aby se ochota podstupovat riziko odpovídajícím způsobem promítla do konkrétních omezení rizik. Funkce řízení rizik by měla rovněž posuzovat strategii obchodních útvarů v oblasti rizik, včetně cílů navrhovaných obchodními útvary, a měla by se podílet na přípravě rozhodnutí vedoucího orgánu o strategiích v oblasti rizik. Cíle by měly být přesvědčivé a v souladu se strategií instituce v oblasti rizik.

171. Zapojení funkce řízení rizik do rozhodovacích procesů by mělo zajistit, aby byly odpovídajícím způsobem zohledňovány aspekty rizik. Odpovědnost za rozhodnutí by však měla zůstat na příslušných obchodních a interních útvarech a v konečném důsledku na vedoucím orgánu.

20.2 Úloha funkce řízení rizik v oblasti podstatných změn

172. V souladu s oddílem 18 by se funkce řízení rizik před přijetím rozhodnutí o podstatných změnách nebo mimořádných transakcích měla podílet na hodnocení dopadu takových změn a mimořádných transakcí na celkovou úroveň rizika instituce a skupiny a před přijetím rozhodnutí by o svých zjištěních měla přímo informovat vedoucí orgán.

173. Funkce řízení rizik by měla vyhodnocovat, jak by mohla zjištěná rizika ovlivnit schopnost instituce nebo skupiny řídit vlastní rizikový profil, likviditu a řádnou kapitálovou základnu za obvyklých a za nepříznivých okolností.

20.3 Úloha funkce řízení rizik při určování, měření, posuzování, řízení, zmírňování, sledování a vykazování rizik

174. Funkce řízení rizik by měla zajistit, aby příslušné útvary v dané instituci určily, posoudily, změřily, sledovaly, řídily a řádně vykazovaly všechna rizika.

175. Funkce řízení rizik by měla zajistit, aby se při určování a posuzování rizik nevycházelo pouze z kvantitativních informací nebo výstupů modelů a aby byly zohledněny také kvalitativní přístupy. Funkce řízení rizik by měla vedoucí orgán průběžně informovat o předpokladech používaných v modelech rizik a při analýze rizik a o potenciálních nedostatcích modelů a analýzy rizik.

176. Funkce řízení rizik by měla zajistit, aby byly přezkoumávány transakce se spřízněnými stranami a aby byla identifikována a přiměřeně posuzována rizika, která tyto transakce pro instituci představují.

177. Funkce řízení rizik by měla zajistit, aby všechna zjištěná rizika byla obchodními útvary účinně sledována.

178. Funkce řízení rizik by měla pravidelně sledovat skutečný rizikový profil instituce a srovnávat jej se strategickými cíli instituce a její ochotou podstupovat riziko tak, aby umožnila vedoucímu orgánu v jeho řídící funkci rozhodování a vedoucímu orgánu v jeho kontrolní funkci provádění kontroly.

179. Funkce řízení rizik by měla analyzovat trendy a rozpoznávat nová či vznikající rizika a zvýšení rizik v důsledku měnících se okolností a podmínek. Měla by také pravidelně přezkoumávat skutečné výsledky v oblasti rizik v porovnání s předchozími odhady (tj. zpětné testování) s cílem posoudit a zlepšit přesnost a účinnost procesu řízení rizik.

180. Funkce řízení rizik by měla vyhodnotit možné způsoby zmírnění rizik. Zprávy podávané vedoucímu orgánu by měly zahrnovat navrhovaná vhodná opatření s cílem zmírnit rizika.

20.4 Úloha funkce řízení rizik v oblasti neschválených expozic

181. Funkce řízení rizik by měla nezávisle posoudit nedodržení ochoty podstupovat riziko nebo omezení rizik (včetně zjištění příčiny a provedení právní a ekonomické analýzy skutečných nákladů uzavření, snížení nebo zajištění expozice v porovnání s potenciálními náklady jejího zachování). Funkce řízení rizik by měla informovat dotčené obchodní útvary a vedoucí orgán a doporučit možná nápravná opatření. Aniž by byla dotčena povinnost funkce řízení rizik podávat zprávy jiným interním funkcím a výborům, podstatná porušení by funkce řízení rizik měla oznámit přímo vedoucímu orgánu v kontrolní funkci.

182. Funkce řízení rizik by měla hrát klíčovou úlohu při zajišťování toho, aby bylo rozhodnutí na základě jejího doporučení přijato na příslušné úrovni, aby je příslušné obchodní útvary dodržovaly a aby bylo odpovídajícím způsobem oznámeno vedoucímu orgánu a případně zřízenému výboru pro rizika.

20.5 Vedoucí funkce řízení rizik

183. Vedoucí funkce řízení rizik by měl nést odpovědnost za poskytování komplexních a srozumitelných informací o rizicích a poradenství, které vedoucímu orgánu umožňují pochopit celkový rizikový profil instituce. Totéž se týká vedoucího funkce řízení rizik mateřské instituce, pokud jde o konsolidovanou situaci.

184. Vedoucí funkce řízení rizik by měl mít dostatečné odborné znalosti, nezávislost a služební postavení, aby mohl kriticky zhodnotit rozhodnutí, jež mají vliv na expozici instituce vůči riziku. Není-li vedoucí funkce řízení rizik členem vedoucího orgánu, významné instituce by měly jmenovat nezávislého vedoucího funkce řízení rizik, který nenese žádnou odpovědnost za jiné funkce a podléhá přímo vedoucímu orgánu. Pokud není s ohledem na zásadu proporcionality uvedenou v hlavě I přiměřené jmenovat osobu, která vykonává pouze úlohu vedoucího funkce řízení rizik, tuto funkci lze spojit s funkcí vedoucího funkce zajišťování shody s předpisy nebo ji může vykonávat jiný člen vrcholného vedení, a to za předpokladu, že mezi spojenými funkcemi neexistuje střet zájmů. Tato osoba by v každém případě měla mít dostatečnou pravomoc, váhu a nezávislost (např. se může jednat o vedoucího právního oddělení).

185. Vedoucí funkce řízení rizik by měl být schopen kriticky zhodnotit rozhodnutí přijatá vedením a vedoucím orgánem instituce a důvody pro vznesené námitky by měly být formálně zdokumentovány. Jestliže chce instituce udělit vedoucímu funkce řízení rizik právo vetovat rozhodnutí (např. úvěrové nebo investiční rozhodnutí nebo stanovení limitu) přijatá na nižších úrovních než na úrovni vedoucího orgánu, měla by vymezit rozsah takového práva veta, postupy pro předání na vyšší úroveň řízení a podání odvolání i to, jak bude zapojen vedoucí orgán.

186. Instituce by měly stanovit posílené postupy pro schvalování rozhodnutí, ke kterým se vedoucí funkce řízení rizik vyjádřil záporně. Vedoucí orgán v kontrolní funkci by měl být schopen o důležitých otázkách týkajících se rizik, včetně vývoje, který není v souladu s ochotou instituce podstupovat riziko a strategií instituce v oblasti rizik, komunikovat přímo s vedoucím funkce řízení rizik.

21 Funkce zajišťování shody s předpisy (compliance)

187. Instituce by měly zřídit trvalou a účinnou funkci zajišťování shody s předpisy (compliance) s cílem řídit riziko nedodržení předpisů a měly by jmenovat osobu odpovědnou za tuto funkci v celé instituci (hlavního manažera pro dodržování předpisů nebo vedoucího oddělení zajišťování shody s předpisy).

188. Není-li s ohledem na zásadu proporcionality uvedenou v hlavě I přiměřené jmenovat osobu, která vykonává pouze úlohu vedoucího funkce zajišťování shody s předpisy, tuto funkci lze spojit s funkcí vedoucího funkce řízení rizik nebo ji může vykonávat jiný člen vrcholného vedení (např. vedoucí právního oddělení), a to za předpokladu, že mezi spojenými funkcemi neexistuje střet zájmů.

189. Funkce zajišťování shody s předpisy, včetně vedoucího funkce zajišťování shody s předpisy, by měla být nezávislá na liniích podnikání a interních útvarech, které kontroluje, a měla by mít dostatečnou pravomoc, váhu a zdroje. S ohledem na kritéria proporcionality uvedená v hlavě I může této funkci poskytovat podporu funkce řízení rizik nebo tato funkce může být spojena s funkcí řízení rizik nebo jinými vhodnými funkcemi, např. právním oddělením nebo oddělením lidských zdrojů.

190. Zaměstnanci v rámci funkce zajišťování shody s předpisy by měli mít dostatečné znalosti, dovednosti a zkušenosti týkající se zajišťování shody s předpisy a relevantních postupů a měli by mít přístup k pravidelné odborné přípravě.

191. Vedoucí orgán v kontrolní funkci by měl dohlížet na provádění řádně zdokumentovaných zásad zajišťování shody s předpisy, s nimiž by měli být seznámeni všichni zaměstnanci. Instituce by měly vytvořit postup pro pravidelné posuzování změn zákonů a předpisů vztahujících se k jejich činnosti.

192. Funkce zajišťování shody s předpisy by měla vedoucímu orgánu poskytovat poradenství ohledně opatření, která je potřeba přijmout k zajištění shody s platnými zákony, pravidly, předpisy a standardy, a měla by posuzovat možný dopad jakýchkoli změn právního nebo regulačního prostředí na činnost instituce a její rámec zajišťování shody s předpisy.

193. Funkce zajišťování shody s předpisy by měla zajistit, aby bylo prostřednictvím strukturovaného a dobře vymezeného programu sledování dodržování předpisů kontrolováno jejich dodržování a aby byly dodržovány zásady zajišťování shody s předpisy. Funkce zajišťování shody s předpisy by měla vedoucímu orgánu podávat zprávy o riziku nedodržení předpisů a o řízení tohoto rizika v dané instituci a měla by v těchto otázkách podle potřeby komunikovat s funkcí řízení rizik. Funkce zajišťování shody s předpisy a funkce řízení rizik by měly při plněních svých úkolů spolupracovat a vzájemně si podle potřeby poskytovat informace. Vedoucí orgán a funkce řízení riziky by měly zjištění funkce zajišťování shody s předpisy zohledňovat v rozhodovacích procesech.

194. V souladu s oddílem 18 těchto obecných postupů by funkce zajišťování shody s předpisy měla v úzké spolupráci s funkcí řízení rizik a s právním oddělením rovněž ověřit, zda jsou nové produkty a nové postupy v souladu se stávajícím právním rámcem a s případnými známými nadcházejícími změnami zákonů, předpisů a požadavků dohledu.

195. Instituce by měly přijmout vhodná opatření proti internímu nebo externímu podvodnému jednání a porušování kázně (např. porušování interních postupů, porušování limitů).

196. Instituce by měly zajistit, aby jejich dceřiné podniky a pobočky učinily opatření s cílem zajistit soulad jejich operací s místními zákony a předpisy. Jestliže místní zákony a předpisy brání uplatnění přísnějších, skupinou zavedených postupů a systémů zajišťování shody s předpisy, zejména jestliže znemožňují zveřejňování a výměnu nezbytných informací mezi subjekty v rámci skupiny, měly by dceřiné podniky a pobočky informovat hlavního manažera pro dodržování předpisů nebo vedoucího útvaru zajišťování shody s předpisy v konsolidující instituci.

22 Funkce vnitřního auditu

197. Instituce by měly s přihlédnutím ke kritériím proporcionality uvedeným v hlavě I vytvořit nezávislou a účinnou funkci vnitřního auditu a měly by jmenovat osobu odpovědnou za tuto funkci v celé instituci. Funkce vnitřního auditu by měla být nezávislá a měla být mít dostatečnou pravomoc, váhu a zdroje. Instituce by měla zejména zajistit, aby kvalifikace zaměstnanců funkce vnitřního auditu a zdroje funkce vnitřního auditu, zejména pak auditorské nástroje a metody analýzy rizik, byly přiměřené velikosti a umístění instituce a povaze, rozsahu a složitosti rizik souvisejících s obchodním modelem instituce, její kulturou řízení rizik a ochotou podstupovat riziko.

198. Funkce vnitřního auditu by měla být nezávislá na auditovaných činnostech. Proto by funkce vnitřního auditu neměla být spojována s žádnými jinými funkcemi.

199. Funkce vnitřního auditu by měla na základě posouzení rizik nezávisle přezkoumávat a poskytovat objektivní záruky ohledně zajištění shody všech činností a útvarů instituce, a to včetně externě zajišťovaných činností, se zásadami a postupy instituce i externími požadavky. Do působnosti funkce vnitřního auditu by měl spadat každý subjekt v rámci dané skupiny.

200. Funkce vnitřního auditu by se neměla podílet na navrhování, výběru, vytváření a provádění konkrétních zásad, mechanismů a postupů v oblasti vnitřní kontroly a omezení rizik. To by však nemělo vedoucímu orgánu v řídící funkci bránit v tom, aby si vyžádal od vnitřního auditu informace o záležitostech týkajících se rizik, vnitřních kontrol a dodržování platných pravidel.

201. Funkce vnitřního auditu by měla posoudit, zda je rámec vnitřní kontroly uvedený v oddílu 15 nejen, účinný, ale i efektivní. Funkce vnitřního auditu by zejména měla posoudit:

a. vhodnost rámce pro správu a řízení instituce;

b. zda stávající zásady a postupy jsou i nadále přiměřené a splňují požadavky vyplývající ze zákonů a regulačních předpisů a jsou v souladu s ochotou instituce podstupovat riziko a se strategií instituce v oblasti rizik;

c. soulad postupů s platnými zákony a předpisy a s rozhodnutími vedoucího orgánu;

d. zda jsou postupy správně a účinně prováděny (např. soulad transakcí s předpisy, míra skutečně vzniklého rizika atd.); a

e. přiměřenost, kvalitu a účinnost prováděných kontrol a zpráv podávaných příslušnými obchodními útvary a funkcemi řízení rizik a zajišťování shody s předpisy.

202. Funkce vnitřního auditu by měla zejména ověřovat integritu procesů zajišťující spolehlivost metod a technik instituce, předpokladů a zdrojů informací používaných v jejích interních modelech (například modelování rizik a účetní opatření). Měla by také hodnotit kvalitu a využívání kvalitativních nástrojů určování a posuzování rizik a opatření přijatých s cílem rizika zmírnit.

203. Funkce vnitřního auditu by měla mít v celé instituci neomezený přístup ke všem záznamům, dokumentům, informacím a budovám instituce. Uvedené by mělo zahrnovat přístup k informačním systémům řízení a k zápisům ze zasedání všech výborů a rozhodovacích orgánů.

204. Funkce vnitřního auditu by měla dodržovat vnitrostátní a mezinárodní profesní standardy. Příkladem zmíněných profesních standardů jsou standardy stanovené Institutem interních auditorů.

205. Činnost vnitřního auditu by měla být prováděna v souladu s plánem auditu a s podrobným programem auditu na základě posouzení rizik.

206. Plán vnitřního auditu by měl být vypracován nejméně jednou ročně na základě cílů kontrol prováděných vnitřním auditem, které byly stanoveny pro daný rok. Plán vnitřního auditu by měl být schválen vedoucím orgánem.

207. Všechna doporučení auditu by měla podléhat formálnímu postupu následné kontroly ze strany příslušných úrovní vedení, aby bylo zajištěno a oznamováno jejich účinné a včasné řešení.

Hlava VI – Řízení kontinuity výkonu činnosti

208. Instituce by měly zavést řádný plán řízení kontinuity výkonu činnosti s cílem zajistit svou schopnost provozovat dále činnost a omezit ztráty v případě vážného přerušení obchodní činnosti.

209. Instituce by měly zřídit zvláštní nezávislou funkci kontinuity výkonu činnosti, např. v rámci funkce řízení rizik[26].

210. Podnikání instituce se opírá o několik kritických zdrojů (např. informační systémy, včetně cloudových služeb, komunikační systémy a budovy). Účelem řízení kontinuity výkonu činnosti je snížit provozní, finanční a právní důsledky, důsledky pro pověst instituce a ostatní podstatné důsledky vyplývající z katastrofické události nebo déle trvajícího přerušení těchto zdrojů a následného narušení běžných provozních postupů instituce. Ostatní opatření v oblasti řízení rizik mohou být určena ke snížení pravděpodobnosti takových incidentů nebo přenesení jejich finančního dopadu (např. prostřednictvím pojištění) na třetí strany.

211. Aby zavedla řádný plán řízení kontinuity výkonu činnosti, měla by instituce pečlivě analyzovat svou expozici vůči závažným narušením provozu a posoudit (kvantitativně a kvalitativně) jejich možný dopad pomocí analýzy interních a/nebo externích dat a scénářů. Tato analýza by měla zahrnout všechny linie podnikání a interní útvary, včetně funkce řízení rizik, a zohlednit jejich vzájemnou závislost. Výsledky analýzy by měly přispět k definování priorit a cílů instituce pro obnovu.

212. Na základě výše uvedené analýzy by instituce měla zavést:

a. pohotovostní plány a plány kontinuity výkonu činnosti pro zajištění toho, aby instituce vhodně reagovala na mimořádné události a byla schopna zachovat své nejdůležitější provozní činnosti, pokud dojde k narušení jejích obvyklých provozních postupů; a

b. plány obnovy kritických zdrojů, aby se instituce v přiměřeném časovém rámci mohla vrátit k běžným provozním postupům. Jakékoli zbytkové riziko potenciálních narušení provozu by mělo být v souladu s ochotou instituce podstupovat riziko.

213. Pohotovostní plány, plány zachování provozu a plány obnovy by měly být dokumentovány a pečlivě prováděny. Dokumentace by měla být k dispozici v liniích podnikání, interních útvarech a ve funkci řízení rizik a měla by být uložena v systémech, které budou fyzicky odděleny a v případě mimořádné události budou okamžitě přístupné. Měla by být zajištěna odpovídající odborná příprava. Plány by měly být pravidelně testovány a aktualizovány. Veškeré problémy nebo selhání, k nimž v testech dojde, by měly být dokumentovány a analyzovány a plány by měly být odpovídajícím způsobem upraveny.

Hlava VII – Transparentnost

214. Strategie, zásady a postupy by měly být sdělovány všem příslušným zaměstnancům v celé instituci. Zaměstnanci instituce by měli chápat a dodržovat zásady a postupy, které se týkají jejich povinností a odpovědností.

[26] Viz rovněž článek 312 nařízení (EU) č. 575/2013.

215. V souladu s tím by měl vedoucí orgán příslušným zaměstnancům poskytovat informace a aktualizace týkající se strategií a zásad instituce, a to jasně a jednotně, alespoň na úrovni nutné k plnění jejich konkrétních povinností. Může tak učinit prostřednictvím písemných pokynů, příruček či jiným způsobem.

216. Jestliže příslušné orgány podle čl. 106 odst. 2 směrnice 2013/36/EU vyžadují, aby mateřské podniky každý rok zveřejňovaly popis jejich právní struktury, správy a řízení a organizační struktury dané skupiny institucí, informace by měly zahrnovat všechny subjekty ve struktuře dané skupiny, jak jsou definovány ve směrnici 2013/34/EU[27], a pro jednotlivé země.

217. Takto zveřejňované informace by měly zahrnovat alespoň:

a. přehled vnitřní organizace institucí a struktury skupiny podle vymezení ve směrnici 2013/34/EU a jejich změny, včetně hlavních hierarchických vztahů a povinností;

b. případné podstatné změny od předchozích zveřejněných informací a datum provedení takové podstatné změny;

c. nové právní, správní a řídící či organizační struktury;

d. informace o struktuře, organizaci a členech vedoucího orgánu, včetně počtu členů a počtu osob, které jsou kvalifikovány jako nezávislé, a údaje o pohlaví a délce funkčního období každého člena vedoucího orgánu;

e. nejdůležitější povinnosti a odpovědnosti vedoucího orgánu;

f. seznam výborů vedoucího orgánu v kontrolní funkci a jejich složení;

g. přehled zásad týkajících se střetu zájmů a vztahujících se na instituce a vedoucí orgán;

h. přehled rámce vnitřní kontroly; a

i. přehled rámce řízení kontinuity výkonu činnosti.

[27] Směrnice Evropského parlamentu a Rady 2013/34/EU ze dne 26. červen 2013 o ročních účetních závěrkách, konsolidovaných účetních závěrkách a souvisejících zprávách některých forem podniků, o změně směrnice Evropského parlamentu a Rady 2006/43/ES a o zrušení směrnic Rady 78/660/EHS a 83/349/EHS (Úř. věst. L 182, 29.6.2013, s. 19).

Příloha I – Faktory zohledňované při vytváření interních zásad správy a řízení

V souladu s hlavou III by instituce při dokumentování vnitřních zásad a systémů správy a řízení měly zohlednit následující faktory:

1. Struktura akcionářů
2. Struktura skupiny, je-li to relevantní (právní a funkční struktura)
3. Složení a fungování vedoucího orgánu
   a) kritéria výběru;
   b) počet, délka funkčního období, rotace, věk;
   c) nezávislí členové vedoucího orgánu;
   d) členové vedoucího orgánu zastávající výkonné funkce;
   e) členové vedoucího orgánu zastávající nevýkonné funkce;
   f) případné vnitřní rozdělení úkolů.
4. Struktura správy a řízení a organizační diagram (s případným dopadem na danou skupinu)
   a) specializované výbory
      i. složení;
      ii. fungování;
   b) případný výkonný výbor
      i. složení;
      ii. fungování.
5. Držitelé klíčových funkcí
   a) vedoucí funkce řízení rizik;
   b) vedoucí funkce zajišťování shody s předpisy;
   c) vedoucí funkce vnitřního auditu;
   d) finanční ředitel (CFO);
   e) ostatní držitelé klíčových funkcí.
6. Rámec vnitřní kontroly
   a) popis každé funkce, včetně její organizace, zdrojů, váhy a pravomocí;
   b) popis rámce řízení rizik, včetně strategie v oblasti rizik.
7. Organizační struktura (s případným dopadem na danou skupinu)
   a) provozní struktura, linie podnikání a rozdělení pravomocí a povinností;

b) outsourcing;

c) nabídka produktů a služeb;

d) geografický rozsah činnosti;

e) zdarma poskytované služby;

f) pobočky;

g) dceřiné podniky, společné podniky atd.;

h) používání extrateritoriálních středisek.

8. Etický kodex a kodex chování (s případným dopadem na danou skupinu)

a) strategické cíle a firemní hodnoty;

b) interní předpisy a pravidla, zásady prevence;

c) zásady týkající se střetu zájmů;

d) oznamování podezření na protiprávní jednání (whistleblowing).

9. Stav vnitřních zásad správy a řízení, s uvedením data

a) vypracování;

b) poslední změny;

c) posledního posouzení;

d) schválení vedoucím orgánem.