

EBA/GL/2017/11

21/03/2018

Smjernice

o internom upravljanju

1. Obveze usklađivanja i izvješćivanja

Status ovih smjernica

1. Ovaj dokument sadrži smjernice izdane na temelju članka 16. Uredbe (EU) br. 1093/2010¹. U skladu s člankom 16. stavkom 3. Uredbe (EU) br. 1093/2010 nadležna tijela i financijske institucije moraju ulagati napore da se usklade s ovim smjernicama.
2. Smjernice iznose EBA-ino stajalište o odgovarajućim nadzornim praksama unutar Europskog sustava financijskog nadzora ili o tome kako bi se pravo Unije trebalo primjenjivati u određenom području. Nadležna tijela određena člankom 4. stavkom 2. Uredbe (EU) br. 1093/2010 na koja se smjernice primjenjuju trebala bi se s njima uskladiti tako da ih na odgovarajući način uključe u svoje prakse (npr. izmjenama svojeg pravnog okvira ili nadzornih postupaka), uključujući i u slučajevima kada su smjernice prvenstveno upućene institucijama.

Zahtjevi za izvješćivanje

3. U skladu s člankom 16. stavkom 3. Uredbe (EU) 1093/2010 nadležna tijela moraju obavijestiti EBA-u o tome jesu li usklađena ili se namjeravaju uskladiti s ovim smjernicama, odnosno o razlozima neusklađenosti do 21/05/2017. U slučaju izostanka takve obavijesti unutar ovog roka EBA će smatrati da nadležna tijela nisu usklađena. Obavijesti se dostavljaju slanjem ispunjenog obrasca koji se nalazi na internetskoj stranici EBA-e na adresu compliance@eba.europa.eu s uputom „EBA/GL/2017/11”. Obavijesti bi trebale slati osobe s odgovarajućom nadležnošću za izvješćivanje o usklađenosti u ime svojih nadležnih tijela. Svaka se promjena statusa usklađenosti također mora prijaviti EBA-i.
4. Obavijesti će biti objavljene na EBA-inoj internetskoj stranici u skladu s člankom 16. stavkom 3.

¹ Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ, (SL L 331, 15.12.2010., str. 12.).

2. Predmet, područje primjene i definicije

Predmet

5. U ovim se smjernicama opisuju sustavi, procesi i mehanizmi internog upravljanja koje kreditne institucije i investicijska društva moraju primijeniti u skladu s člankom 74. stavkom 1. Direktive 2013/36/EU² kako bi osigurali učinkovito i razborito upravljanje institucijom.

Adresati

6. Ove smjernice upućene su nadležnim tijelima kako su definirana u članku 4. stavku 1. točki 40. Uredbe (EU) br. 575/2013³, uključujući Europsku središnju banku u vezi s pitanjima o zadaćama koje su joj dodijeljene Uredbom (EU) br. 1024/2013, i institucijama kako su definirane u članku 4. stavku 1. točki 3. Uredbe (EU) br. 575/2013.

Područje primjene

7. Ove smjernice odnose se na sustave upravljanja institucija, uključujući njihovu organizacijsku strukturu i odgovarajuće linije odgovornosti, postupke za utvrđivanje, upravljanje, praćenje i izvješćivanje o rizicima kojima jesu ili bi mogle biti izložene te okvir unutarnje kontrole.
8. Smjernicama se nastoje obuhvatiti sve postojeće strukture odbora i ne zagovara se ni jedna određena struktura. Smjernicama se ne zadire u opću raspodjelu nadležnosti u skladu s nacionalnim pravom trgovačkih društava. Stoga smjernice treba primjenjivati neovisno o strukturi odbora (monistička i/ili dualistička struktura odbora i/ili druga struktura) koja se upotrebljava diljem država članica. Treba imati na umu da bi upravljačko tijelo, kako je definirano u članku 3. stavku 1. točkama 7. i 8. Direktive 2013/36/EU, moralo imati upravljačke (izvršne) i nadzorne (neizvršne) funkcije⁴.
9. U ovim smjernicama pojmovi „upravljačko tijelo u upravljačkoj funkciji” i „upravljačko tijelo u nadzornoj funkciji” upotrebljavaju se bez upućivanja na neku određenu upravljačku strukturu te bi se trebalo smatrati da se upućivanja na upravljačku (izvršnu) ili nadzornu (neizvršnu) funkciju primjenjuju na tijela ili članove upravljačkog tijela odgovorne za tu funkciju u skladu s nacionalnim pravom. Pri provedbi ovih smjernica nadležna tijela trebaju uzeti u obzir svoje

² Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ, (SL L 176, 27.6.2013., str. 338.).

³ Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1. – 337.).

⁴ Vidjeti i uvodnu izjavu 56. Direktive 2013/36/EU.

nacionalno pravo trgovačkih društava i po potrebi utvrditi na koje se tijelo ili članove upravljačkog tijela te funkcije primjenjuju.

10. U državama članicama u kojima upravljačko tijelo djelomično ili u cijelosti prenese izvršne funkcije osobi ili unutarnjem izvršnom tijelu (npr. glavnom izvršnom direktoru (CEO), upravljačkom timu ili izvršnom odboru) osobe koje na temelju tog prijenosa odgovornosti obavljaju te izvršne funkcije trebaju se smatrati upravljačkom funkcijom upravljačkog tijela. Za potrebe ovih smjernica sva upućivanja na upravljačko tijelo u upravljačkoj funkciji uključuju i članove izvršnog tijela ili glavnog izvršnog direktora, kako su definirani u ovim smjernicama, čak i ako oni nisu predloženi ni imenovani kao službeni članovi jednog upravljačkog tijela ili više njih u skladu s nacionalnim pravom.
11. U državama članicama u kojima dioničari, članovi ili vlasnici institucije izravno izvršavaju određene odgovornosti umjesto upravljačkog tijela institucije trebaju osigurati da su te odgovornosti i povezane odluke u najvećoj mogućoj mjeri u skladu sa smjernicama primjenjivima na upravljačko tijelo.
12. Upotrijebljene definicije glavnog izvršnog direktora, glavnog financijskog direktora (CFO) i nositelja ključnih funkcija vrijede isključivo za ove smjernice i nije im cilj nametnuti imenovanje tih službenika ili stvaranje tih položaja, osim ako je to propisano mjerodavnim pravom EU-a ili nacionalnim pravom.
13. Institucije se trebaju uskladiti, a nadležna tijela trebaju osigurati usklađenost institucija s ovim smjernicama na pojedinačnoj, potkonsolidiranoj i konsolidiranoj osnovi u skladu s razinom primjene utvrđenom člankom 109. Direktive 2013/36/EU.

Definicije

14. Osim ako je drukčije naznačeno, pojmovi upotrijebljeni i utvrđeni u Direktivi 2013/36/EU imaju isto značenje u ovim smjernicama. Osim toga, za potrebe ovih smjernica primjenjuju se sljedeće definicije:

Sklonost preuzimanju rizika	ukupna razina i vrste rizika koje je institucija spremna preuzeti u sklopu svoje sposobnosti podnošenja rizika, u skladu sa svojim poslovnim modelom, kako bi ostvarila svoje strateške ciljeve.
Sposobnost podnošenja rizika	najveća razina rizika koju institucija može preuzeti s obzirom na svoju kapitalnu osnovu, sposobnosti upravljanja rizicima i kontrole te regulatorna ograničenja.
Kultura rizika	norme, stavovi i ponašanja povezani sa svijesti o rizicima, preuzimanjem rizika i upravljanjem rizicima te kontrole na temelju kojih se donose odluke o rizicima. Kultura rizika utječe na odluke rukovodstva i zaposlenika u svakodnevnom poslovanju te na rizike koje preuzimaju.

Institucije	kreditne institucije i investicijska društva kako su definirani u članku 4. stavku 1. točkama 1. i 2. Uredbe (EU) br. 575/2013
Radnici	svi zaposlenici institucije i njezinih društava kćeri unutar opsega njezine konsolidacije, uključujući društva kćeri na koje se ne primjenjuje Direktiva 2013/36/EU, i svi članovi upravljačkog tijela u upravljačkoj funkciji i upravljačkog tijela u nadzornoj funkciji
Glavni izvršni direktor (CEO)	osoba koja je odgovorna za upravljanje cjelokupnim poslovnim aktivnostima institucije i njihovo vođenje
Glavni financijski direktor (CFO)	osoba koja je odgovorna za cjelokupno upravljanje svim sljedećim aktivnostima: upravljanje financijskim sredstvima, financijsko planiranje i financijsko izvješćivanje
Osobe odgovorne za rad kontrolnih funkcija	osobe na najvišoj razini hijerarhije odgovorne za učinkovito upravljanje svakodnevnim aktivnostima neovisnih funkcija upravljanja rizicima, praćenja usklađenosti i unutarnje revizije
Nositelji ključnih funkcija	osobe koje imaju znatan utjecaj nad vođenjem institucije, no koje nisu članovi upravljačkog tijela, kao ni glavni izvršni direktor. Oni uključuju osobe odgovorne za rad kontrolnih funkcija i glavnog financijskog direktora kada oni nisu članovi upravljačkog tijela te ostale nositelje ključnih funkcija kada to odrede institucije pristupom koji se temelji na procjeni rizika. Ostali nositelji ključnih funkcija mogu uključivati voditelje važnih poslovnih linija, podružnica u europskom gospodarskom prostoru / Europskom udruženju za slobodnu trgovinu, društava kćeri u trećim zemljama i drugih unutarnjih funkcija.
Bonitetna konsolidacija	primjena bonitetnih pravila utvrđenih u Direktivi 2013/36/EU i Uredbi (EU) br. 575/2013 na konsolidiranoj ili potkonsolidiranoj osnovi u skladu s dijelom 1. glavom 2. poglavljem 2. Uredbe (EU) br. 575/2013. Bonitetna konsolidacija uključuje sva društva kćeri koja su institucije ili financijske institucije, kako su definirana u članku 4. stavku 3. odnosno 26. Uredbe (EU) br. 575/2013, a može uključivati i društva za pomoćne usluge s poslovnim nastanom unutar ili izvan EU-a, kako su definirana u članku 2. stavku 18. te Uredbe.
Konsolidirajuća institucija	institucija od koje se zahtijeva pridržavanje bonitetnih zahtjeva na temelju konsolidiranog položaja u skladu s dijelom 1. glavom 2. poglavljem 2. Uredbe (EU) br. 575/2013
Značajne institucije	institucije iz članka 131. Direktive 2013/36/EU (globalne sistemski važne institucije (GSV institucije) i ostale sistemski važne institucije (OSV institucije)) i po potrebi druge institucije koje određuje nadležno tijelo ili se određuju prema nacionalnom pravu na

temelju procjene veličine i interne organizacije institucija te vrste, opsega i složenosti njihovih aktivnosti

Uvrštene institucije na koje se primjenjuje Direktiva o kapitalnim zahtjevima (CRD)	institucije čiji su financijski instrumenti uvršteni za trgovanje na uređenom tržištu ili multilateralnoj trgovinskoj platformi, kako je definirana u članku 4. stavcima 21. i 22. Direktive 2014/65/EU, u jednoj državi članici ili više njih ⁵
Dioničar	osoba koja je vlasnik dionica određene institucije ili, ovisno o pravnom obliku institucije, drugi vlasnici ili članovi institucije
Direktorska pozicija	rad na položaju člana upravljačkog tijela institucije ili druge pravne osobe

3. Provedba

Datum primjene

15. Ove smjernice primjenjuju se od 30. lipnja 2018.

Stavljanje izvan snage

16. Smjernice EBA-e o internom upravljanju (GL 44) od 27. rujna 2011. stavljaju se izvan snage od 30. lipnja 2018.

⁵ Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU (SL L 173, 12.6.2014., str. 349.)

4. Smjernice

Glava I. – Razmjernost

17. Načelom razmjernosti, koje je propisano člankom 74. stavkom 2. Direktive 2013/36/EU, nastoji se osigurati dosljednost sustava internog upravljanja s pojedinačnim profilom rizičnosti i poslovnim modelom institucije kako bi se osiguralo učinkovito ispunjenje regulatornih zahtjeva.
18. Institucije trebaju uzeti u obzir svoju veličinu i internu organizaciju te vrstu, opseg i složenost svojih aktivnosti pri razvoju i provedbi sustava internog upravljanja. Značajne institucije trebaju imati naprednije sustave upravljanja, dok i male i manje složene institucije mogu imati jednostavnije upravljačke sustave.
19. Radi primjene načela razmjernosti i osiguranja odgovarajuće provedbe zahtjeva, institucije i nadležna tijela trebaju uzeti u obzir sljedeće kriterije:
 - a. veličinu u smislu ukupne bilance institucije i njezinih društava kćeri unutar opsega bonitetne konsolidacije;
 - b. geografsku prisutnost institucije i opseg poslovanja u svakoj nadležnosti;
 - c. pravni oblik institucije, uključujući je li institucija dio grupe i, ako je to slučaj, procjenu razmjernosti za grupu;
 - d. je li institucija uvrštena na tržište ili ne;
 - e. je li instituciji odobrena uporaba internih modela za mjerenje kapitalnih zahtjeva (npr. pristup zasnovan na internim rejting-sustavima);
 - f. vrstu odobrenih djelatnosti i usluga koje obavlja institucija (npr. vidjeti i Prilog 1. Direktivi 2013/36/EU i Prilog 1. Direktivi 2014/65/EU);
 - g. osnovni poslovni model i strategiju, vrstu i složenost poslovnih aktivnosti te organizacijsku strukturu institucije;
 - h. strategiju upravljanja rizicima, sklonost preuzimanju rizika i stvarni profil rizičnosti institucije, pritom uzimajući u obzir i rezultate procjene kapitala SREP-om i procjene likvidnosti SREP-om;
 - i. vlasničku strukturu i strukturu financiranja institucije;

- j. vrstu klijenata (npr. stanovništvo, trgovačka društva, institucije, mala poduzeća, tijela javne vlasti) i složenost proizvoda ili ugovora;
- k. eksternalizirane aktivnosti i distribucijske kanale te
- l. postojeće sustave informacijske tehnologije (IT), uključujući sustave za osiguranje kontinuiteta i aktivnosti eksternalizacije u predmetnom području.

Glava II. – Uloga i sastav upravljačkog tijela i odbora

1 Uloga i odgovornosti upravljačkog tijela

- 20. U skladu s člankom 88. stavkom 1. Direktive 2013/36/EU upravljačko tijelo mora imati krajnju i potpunu odgovornost za instituciju te definira, nadzire i odgovorno je za provedbu sustava upravljanja u instituciji kojim se osigurava učinkovito i razborito upravljanje institucijom.
- 21. Dužnosti upravljačkog tijela trebaju biti jasno definirane, pri čemu treba razlikovati dužnosti upravljačke (izvršne) funkcije od nadzorne (neizvršne) funkcije. Odgovornosti i dužnosti upravljačkog tijela trebaju se opisati u pisanom dokumentu, a upravljačko tijelo treba ih propisno odobriti.
- 22. Svi članovi upravljačkog tijela trebaju biti u potpunosti upoznati sa strukturom i odgovornostima upravljačkog tijela te podjelom zadaća među različitim funkcijama upravljačkog tijela i njegovih odbora. Kako bi se uspostavio odgovarajući sustav provjere, donošenje odluka ne smije biti u rukama jednog člana ili male podskupine članova. Treba postojati učinkovita interakcija između upravljačkog tijela u nadzornoj funkciji i upravljačkog tijela u upravljačkoj funkciji. Obje funkcije trebaju si međusobno pružiti dostatnu količinu informacija koja će im omogućiti izvršavanje njihovih uloga.
- 23. Odgovornosti upravljačkog tijela trebaju uključivati uspostavu, odobravanje i nadzor provedbe:
 - a. cjelokupne poslovne strategije i ključnih politika institucije unutar primjenjivog pravnog i regulatornog okvira, pritom uzimajući u obzir dugoročne financijske interese i solventnost institucije;
 - b. cjelokupne strategije upravljanja rizicima, uključujući sklonost preuzimanju rizika te okvir i mjere upravljanja rizicima institucije, kako bi se osiguralo da upravljačko tijelo posveti dovoljno vremena pitanjima rizika;
 - c. odgovarajućeg i učinkovitog okvira internog upravljanja i unutarnje kontrole koji uključuje jasnu organizacijsku strukturu te dobro funkcionirajuće, neovisne unutarnje funkcije upravljanja rizicima, praćenja usklađenosti i revizije koje imaju dostatne ovlasti, uporište i resurse za izvršavanje svojih funkcija;

- d. iznosa, vrsti i raspodjele internog kapitala i regulatornog kapitala potrebnih za adekvatno pokrivanje rizika institucije;
- e. ciljeva upravljanja likvidnošću institucije;
- f. politiku primitaka koja je u skladu s načelima primitaka utvrđenima u člancima od 92. do 95. Direktive 2013/36/EU i smjernicama EBA-e o dobrim politikama primitaka na temelju članka 74. stavka 3. i članka 75. stavka 2. Direktive 2013/36/EU⁶;
- g. sustava čiji je cilj osigurati učinkovitu provedbu procjene pojedinačne i zajedničke primjerenosti koju provodi upravljačko tijelo, prikladan sastav i planiranje nasljeđivanja članova upravljačkog tijela te učinkovito izvršavanje funkcija upravljačkog tijela⁷;
- h. postupka odabira i procjene primjerenosti nositelja ključnih funkcija⁸;
- i. sustava čiji je cilj osigurati unutarnje djelovanje svih odbora upravljačkog tijela, ako su osnovani, i u kojem se razrađuju:
 - i. uloga, sastav i zadaće svakog odbora;
 - ii. odgovarajući protok informacija, uključujući dokumentaciju s preporukama i zaključcima, i linije izvješćivanja između svakog odbora i upravljačkog tijela, nadležnih tijela i drugih strana;
- j. kulture rizika u skladu s odjeljkom 9. ovih smjernica u kojima se govori o svijesti institucije o rizicima i njezinom preuzimanju rizika;
- k. korporativne kulture i vrijednosti u skladu s odjeljkom 10. kojima se potiče odgovorno i etičko ponašanje, uključujući kodeks ponašanja ili sličan instrument;
- l. politike upravljanja sukobima interesa na razini institucije u skladu s odjeljkom 11. i politike upravljanja sukobima interesa za radnike u skladu s odjeljkom 12. i
- m. sustava čiji je cilj osigurati integritet računovodstvenog sustava i sustava financijskog izvješćivanja, uključujući financijske i operativne kontrole te usklađenost sa zakonom i mjerodavnim standardima.

24. Upravljačko tijelo mora nadzirati proces objave i priopćavanja (informacija) vanjskim dionicima i nadležnim tijelima.

⁶ Smjernice EBA-e o dobrim politikama primitaka na temelju članka 74. stavka 3. i članka 75. stavka 2. Direktive 2013/36/EU i objava na temelju članka 450. Uredbe (EU) br. 575/2013 (EBA/GL/2015/22)

⁷ Vidjeti i zajedničke smjernice ESMA-e i EBA-e za procjenu primjerenosti članova upravljačkog tijela i nositelja ključnih funkcija na temelju Direktive 2013/36/EU i Direktive 2014/65/EU.

⁸ Vidjeti i zajedničke smjernice ESMA-e i EBA-e za procjenu primjerenosti članova upravljačkog tijela i nositelja ključnih funkcija na temelju Direktive 2013/36/EU i Direktive 2014/65/EU.

25. Sve članove upravljačkog tijela treba obavješćivati o cjelokupnim aktivnostima, financijskoj situaciji i profilu rizičnosti institucije, pritom uzimajući u obzir gospodarsko okruženje, te o donesenim odlukama koje imaju veliki utjecaj na poslovanje institucije.
26. Član upravljačkog tijela može biti odgovoran za kontrolnu funkciju, kako je navedeno u glavi V. odjeljku 19.1, pod uvjetom da član nema nikakvih drugih mandata kojima bi se ugrozile njegove aktivnosti unutarnje kontrole i neovisnost kontrolne funkcije.
27. Upravljačko tijelo treba nadzirati, redovito preispitivati i rješavati sve slabosti utvrđene u provedbi postupaka, strategija i politika povezanih s odgovornostima navedenima u stavcima 23. i 24. Okvir internog upravljanja i njegova provedba trebaju se redovito preispitivati i ažurirati pritom uzimajući u obzir načelo razmjernosti kako je dodatno objašnjeno u glavi I. Podrobnije preispitivanje treba provesti kada se u instituciji dogode značajne promjene.

2 Upravljačka funkcija upravljačkog tijela

28. Upravljačko tijelo u upravljačkoj funkciji treba se aktivno angažirati u poslovanju institucije i donositi odluke na temelju pouzdanih informacija i dobre informiranosti.
29. Upravljačko tijelo u upravljačkoj funkciji treba biti odgovorno za provedbu strategija koje je utvrdilo upravljačko tijelo te treba redovito raspravljati o provedbi i prikladnosti tih strategija s upravljačkim tijelom u nadzornoj funkciji. Rukovodstvo institucije može biti odgovorno za operativnu provedbu.
30. Upravljačko tijelo u upravljačkoj funkciji treba pri donošenju prosudbi i odluka konstruktivno propitivati i kritički analizirati primljene prijedloge, objašnjenja i informacije. Upravljačko tijelo u upravljačkoj funkciji treba, po potrebi bez odgode, sveobuhvatno izvješćivati i redovito obavješćivati upravljačko tijelo u nadzornoj funkciji o bitnim elementima za procjenu stanja, rizika i kretanja koji utječu ili bi mogli utjecati na instituciju, npr. o bitnim odlukama o poslovnim aktivnostima i preuzetim rizicima, ocjeni gospodarskog i poslovnog okruženja institucije, likvidnosti i dobroj kapitalnoj osnovi te o procjeni njezine izloženosti značajnim rizicima.

3 Nadzorna funkcija upravljačkog tijela

31. Uloga članova upravljačkog tijela u nadzornoj funkciji treba uključivati praćenje i konstruktivno propitivanje strategije institucije.
32. Ne dovodeći u pitanje nacionalno pravo, upravljačko tijelo u nadzornoj funkciji treba uključiti neovisne članove kako je predviđeno odjeljkom 9.3 zajedničkih smjernica ESMA-e i EBA-e za procjenu primjerenosti članova upravljačkog tijela i nositelja ključnih funkcija na temelju Direktive 2013/36/EU i Direktive 2014/65/EU.
33. Ne dovodeći u pitanje odgovornosti dodijeljene prema mjerodavnom nacionalnom pravu trgovačkih društava, upravljačko tijelo u nadzornoj funkciji treba:

- a. nadzirati i pratiti donošenje odluka i postupanje rukovodstva te učinkovito nadzirati upravljačko tijelo u upravljačkoj funkciji, uključujući praćenje i temeljitu analizu pojedinačne i zajedničke uspješnosti te provedbu strategije i ciljeva institucije;
- b. konstruktivno propitivati i kritički analizirati prijedloge i informacije koje pružaju članovi upravljačkog tijela u upravljačkoj funkciji te njihove odluke;
- c. uzimajući u obzir načelo razmjernosti kako je utvrđeno u glavi I., propisno ispunjavati dužnosti i uloge odbora za rizike, odbora za primitke i odbora za imenovanja kada ti odbori nisu osnovani;
- d. osigurati i redovito procjenjivati učinkovitost okvira internog upravljanja institucije i poduzimati odgovarajuće mjere za rješavanje svih utvrđenih nedostataka;
- e. nadzirati i pratiti provode li se dosljedno strateški ciljevi, organizacijska struktura i strategija upravljanja rizicima institucije, uključujući njezinu sklonost preuzimanju rizika i okvir upravljanja rizicima, te druge politike (npr. politika primitaka) i okvir objavljivanja;
- f. pratiti provodi li se dosljedno kultura rizika institucije;
- g. nadzirati provedbu i održavanje kodeksa ponašanja ili sličnih i učinkovitih politika za utvrđivanje i smanjenje stvarnih i potencijalnih sukoba interesa te upravljanje njima;
- h. nadzirati cjelovitost financijskih informacija i izvješćivanja te okvira unutarnje kontrole, uključujući učinkovit i dobar okvir upravljanja rizicima;
- i. osigurati da osobe odgovorne za rad kontrolnih funkcija mogu neovisno djelovati te, neovisno o odgovornosti izvješćivanja drugih unutarnjih tijela, poslovnih linija ili jedinica, postavljati pitanja i po potrebi izravno upozoriti upravljačko tijelo u nadzornoj funkciji kada nepovoljna kretanja u području rizika utječu ili mogu utjecati na instituciju i
- j. pratiti provedbu plana unutarnje revizije nakon prethodnog uključivanja odbora za rizike i odbora za reviziju kada su ti odbori osnovani.

4 Uloga predsjednika upravljačkog tijela

- 34. Predsjednik upravljačkog tijela treba voditi upravljačko tijelo, pridonositi djelotvornom protoku informacija u upravljačkom tijelu te između upravljačkog tijela i njegovih odbora, ako postoje, i snositi odgovornost za njegov učinkovit cjelokupan rad.
- 35. Predsjednik treba poticati i promicati otvorenu i kritičnu raspravu te osigurati izražavanje različitih mišljenja i raspravljanje o njima u procesu odlučivanja.

36. Opće je načelo da neizvršni član treba biti predsjednik upravljačkog tijela. Kada se predsjedniku dopusti preuzimanje izvršnih dužnosti, institucija treba imati uspostavljene mjere za smanjenje mogućih nepovoljnih učinaka na sustav provjere institucije (npr. imenovanjem glavnog člana odbora ili višeg neovisnog člana odbora ili povećanjem broja neizvršnih članova u upravljačkom tijelu u nadzornoj funkciji). Točnije, u skladu s člankom 88. stavkom 1. točkom (e) Direktive 2013/36/EU predsjednik upravljačkog tijela u nadzornoj funkciji institucije ne smije istodobno obnašati funkciju glavnog izvršnog direktora u istoj instituciji, osim ako to ne opravda institucija i ne odobre nadležna tijela.
37. Predsjednik treba sastavljati dnevne redove sastanaka i osigurati prioritarno razmatranje strateških pitanja. Treba osigurati da upravljačko tijelo donosi odluke na temelju pouzdanih informacija i dobre informiranosti te da se dokumenti i informacije prime dovoljno rano prije sastanka.
38. Predsjednik upravljačkog tijela treba pridonositi jasnoj raspodjeli dužnosti između članova upravljačkog tijela i održavanju djelotvornog protoka informacija među njima kako bi se članovima upravljačkog tijela u nadzornoj funkciji omogućilo da konstruktivno pridonose raspravama i daju svoj glas na temelju pouzdanih informacija i dobre informiranosti.

5 Odbori upravljačkog tijela u nadzornoj funkciji

5.1 Uspostava odbora

39. U skladu s člankom 109. stavkom 1. Direktive 2013/36/EU zajedno s člankom 76. stavkom 3., člankom 88. stavkom 2. i člankom 95. stavkom 1. Direktive 2013/36/EU sve institucije koje su značajne u pogledu pojedinačne, potkonsolidirane i konsolidirane razine trebaju uspostaviti odbor za rizike, odbor za imenovanja⁹ i odbor za primitke¹⁰ radi savjetovanja upravljačkog tijela u nadzornoj funkciji i pripreme odluka koje će to tijelo donijeti. Institucije koje nisu značajne, i onda kada ulaze u opseg bonitetne konsolidacije institucije koja je značajna u potkonsolidiranom ili konsolidiranom položaju, nemaju obvezu uspostave tih odbora.
40. Ako odbor za rizike ili odbor za imenovanja nije osnovan, a na te se odbore upućuje u ovim smjernicama, treba se smatrati da se ta upućivanja odnose na upravljačko tijelo u nadzornoj funkciji pritom uzimajući u obzir načelo razmjernosti kako je utvrđeno u glavi I.
41. Uzimajući u obzir kriterije utvrđene u glavi I. ovih smjernica, institucije mogu uspostaviti druge odbore (npr. odbor za etiku, odbor za ponašanje i odbor za usklađenost).
42. Institucije trebaju osigurati jasnu raspodjelu i razdiobu dužnosti i zadaća između specijaliziranih odbora upravljačkog tijela.

⁹ Vidjeti i zajedničke smjernice ESMA-e i EBA-e za procjenu primjerenosti članova upravljačkog tijela i nositelja ključnih funkcija na temelju Direktive 2013/36/EU i Direktive 2014/65/EU.

¹⁰ Više informacija o odboru za primitke potražite u smjernicama EBA-e o dobrim praksama primitaka.

43. Za svaki odbor treba dokumentirati mandat, uključujući opseg njegovih odgovornosti, koji mu je dodijelilo upravljačko tijelo u nadzornoj funkciji i uspostaviti odgovarajuće radne postupke.
44. Odbori trebaju pružati potporu nadzornoj funkciji u određenim područjima te olakšati razvoj i provedbu dobrog okvira korporativnog upravljanja. Povjeravanje dužnosti odborima ni na koji način ne oslobađa upravljačko tijelo u nadzornoj funkciji od zajedničkog ispunjavanja njegovih dužnosti i odgovornosti.

5.2 Sastav odbora¹¹

45. Predsjednici odbora trebaju biti neizvršni članovi upravljačkog tijela koji su sposobni donositi objektivne prosudbe.
46. Neovisni članovi¹² upravljačkog tijela u nadzornoj funkciji trebaju aktivno sudjelovati u odborima.
47. Kada su osnovani u skladu s Direktivom 2013/36/EU ili nacionalnim pravom, odbori trebaju imati najmanje tri člana.
48. Uzimajući u obzir veličinu upravljačkog tijela i broj neovisnih članova upravljačkog tijela u nadzornoj funkciji, institucije trebaju osigurati da se odbor ne sastoji od iste skupine članova koja već čini neki drugi odbor.
49. Institucije trebaju razmisliti o povremenoj rotaciji predsjednika i članova odbora pritom uzimajući u obzir specifična iskustva, znanja i vještine koji su na pojedinačnoj ili zajedničkoj razini potrebni u tim odborima.
50. Odbor za rizike i odbor za imenovanja trebaju se sastojati od neizvršnih članova upravljačkog tijela u nadzornoj funkciji predmetne institucije. Sastav odbora za reviziju treba biti u skladu s člankom 41. Direktive 2006/43/EZ¹³. Sastav odbora za primitke treba biti u skladu s odjeljkom 2.4.1 smjernica EBA-e o dobrim politikama primitaka¹⁴.
51. Odbor za imenovanja u globalnim sistemski važnim institucijama i ostalim sistemski važnim institucijama treba se većinski sastojati od neovisnih članova i njime treba predsjedati neovisni član. Odbor za imenovanja u drugim značajnim institucijama, koje su odredila nadležna tijela ili su određene na temelju nacionalnog prava, treba uključivati dovoljan broj neovisnih članova.

¹¹ Ovaj odjeljak treba tumačiti zajedno sa zajedničkim smjernicama ESMA-e i EBA-e za procjenu primjerenosti članova upravljačkog tijela i nositelja ključnih funkcija na temelju Direktive 2013/36/EU i Direktive 2014/65/EU.

¹² Kako je definirano u odjeljku 9.3 zajedničkih smjernica ESMA-e i EBA-e za procjenu primjerenosti članova upravljačkog tijela i nositelja ključnih funkcija na temelju Direktive 2013/36/EU i Direktive 2014/65/EU.

¹³ Direktiva 2006/43/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o zakonskim revizijama godišnjih financijskih izvještaja i konsolidiranih financijskih izvještaja, kojom se mijenjaju direktive Vijeća 78/660/EEZ i 83/349/EEZ i stavlja izvan snage Direktiva Vijeća 84/253/EEZ (SL L 157, 9.6.2006., str. 87.) kako je zadnje izmijenjena Direktivom 2014/56/EU Europskog parlamenta i Vijeća od 16. travnja 2014.

¹⁴ Smjernice EBA-e o dobrim politikama primitaka na temelju članka 74. stavka 3. i članka 75. stavka 2. Direktive 2013/36/EU i objava na temelju članka 450. Uredbe (EU) br. 575/2013 (EBA/GL/2015/22)

Takve institucije mogu razmisliti i o dobroj praksi imenovanja neovisnog predsjednika odbora za imenovanja.

52. Članovi odbora za imenovanja trebaju pojedinačno ili kao cjelina posjedovati odgovarajuće znanje, vještine i stručnost u pogledu postupka odabira i zahtjeva u pogledu primjerenosti.
53. Odbor za rizike u globalnim sistemski važnim institucijama i ostalim sistemski važnim institucijama treba se većinski sastojati od neovisnih članova. Predsjednik odbora za rizike u globalnim sistemski važnim institucijama i ostalim sistemski važnim institucijama treba biti neovisan član. Odbor za rizike u drugim značajnim institucijama, koje su odredila nadležna tijela ili su određene nacionalnim pravom, trebaju uključivati dovoljan broj neovisnih članova, a odborom za rizike treba po mogućnosti predsjedati neovisni član. U svim institucijama predsjednik odbora za rizike ne smije biti predsjednik upravljačkog tijela ni predsjednik nekog drugog odbora.
54. Članovi odbora za rizike trebaju pojedinačno ili kolektivno posjedovati odgovarajuće znanje, vještine i stručnost u pogledu praksi upravljanja rizicima i kontrole.

5.3 Postupci odbora

55. Odbori trebaju redovito izvješćivati upravljačko tijelo u nadzornoj funkciji.
56. Među odborima treba postojati odgovarajuća međusobna interakcija. Ne dovodeći u pitanje stavak 48., ta interakcija može se ostvariti u obliku međuodborskog sudjelovanja u okviru kojeg predsjednik ili član jednog odbora može biti i član nekog drugog odbora.
57. Članovi odbora trebaju sudjelovati u otvorenim i kritičkim raspravama u kojima se konstruktivno razgovara o različitim mišljenjima.
58. Odbori trebaju evidentirati dnevne redove sastanaka odbora te glavne rezultate i zaključke s tih sastanaka.
59. Odbor za rizike i odbor za imenovanja najmanje trebaju:
 - a. imati pristup svim važnim informacijama i podacima potrebnim za izvršavanje svoje uloge, uključujući informacije i podatke relevantnih korporativnih i kontrolnih funkcija (npr. pravni poslovi, financije, ljudski resursi, IT, rizici, usklađenost, revizija itd.);
 - b. od osoba odgovornih za rad kontrolnih funkcija primati redovita izvješća, *ad hoc* informacije, priopćenja i mišljenja o trenutačnom profilu rizičnosti institucije, njezinoj kulturi rizika i ograničenjima rizika te o svim potencijalnim bitnim kršenjima, navodeći detaljne informacije i preporuke o korektivnim mjerama koje su poduzete, koje će se poduzeti ili koje se preporučuju za njihovo ispravljanje;
 - c. redovito preispitivati sadržaj, format i učestalost dostave informacija o rizicima o kojima će ih se izvješćivati te donositi odluke o svemu prethodno navedenome i

- d. po potrebi osigurati odgovarajuće sudjelovanje kontrolnih funkcija i ostalih bitnih funkcija (ljudski resursi, pravni poslovi, financije) u njihovim područjima stručnosti i/ili tražiti savjet vanjskog stručnjaka.

5.4 Uloga odbora za rizike

60. Ako je osnovan, odbor za rizike najmanje treba:

- a. pružati savjete i potporu upravljačkom tijelu u nadzornoj funkciji u pogledu praćenja cjelokupne stvarne i buduće sklonosti preuzimanju rizika i strategije upravljanja rizicima institucije, uzimajući u obzir sve vrste rizika, kako bi se osiguralo da su one u skladu s poslovnom strategijom, ciljevima, korporativnom kulturom i vrijednostima institucije;
- b. pomagati upravljačkom tijelu u nadzornoj funkciji u nadzoru provedbe strategije upravljanja rizicima institucije i odgovarajućih utvrđenih ograničenja;
- c. nadzirati provedbu strategija za upravljanje kapitalom i likvidnošću te za sve druge bitne rizike institucije, kao što su tržišni, kreditni, operativni (uključujući pravne rizike i IT-rizike) i reputacijski rizik, kako bi procijenio njihovu prikladnost u odnosu na odobrenu sklonost preuzimanju rizika i strategiju upravljanja rizicima;
- d. pružati upravljačkom tijelu u nadzornoj funkciji preporuke o potrebnim prilagodbama strategije upravljanja rizicima koje proizlaze iz, među ostalim, izmjena u poslovnom modelu institucije, tržišnih kretanja ili preporuka funkcije upravljanja rizicima;
- e. pružati savjete o imenovanju vanjskih savjetnika koje nadzorna funkcija odluči angažirati za savjetovanje ili potporu;
- f. analizirati niz mogućih scenarija, uključujući stresne scenarije, kako bi procijenio koji će učinak vanjski i unutarnji događaji imati na profil rizičnosti institucije;
- g. nadzirati usklađenost svih bitnih financijskih proizvoda i usluga ponuđenih klijentima te poslovnog modela i strategije upravljanja rizicima institucije¹⁵. Odbor za rizike treba procjenjivati rizike povezane s ponuđenim financijskim proizvodima i uslugama te uzimati u obzir usklađenost cijena tih proizvoda i usluga te dobiti ostvarenih njima i
- h. procjenjivati preporuke unutarnjih ili vanjskih revizora i dalje pratiti ispravnu provedbu poduzetih mjera.

¹⁵ Vidjeti i smjernice EBA-e o sustavima nadzora i upravljanja proizvodima namijenjenim potrošačima <http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products>.

61. Odbor za rizike treba surađivati s drugim odborima čije bi aktivnosti mogle utjecati na strategiju upravljanja rizicima (npr. odbor za reviziju i odbor za primitke) i redovito komunicirati s kontrolnim funkcijama institucije, osobito funkcijom upravljanja rizicima.
62. Ako je osnovan, odbor za rizike treba, ne dovodeći u pitanje zadaće odbora za primitke, provjeriti uzimaju li se u poticajima iz politika i praksi primitaka u obzir rizici, kapital i likvidnost institucije te vjerojatnost i vrijeme isplate zarade.

5.5 Uloga odbora za reviziju

63. U skladu s Direktivom 2006/43/EZ¹⁶, ako je osnovan, odbor za reviziju treba među ostalim:
- a. pratiti učinkovitost sustava unutarnje kontrole kvalitete i upravljanja rizicima institucije i, gdje je primjenjivo, njezine funkcije unutarnje revizije u smislu financijskog izvješćivanja institucije nad kojom se obavlja revizija bez ugrožavanja neovisnosti te funkcije;
 - b. nadzirati donošenje računovodstvenih politika u instituciji;
 - c. pratiti postupak financijskog izvješćivanja i izrađivati preporuke čiji je cilj osiguranje njegove cjelovitosti;
 - d. preispitivati i pratiti neovisnost ovlaštenog revizora ili revizorskih društava u skladu s člancima 22., 22.a, 22.b, 24.a i 24.b Direktive 2006/43/EU i člankom 6. Uredbe (EU) br. 537/2014¹⁷ i osobito prikladnost pružanja nerevizorskih usluga instituciji nad kojom se obavlja revizija u skladu s člankom 5. te Uredbe;
 - e. pratiti zakonsku reviziju godišnjih i konsolidiranih financijskih izvještaja, osobito njezinu provedbu, uzimajući u obzir sve nalaze i zaključke nadležnog tijela u skladu s člankom 26. stavkom 6. Uredbe (EU) br. 537/2014;
 - f. biti odgovoran za postupak odabira vanjskog ovlaštenog revizora (ili više njih) ili revizorskog društva (ili više njih) i preporučiti nadležnom tijelu institucije da odobri njegovo (ili njihovo) imenovanje (u skladu s člankom 16. Uredbe (EU) br. 537/2014 osim kada se primjenjuje članak 16. stavak 8. Uredbe (EU) br. 537/2014), naknadu za rad i razrješenje;
 - g. provjeriti opseg revizije i učestalost zakonske revizije godišnjih ili konsolidiranih financijskih izvještaja;

¹⁶ Direktiva 2006/43/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o zakonskim revizijama godišnjih financijskih izvještaja i konsolidiranih financijskih izvještaja, kojom se mijenjaju direktive Vijeća 78/660/EEZ i 83/349/EEZ i stavlja izvan snage Direktiva Vijeća 84/253/EEZ (SL L 157, 9.6.2006., str. 87.) kako je zadnje izmijenjena Direktivom 2014/56/EU Europskog parlamenta i Vijeća od 16. travnja 2014.

¹⁷ Uredba (EU) br. 537/2014 Europskog parlamenta i Vijeća od 16. travnja 2014. o posebnim zahtjevima u vezi zakonske revizije subjekata od javnog interesa i stavljanju izvan snage Odluke Komisije 2005/909/EZ (SL L 158, 27.5.2014., str. 77.)

- h. u skladu s člankom 39. stavkom 6. točkom (a) Direktive 2006/43/EU obavješćivati administrativno ili nadzorno tijelo subjekta nad kojima se obavlja revizija o ishodima zakonske revizije i objasniti kako je zakonska revizija pridonijela cjelovitosti financijskog izvješćivanja i koju je ulogu odbor za reviziju imao u tom procesu i
- i. primati i razmatrati revizorska izvješća.

5.6 Udruženi odbori

- 64. U skladu s člankom 76. stavkom 3. Direktive 2013/36/EU nadležna tijela mogu dopustiti institucijama koje se ne smatraju značajnima udruživanje odbora za rizike s odborom za reviziju (ako je osnovan) kako je navedeno u članku 39. Direktive 2006/43/EZ.
- 65. Ako su odbor za rizike i odbor za imenovanja osnovani u institucijama koje nisu značajne, oni se mogu udružiti. Ako to učine, te institucije trebaju evidentirati razloge zbog kojih su odlučile udružiti odbore i način na koji se tim pristupom ispunjavaju ciljevi odbora.
- 66. Institucije trebaju u svakom trenutku osigurati da svi članovi udruženih odbora pojedinačno i kao cjelina posjeduju potrebno znanje, vještine i stručnost za potpuno razumijevanje dužnosti koje treba izvršavati udruženi odbor¹⁸.

Glava III. – Okvir upravljanja

6 Organizacijski okvir i struktura

6.1 Organizacijski okvir

- 67. Upravljačko tijelo institucije treba osigurati prikladnu i transparentnu organizacijsku i operativnu strukturu institucije te sastaviti njezin pisani opis. Strukturu se treba promicati i odražavati učinkovitost i razborito upravljanje institucijom na pojedinačnoj, potkonsolidiranoj i konsolidiranoj razini. Upravljačko tijelo treba osigurati neovisnost kontrolnih funkcija u odnosu na poslovne linije koje nadziru, uključujući prikladno razgraničavanje dužnosti, te odgovarajuće financijske i ljudske resurse i ovlasti koji su im potrebni za učinkovito izvršavanje svojih uloga. Linije izvješćivanja i raspodjela odgovornosti, osobito među nositeljima ključnih funkcija, u instituciji trebaju biti jasne, dobro definirane, dosljedne, izvršive i propisno dokumentirane. Dokumentaciju se po potrebi treba ažurirati.
- 68. Struktura institucije ne smije onemogućavati upravljačko tijelo u nadzoru rizika s kojima se institucija ili grupa suočavaju, odnosno u učinkovitom upravljanju njima, kao ni nadležno tijelo u učinkovitom nadzoru institucije.

¹⁸Vidjeti i zajedničke smjernice ESMA-e i EBA-e za procjenu primjerenosti članova upravljačkog tijela i nositelja ključnih funkcija na temelju Direktive 2013/36/EU i Direktive 2014/65/EU.

69. Upravljačko tijelo treba procijeniti utječu li značajne promjene u strukturi grupe (npr. osnivanje novih društava kćeri, spajanja i pripajanja, prodaja ili likvidacija dijelova grupe ili vanjska kretanja) na stabilnost organizacijskog okvira institucije i ako utječu, na koji način. Ako se utvrde slabosti, upravljačko tijelo treba brzo provesti sve potrebne prilagodbe.

6.2 Poznavanje strukture

70. Upravljačko tijelo treba u potpunosti poznavati i razumjeti pravnu, organizacijsku i operativnu strukturu institucije („poznavanje strukture”) i osigurati da je ona u skladu s odobrenom poslovnom strategijom, strategijom upravljanja rizicima i sklonošću preuzimanju rizika.
71. Upravljačko tijelo treba biti odgovorno za odobrenje dobrih strategija i politika za uspostavu novih struktura. Kada institucija osnuje velik broj pravnih osoba unutar svoje grupe, njihov broj i osobito njihove međusobne veze i transakcije među njima ne bi trebale predstavljati izazov u osmišljavanju korporativnog upravljanja i u učinkovitom upravljanju i nadzoru rizika grupe kao cjeline. Upravljačko tijelo treba osigurati jasnoću, djelotvornost i transparentnost strukture institucije i, gdje je primjenjivo, struktura unutar grupe, uzimajući u obzir kriterije navedene u odjeljku 7., u pogledu radnika, dioničara i drugih dionika institucije te nadležnog tijela.
72. Upravljačko tijelo treba usmjeravati strukturu institucije, njezin razvoj i ograničenja te treba osigurati strukturu koja je opravdana i učinkovita te koja nije nepotrebno ili neprimjereno složena.
73. Upravljačko tijelo konsolidirajuće institucije treba razumjeti ne samo pravnu, organizacijsku i operativnu strukturu grupe, nego i svrhu i aktivnosti njezinih različitih subjekata te veze i odnose među njima. To znači i da treba razumjeti operativne rizike specifične za grupu i unutargrupne izloženosti te kako će oni utjecati na financiranje, kapital, likvidnost i profil rizičnosti grupe u normalnim i nepovoljnim okolnostima. Upravljačko tijelo treba instituciji omogućiti pravodobno sastavljanje informacija o grupi u pogledu vrste, značajki, organizacijske sheme, vlasničke strukture i djelatnosti svake pravne osobe te osigurati da institucije unutar grupe ispunjavaju sve nadzorne izvještajne zahtjeve na pojedinačnoj, potkonsolidiranoj i konsolidiranoj osnovi.
74. Upravljačko tijelo konsolidirajuće institucije treba osigurati da različiti subjekti grupe (uključujući samu konsolidirajuću instituciju) prime dovoljno informacija za dobivanje jasne slike o općim ciljevima, strategijama i profilu rizičnosti grupe te načinu na koji je predmetni subjekt grupe uključen u strukturu i operativno funkcioniranje grupe. Te informacije i njihove promjene treba dokumentirati i učiniti dostupnima relevantnim predmetnim funkcijama, uključujući upravljačko tijelo, poslovne linije i kontrolne funkcije. Članovi upravljačkog tijela konsolidirajuće institucije trebaju se redovito informirati o rizicima koji proizlaze iz strukture grupe pritom uzimajući u obzir kriterije navedene u odjeljku 7. ovih smjernica. To uključuje primanje:

- a. informacija o glavnim činiteljima rizika;

- b. redovitih izvješća u kojima se procjenjuje cjelokupna struktura institucije i ocjenjuje usklađenost aktivnosti pojedinačnih subjekata s odobrenom strategijom na razini grupe i
- c. redovitih izvješća o temama za koje je regulatornim okvirom propisana obveza usklađenosti na pojedinačnoj, potkonsolidiranoj i konsolidiranoj razini.

6.3 Složene strukture i nestandardne ili netransparentne aktivnosti

75. Institucije trebaju izbjegavati uspostavu složenih i potencijalno netransparentnih struktura. Pri donošenju odluka institucije trebaju uzeti u obzir rezultate procjene rizika, koja je provedena kako bi se utvrdilo mogu li se te strukture upotrijebiti za svrhu povezanu s pranjem novca ili drugim financijskim kaznenim djelima, i odgovarajuće uspostavljene kontrole i pravni okvir¹⁹. U tu svrhu institucije trebaju uzeti u obzir najmanje sljedeće:
- a. u kojoj mjeri nadležnost u kojoj će se struktura uspostaviti ispunjava standarde EU-a i međunarodne standarde o poreznoj transparentnosti, sprečavanju pranja novca i borbi protiv financiranja terorizma;
 - b. u kojoj mjeri struktura služi jasnoj gospodarskoj i zakonitoj svrsi;
 - c. u kojoj mjeri se struktura može upotrijebiti za skrivanje identiteta krajnjeg stvarnog vlasnika;
 - d. u kojoj mjeri zahtjev klijenta, čija je moguća posljedica uspostava strukture, izaziva zabrinutost;
 - e. bi li struktura mogla onemogućiti upravljačko tijelo institucije u provedbi odgovarajućeg nadzora ili instituciju u upravljanju s time povezanim rizicima i
 - f. je li struktura prepreka učinkovitom nadzoru koji provode nadležna tijela.
76. Institucije u svakom slučaju ne smiju uspostaviti netransparentne ili nepotrebno složene strukture koje nemaju jasan gospodarski temelj ni pravnu svrhu ili ako su institucije zabrinute da bi se te strukture mogle upotrijebiti za svrhu povezanu s financijskim kaznenim djelom.
77. Pri uspostavi tih struktura upravljačko tijelo treba razumjeti sama tijela, njihovu svrhu i posebne rizike povezane s njima te osigurati uključivanje odgovarajućih kontrolnih funkcija. Te strukture trebaju se odobriti i zadržati samo kada je njihova svrha jasno određena i shvaćena

¹⁹ Dodatne pojedinosti o procjeni rizika države i rizika povezanog s pojedinačnim proizvodima i klijentima institucije trebaju potražiti i u konačnim zajedničkim smjernicama o čimbenicima rizika (kada budu objavljene): <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>.

te kada je upravljačko tijelo sigurno da su utvrđeni svi značajni rizici, uključujući reputacijske rizike, da se svim rizicima može upravljati učinkovito i o njima izvješćivati na odgovarajući način te da je zajamčen učinkovit nadzor. Što je organizacijska i operativna struktura složenija i netransparentnija, to su rizici veći, a nadzor te strukture treba biti opsežniji.

78. Institucije trebaju dokumentirati svoje odluke i biti sposobne opravdati svoje odluke nadležnim tijelima.
79. Upravljačko tijelo treba osigurati poduzimanje odgovarajućih radnji za izbjegavanje ili smanjenje rizika povezanih s aktivnostima u tim strukturama. To uključuje osiguranje da:
- a. institucija ima uspostavljene odgovarajuće politike i postupke te dokumentirane procese (npr. primjenjiva ograničenja, obveze informiranja) za razmatranje, osiguranje usklađenosti, odobrenje i upravljanje rizicima tih aktivnosti pritom uzimajući u obzir posljedice za organizacijsku i operativnu strukturu grupe, njezin profil rizičnosti i reputacijski rizik;
 - b. informacije o tim aktivnostima i njihovim rizicima dostupne su konsolidirajućoj instituciji te unutarnjim i vanjskim revizorima i o njima se izvješćuje upravljačko tijelo u nadzornoj funkciji i nadležno tijelo koje je izdalo odobrenje i
 - c. institucije redovito procjenjuju stalnu potrebu za održavanjem tih struktura.
80. Funkcija unutarnje revizije treba redovito preispitivati te strukture i aktivnosti, uključujući njihovu usklađenost sa zakonodavstvom i profesionalnim standardima, primjenom pristupa koji se temelji na procjeni rizika.
81. Institucije trebaju poduzeti iste mjere upravljanja rizicima kao što su one za vlastite poslovne aktivnosti kada provode nestandardne ili netransparentne aktivnosti za klijente (npr. kada pomažu klijentima u uspostavi subjekata u izvanteritorijalnim nadležnostima, kada razvijaju složene strukture, kada financiraju transakcije za njih ili pružaju usluge povjerenika) koje predstavljaju slične izazove u internom upravljanju te stvaraju značajne operativne i reputacijske rizike. Institucije posebno trebaju analizirati razlog zbog kojeg klijent želi uspostaviti određenu strukturu.

7 Organizacijski okvir u kontekstu grupe

82. U skladu s člankom 109. stavkom 2. Direktive 2013/36/EU matična društva i društva kćeri na koje se odnosi ta Direktiva trebaju osigurati dosljednost sustava, procesa i mehanizama upravljanja te njihovu dobru integraciju na konsolidiranoj i potkonsolidiranoj osnovi. U tu svrhu matična društva i društva kćeri koja ulaze u opseg bonitetne konsolidacije trebaju provesti te sustave, procese i mehanizme u svojim društvima kćerima na koje se ne primjenjuje Direktiva 2013/36/EU kako bi se osigurali robusni sustavi upravljanja na konsolidiranoj i potkonsolidiranoj osnovi. Nadležne funkcije u konsolidirajućoj instituciji i njezinim društvima kćerima trebaju međusobno komunicirati i po potrebi razmjenjivati podatke i informacije.

Sustavima, procesima i mehanizmima upravljanja treba se osigurati dovoljna količina podataka i informacija za konsolidirajuću instituciju te njezina sposobnost procjene profila rizičnosti na razini grupe kako je opisano u odjeljku 6.2.

83. Upravljačko tijelo društva kćeri na koje se primjenjuje Direktiva 2013/36/EU treba donijeti i na pojedinačnoj razini provesti grupne politike upravljanja uspostavljene na konsolidiranoj i potkonsolidiranoj razini na način kojim se ispunjavaju svi posebni zahtjevi iz prava EU-a i nacionalnog prava.
84. Na konsolidiranoj i potkonsolidiranoj razini konsolidirajuća institucija treba osigurati da se sve institucije i drugi subjekti u opsegu bonitetne konsolidacije, uključujući njihova društva kćeri na koja se ne primjenjuje Direktiva 2013/36/EU, pridržavaju grupnih politika upravljanja. Pri provedbi politika upravljanja konsolidirajuća institucija treba osigurati da su uspostavljeni robusni sustavi upravljanja za svako društvo kći i uzeti u obzir posebne sustave, procese i mehanizme kada su poslovne aktivnosti organizirane u matricu poslovnih linija koja obuhvaća veći broj pravnih osoba umjesto u zasebne pravne osobe.
85. Konsolidirajuća institucija treba uzeti u obzir interese svih svojih društava kćeri te način na koji strategije i politike dugoročno pridonose interesu svakog društva kćeri i interesu grupe kao cjeline.
86. Matična društva i njihova društva kćeri trebaju osigurati da institucije i subjekti unutar grupe ispunjavaju sve posebne zahtjeve iz svih relevantnih nadležnosti.
87. Konsolidirajuća institucija treba osigurati da društva kćeri osnovana u trećim zemljama i uključena u opseg bonitetne konsolidacije imaju uspostavljene sustave, procese i mehanizme upravljanja koji su dosljedni s grupnim politikama upravljanja i usklađeni sa zahtjevima iz članaka od 74. do 96. Direktive 2013/36/EU i ovim smjernicama sve dok to nije u suprotnosti sa zakonima treće zemlje.
88. Zahtjevi u pogledu upravljanja iz Direktive 2013/36/EU i ove smjernice primjenjuju se na institucije bez obzira na to jesu li one društva kćeri matičnog društva u trećoj zemlji. U slučaju kada je konsolidirajuća institucija društvo kćer iz EU-a čije se matično društvo nalazi u trećoj zemlji, opseg bonitetne konsolidacije ne uključuje razinu matičnog društva koje se nalazi u trećoj zemlji i druga izravna društva kćeri tog matičnog društva. Konsolidirajuća institucija treba osigurati da se grupna politika upravljanja matične institucije iz treće zemlje uzima u obzir u okviru njezinih politika upravljanja ako navedeno nije u suprotnosti sa zahtjevima iz mjerodavnog prava EU-a ili nacionalnog prava, uključujući Direktivu 2013/36/EU i ove smjernice.
89. Pri uspostavi politika i dokumentiranju sustava upravljanja institucije trebaju uzeti u obzir aspekte navedene u Prilogu I. ovim smjernicama. Iako politike i dokumentacija mogu biti zasebni dokumenti, institucije trebaju razmotriti njihovo spajanje ili upućivanje na njih u jedinstvenom dokumentu o okviru upravljanja.

8 Politika eksternalizacije²⁰

90. Upravljačko tijelo treba odobriti te redovito preispitivati i ažurirati politiku eksternalizacije institucije i time osigurati pravodobnu provedbu odgovarajućih promjena.
91. Politikom eksternalizacije treba se uzeti u obzir učinak eksternalizacije na poslovanje institucije i rizike s kojima se suočava (kao što su operativni rizici, uključujući pravne rizike i IT-rizike, reputacijski rizici i koncentracijski rizici). U politici se trebaju opisati sustavi izvješćivanja i praćenja koji će se provoditi od sklapanja do završetka ugovora o eksternalizaciji (uključujući pripremu poslovnog slučaja za eksternalizaciju, sklapanje ugovora o eksternalizaciji, provedbu ugovora do njegova isteka, planove postupanja u kriznim situacijama i izlazne strategije). Institucija snosi odgovornost za sve eksternalizirane usluge i aktivnosti te odluke o upravljanju koje proizlaze iz njih. Stoga se u politici eksternalizacije jasno treba navesti da se eksternalizacijom instituciju ne oslobađa od regulatornih obveza i njezinih obveza prema klijentima.
92. U politici treba navesti da sustavi eksternalizacije ne smiju ometati učinkovit izravan ili neizravan nadzor institucije niti biti u suprotnosti s nadzornim ograničenjima u pogledu usluga i djelatnosti. Politikom treba obuhvatiti i unutargrupnu eksternalizaciju (tj. usluge koje pruža zaseban pravni subjekt unutar grupe institucije) i uzeti u obzir sve posebne okolnosti na razini grupe.
93. U okviru politike od institucije treba zahtijevati da pri odabiru značajnih vanjskih pružatelja usluga ili u aktivnostima eksternalizacije uzme u obzir ima li pružatelj usluga uspostavljene odgovarajuće etičke standarde ili kodeks ponašanja.

Glava IV. – Kultura rizika i poslovno ponašanje

9 Kultura rizika

94. Dobra i dosljedna kultura rizika treba biti ključni element u učinkovitom upravljanju rizicima institucije i treba omogućiti institucijama da donose dobre odluke na temelju informiranosti.
95. Institucije trebaju razviti integriranu kulturu rizika na razini institucije koja se temelji na potpunom razumijevanju i holističkom pristupu rizicima s kojima se suočavaju i načinu na koji njima upravljaju pritom uzimajući u obzir sklonost preuzimanju rizika institucije.
96. Institucije trebaju razviti kulturu rizika politikama, komunikacijom i osposobljavanjem radnika u pogledu djelatnosti, strategije i profila rizičnosti institucije te trebaju prilagoditi komunikaciju i osposobljavanje radnika tako da se u njima obrađuju i odgovornosti radnika u pogledu preuzimanja rizika i upravljanja rizicima.

²⁰ U ovim se smjernicama govori samo o općoj politici eksternalizacije, a posebni aspekti eksternalizacije obrađuju se u smjernicama CEBS-a o eksternalizaciji koje se moraju revidirati. Te smjernice dostupne su na <https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing>.

97. Radnici trebaju biti u potpunosti upoznati sa svojim odgovornostima povezanim s upravljanjem rizicima. Upravljanje rizicima ne smije biti ograničeno na stručnjake za rizike ili kontrolne funkcije. Poslovne jedinice pod nadzorom upravljačkog tijela prvenstveno trebaju biti odgovorne za svakodnevno upravljanje rizicima u skladu s politikama, postupcima i kontrolama institucije pritom uzimajući u obzir sklonost institucije preuzimanju rizika i njezinu sposobnost podnošenja rizika.
98. Snažna kultura rizika treba uključivati, no nije nužno ograničena na:
- a. rukovodstvo kao uzor (engl. *tone from the top*): upravljačko tijelo treba biti odgovorno za uspostavu i priopćavanje informacija o temeljnim vrijednostima i očekivanjima institucije. Ponašanje njezinih članova treba odražavati vrijednosti za koje se zalažu. Rukovodstvo institucije, uključujući nositelje ključnih funkcija, treba pridonijeti unutarnjem informiranju radnika o temeljnim vrijednostima i očekivanjima. Radnici trebaju postupati u skladu sa svim mjerodavnim zakonima i propisima te bez odgode upozoriti na opaženu neusklađenost unutar ili izvan institucije (npr. nadležno tijelu u okviru postupka zviždanja). Upravljačko tijelo treba neprekidno promicati, pratiti i procjenjivati kulturu rizika institucije, razmatrati učinak kulture rizika na financijsku stabilnost, profil rizičnosti i robusno upravljanje institucijom te po potrebi provesti promjene.
 - b. odgovornost: relevantni radnici na svim razinama trebaju poznavati i razumjeti temeljne vrijednosti institucije te njezinu sklonost preuzimanju rizika i sposobnost podnošenja rizika u mjeri u kojoj je to potrebno za njihovu ulogu. Oni trebaju biti sposobni izvršavati svoje zadatke i svjesni da će snositi odgovornost za svoje postupanje povezano s preuzimanjem rizika institucije.
 - c. učinkovitu komunikaciju i izazov: dobrom kulturom rizika promiče se okruženje otvorene komunikacije i učinkovitog propitivanja u kojem se u postupcima donošenja odluka potiču različita mišljenja, omogućuje ispitivanje postojećih praksi, njeguje konstruktivno kritičko razmišljanje među radnicima te promiče okruženje otvorenog i konstruktivnog sudjelovanja u cijeloj organizaciji.
 - d. poticaje: odgovarajući poticaji trebaju imati ključnu ulogu u usklađivanju postupaka preuzimanja rizika s profilom rizičnosti institucije i njezinim dugoročnim interesom²¹.

10 Korporativne vrijednosti i kodeks ponašanja

99. Upravljačko tijelo treba razviti, donijeti i promicati visoke etičke i profesionalne standarde te ih se pridržavati, uzimajući u obzir potrebe i značajke institucije, i treba osigurati provedbu takvih standarda (kroz kodeks ponašanja ili sličan instrument). Treba i nadzirati pridržavaju li se radnici tih standarda. Upravljačko tijelo može, gdje je primjenjivo, donositi i provoditi

²¹ Vidjeti i smjernice EBA-e o dobrim politikama primitaka na temelju članka 74. stavka 3. i članka 75. stavka 2. Direktive 2013/36/EU i objava na temelju članka 450. Uredbe (EU) br. 575/2013 (EBA/GL/2015/22) dostupne na <https://www.eba.europa.eu/regulation-and-policy/remuneration>.

standarde institucije na razini grupe ili zajedničke standarde koje su objavile udruge ili druge nadležne organizacije.

100. Cilj provedenih standarda treba biti smanjenje rizika kojima je institucija izložena, osobito operativnih i reputacijskih rizika koji mogu imati značajan nepovoljni učinak na profitabilnost i održivost institucije u obliku novčanih kazni, sudskih troškova, ograničenja koja će nametnuti nadležna tijela, ostalih novčanih i kaznenih sankcija te gubitak vrijednosti robne marke i pouzdanja potrošača.

101. Upravljačko tijelo treba imati jasne i dokumentirane politike o načinu na koji treba ispuniti te standarde. U tim se politikama treba:

- a. podsjetiti čitatelje da se sve aktivnosti institucije trebaju provoditi u skladu s mjerodavnim pravom i korporativnim vrijednostima institucije;
- b. u skladu s odjeljkom 9. ovih smjernica promicati svijest o rizicima snažnom kulturom rizika kojom se prenose očekivanja upravljačkog tijela da će aktivnosti ostati unutar granica sklonosti preuzimanju rizika i ograničenja koje je odredila institucija te povezanih odgovornosti radnika;
- c. utvrditi načela i pružiti primjere prihvatljivog i neprihvatljivog ponašanja povezanog osobito s pogrešnim financijskim izvješćivanjem i povredama dužnosti, gospodarskim i financijskim kaznenim djelima (uključujući prijevaru, pranje novca i protumonopolske prakse, novčane kazne, mito i korupciju, manipuliranje tržištem, neprimjerenu prodaju i druga kršenja zakona o zaštiti potrošača);
- d. razjasniti da se od radnika očekuje ne samo da ispunjavaju pravne i regulatorne zahtjeve te interne politike nego i da postupaju pošteno i s integritetom te izvršavaju svoje dužnosti s odgovarajućom vještinom, dužnom pažnjom i trudom te
- e. osigurati da su radnici svjesni mogućih unutarnjih i vanjskih disciplinskih postupaka, pravnih postupaka i kazni koje mogu proizaći iz povreda dužnosti i neprihvatljivog ponašanja.

102. Institucije trebaju nadzirati usklađenost s tim standardima i osigurati osviještenost radnika u tom pogledu, npr. osposobljavanjem. Institucije trebaju odrediti funkciju koja je odgovorna za praćenje usklađenosti s kodeksom ponašanja ili sličnim instrumentom i ocjenjivanje njihovih povreda te odrediti postupak za rješavanje pitanja neusklađenosti. O rezultatima treba redovito izvješćivati upravljačko tijelo.

11 Politika upravljanja sukobima interesa na razini institucije

103. Upravljačko tijelo treba biti odgovorno za uspostavu, odobrenje i nadzor provedbe i održavanja učinkovitih politika za utvrđivanje, procjenu i smanjenje ili sprečavanje stvarnih i potencijalnih sukoba interesa na razini institucije te upravljanje njima, npr. kao posljedica različitih aktivnosti

i uloga institucije, različitih institucija u opsegu bonitetne konsolidacije ili različitih poslovnih linija ili jedinica unutar institucije ili u vezi s vanjskim dionicima.

104. Institucije trebaju, u okviru svojih organizacijskih i administrativnih sustava, poduzeti odgovarajuće mjere kojima se sprečava nepovoljan učinak sukoba interesa na interese klijenata.
105. Mjere institucija za upravljanje sukobima interesa ili, gdje je primjenjivo, njihovo smanjenje trebaju se dokumentirati i trebaju uključivati među ostalim:
- a. odgovarajuće razgraničavanje dužnosti, npr. povjeravanje sukobljenih aktivnosti u obradi transakcija ili pružanju usluga različitim osobama ili povjeravanje nadzornih i izvještajnih odgovornosti za sukobljene aktivnosti različitim osobama;
 - b. uspostavu informacijskih prepreka, npr. fizičkim odvajanjem određenih poslovnih linija ili jedinica i
 - c. uspostavu odgovarajućih postupaka za transakcije s povezanim stranama, npr. zahtijevanje provedbe transakcija po tržišnim uvjetima.

12 Politika upravljanja sukobima interesa za radnike²²

106. Upravljačko tijelo treba biti odgovorno za uspostavu, odobrenje i nadzor provedbe i održavanje učinkovitih politika za utvrđivanje, procjenu i smanjenje ili sprečavanje stvarnih i potencijalnih sukoba interesa institucije i privatnih interesa radnika, uključujući članova upravljačkog tijela, koji bi mogli nepovoljno utjecati na izvršavanje njihovih dužnosti i odgovornosti te upravljanje njima. Konsolidirajuća institucija treba uzeti u obzir interese u grupnoj politici upravljanja sukobima interesa na konsolidiranoj ili potkonsolidiranoj osnovi.
107. Cilj politike treba biti utvrđivanje sukoba interesa radnika, uključujući interese članova njihove uže obitelji. Institucije trebaju uzeti u obzir da sukobi interesa mogu proizaći ne samo iz sadašnjih nego i prošlih osobnih ili profesionalnih odnosa. Kada dođe do sukoba interesa, institucije trebaju procijeniti njihovu značajnost te odabrati i provesti odgovarajuće mjere smanjenja.
108. U pogledu sukoba interesa koji mogu proizaći iz prošlih odnosa institucije trebaju utvrditi odgovarajući rok u kojem žele da radnici prijave takve sukobe interesa zbog toga što oni i dalje mogu imati utjecaj na ponašanje radnika i njihovo sudjelovanje u donošenju odluka.
109. Politikom treba obuhvatiti najmanje sljedeće situacije ili odnose u kojima mogu nastati sukobi interesa:

²² Ovaj odjeljak treba tumačiti zajedno sa zajedničkim smjernicama ESMA-e i EBA-e za procjenu prikladnosti članova upravljačkog tijela i nositelja ključnih funkcija na temelju Direktive 2013/36/EU i Direktive 2014/65/EU.

- a. gospodarski interesi (npr. dionice, druga vlasnička prava i članstva, financijski udjeli i drugi gospodarski interesi u komercijalnim klijentima, prava intelektualnog vlasništva, krediti koje je institucija dala društvu u vlasništvu radnika, članstvo u tijelu ili vlasništvo tijela ili subjekta sa sukobljenim interesima);
 - b. osobni ili profesionalni odnosi s vlasnicima kvalificiranih udjela u instituciji;
 - c. osobni ili profesionalni odnosi s radnicima institucije ili subjekata uključenih u opseg bonitetne konsolidacije (npr. obiteljski odnosi);
 - d. ostala radna mjesta i prethodna radna mjesta u kraćem prošlom razdoblju (npr. pet godina);
 - e. osobni ili profesionalni odnosi s bitnim vanjskim dionicima (npr. povezanost sa značajnim dobavljačima, savjetnicima ili drugim pružateljima usluga) i
 - f. politički utjecaj ili politički odnosi.
110. Ne dovodeći u pitanje prethodno navedeno, institucije trebaju uzeti u obzir da činjenica da je netko dioničar institucije ili ima privatne račune ili kredite kod institucije ili se koristi njezinim drugim uslugama ne bi trebala dovesti do situacije u kojoj se smatra da su radnici u sukobu interesa ako se pridržavaju odgovarajućeg minimalnog praga.
111. Politikom se trebaju uspostaviti postupci izvješćivanja i obavješćivanja funkcije čija je odgovornost propisana politikom. Radnici trebaju biti obvezni odmah interno prijaviti sva pitanja koja mogu dovesti ili su već dovela do sukoba interesa.
112. U politici treba razlikovati sukobe interesa koji su stalni i koje treba trajno riješiti te sukobe interesa koji se pojavljuju neočekivano u vezi s određenim događajem (npr. transakcijom, odabirom pružatelja usluga itd.) i koji se obično mogu riješiti jednokratnom mjerom. Interesi institucije trebaju u svim okolnostima biti primarni pri donošenju odluka.
113. Politikom se trebaju uspostaviti postupci, mjere, zahtjevi u pogledu dokumentacije i odgovornosti za utvrđivanje i sprečavanje sukoba interesa, procjenu njihove značajnosti i poduzimanje mjera za njihovo smanjenje. Ti postupci, zahtjevi, odgovornosti i mjere trebaju uključivati:
- a. povjeravanje sukobljenih aktivnosti ili transakcija različitim osobama;
 - b. sprečavanje radnika koji su aktivni i izvan institucije u ostvarivanju neprikladnog utjecaja unutar institucije u pogledu tih drugih aktivnosti;
 - c. utvrđivanje obveze članova upravljačkog tijela da se suzdrže od glasovanja o bilo kojoj stvari kada član jest ili bi mogao biti u sukobu interesa ili kada je na drugi način

ugrožena objektivnost ili sposobnost člana da propisno ispuni svoje dužnosti u instituciji;

- d. uspostavu odgovarajućih postupaka za transakcije s povezanim stranama (institucije mogu, među ostalim, razmisliti o obvezi provedbe transakcija po tržišnim uvjetima, obvezi potpune primjene svih relevantnih postupaka unutarnje kontrole u tim transakcijama, obvezi traženja obvezujućeg savjeta od neovisnih članova upravljačkog tijela, obveznom odobrenju svih bitnih transakcija od strane dionika i ograničavanju izloženosti takvim transakcijama) i
- e. onemogućavanje članovima upravljačkog tijela da drže direktorske pozicije u konkurentnim institucijama, osim kada je riječ o institucijama koje pripadaju istom institucionalnom sustavu zaštite, kako je navedeno u članku 113. stavku 7. Uredbe (EU) br. 575/2013, u kreditnim institucijama koje su stalno povezane sa središnjim tijelom, kako je navedeno u članku 10. Uredbe (EU) br. 575/2013, ili u institucijama u opsegu bonitetne konsolidacije.

114. Politikom bi se osobito trebao obuhvatiti rizik od sukoba interesa na razini upravljačkog tijela i pružiti dostatne smjernice za utvrđivanje i rješavanje sukoba interesa koji bi mogli onemogućiti članove upravljačkog tijela u donošenju objektivnih i nepristranih odluka čiji je cilj ispunjavanje najboljih interesa institucije. Institucije trebaju uzeti u obzir da sukobi interesa mogu imati utjecaj na neovisnost članova upravljačkog tijela²³.

115. Stvarni ili potencijalni sukobi interesa koji su prijavljeni odgovornoj funkciji unutar institucije trebaju se na odgovarajući način procijeniti i riješiti. Ako se utvrdi sukob interesa radnika, institucija treba evidentirati donesenu odluku, osobito ako su sukob interesa i povezani rizici prihvaćeni, te evidentirati način na koji je taj prihvaćeni sukob interesa uspješno smanjen ili ispravljen.

116. Svi stvarni i potencijalni sukobi interesa na razini upravljačkog tijela trebaju se na pojedinačnoj i zajedničkoj razini prikladno dokumentirati, o njima se treba obavijestiti upravljačko tijelo koje tada treba o njima raspraviti, odlučiti i propisno ih riješiti.

13 Postupci unutarnjeg upozoravanja

117. Institucije trebaju uspostaviti i održavati odgovarajuće politike i postupke unutarnjeg upozoravanja kojima se omogućuje radnicima da putem posebnog, neovisnog i samostalnog kanala prijave potencijalna ili stvarna kršenja regulatornih ili unutarnjih zahtjeva, uključujući no ne ograničavajući se na one iz Uredbe (EU) br. 575/2013 i nacionalne odredbe kojima se prenosi Direktiva 2013/36/EU, ili sustava internog upravljanja. Radnici koji prijavljuju kršenje ne trebaju nužno imati dokaze o kršenju, no njihova sigurnost u počinjeno kršenje treba biti dostatno visoka da bi bila dovoljan razlog za pokretanje istrage.

²³ Vidjeti i zajedničke smjernice ESMA-e i EBA-e za procjenu primjerenosti članova upravljačkog tijela i nositelja ključnih funkcija na temelju Direktive 2013/36/EU i Direktive 2014/65/EU.

118. Kako bi se izbjeglo sukobe interesa, radnicima treba omogućiti prijavu kršenja izvan redovitih linija izvješćivanja (npr. putem funkcije praćenja usklađenosti, funkcije unutarnje revizije ili neovisnog unutarnjeg postupka zviždanja). Postupcima upozoravanja treba se osigurati zaštita osobnih podataka osoba koje prijavljuju kršenje i fizičkih osoba koje su navodno odgovorne za kršenje u skladu s Direktivom 95/46/EZ.
119. Postupci upozoravanja trebaju biti dostupni svim radnicima u instituciji.
120. Informacije koje radnici pruže u postupcima upozoravanja trebaju biti, ako je prikladno, dostupne upravljačkom tijelu i drugim odgovornim funkcijama utvrđenima u politici unutarnjeg upozoravanja. Kada to traži radnik koji prijavljuje kršenje, informacije se trebaju dostaviti upravljačkom tijelu i drugim odgovornim funkcijama tako da predmetni radnik ostane anonimn. Institucije mogu uspostaviti i postupak zviždanja kojim se omogućuje anonimna prijava informacija.
121. Institucije trebaju osigurati odgovarajuću zaštitu osobe koja prijavljuje kršenje od svih nepovoljnih učinaka, npr. odmazde, diskriminacije ili drugih vrsta nepoštenog postupanja. Institucija treba osigurati da nijedna osoba pod njezinom kontrolom ne sudjeluje u viktimizaciji osobe koja je prijavila kršenje te poduzeti odgovarajuće mjere protiv osoba odgovornih za tu viktimizaciju.
122. Institucije trebaju zaštititi i prijavljene osobe od svih nepovoljnih učinaka u slučaju da se istragom ne pronađu dokazi kojima bi se opravdalo poduzimanje mjera protiv tih osoba. Ako se poduzmu mjere, institucija ih treba poduzeti tako da zaštiti predmetnu osobu od nenamjernih nepovoljnih učinaka koji nadilaze cilj poduzete mjere.
123. Točnije, postupci unutarnjeg upozoravanja trebaju:
- a. biti dokumentirani (npr. priručnici za radnike);
 - b. pružiti jasna pravila kojima se osigurava povjerljivo postupanje s osobama koje prijavljuju kršenje, prijavljenim osobama i samim kršenjem u skladu s Direktivom 95/46/EZ osim ako obveza objave nije propisana nacionalnim pravom u kontekstu daljnjih istraga ili kasnijih sudskih postupaka;
 - c. zaštititi radnike koji su iskazali zabrinutost oko svoje viktimizacije jer su prijavili kršenja koja se trebaju prijaviti;
 - d. osigurati da se prijavljena potencijalna ili stvarna kršenja procijene i o njima informira uključujući, gdje je prikladno, relevantno nadležno tijelo ili agenciju za provedbu zakona;
 - e. osigurati, gdje je moguće, da se radnicima koji su prijavili potencijalna ili stvarna kršenja izda potvrda o zaprimanju informacija;

- f. osigurati praćenje ishoda istrage prijavljenog kršenja i
- g. osigurati odgovarajuće vođenje evidencije.

14 Izvješćivanje nadležnih tijela o kršenjima

124. Nadležna tijela trebaju uspostaviti učinkovite i pouzdane mehanizme koji omogućuju radnicima institucija izvješćivanje nadležnih tijela o bitnim potencijalnim ili stvarnim kršenjima regulatornih zahtjeva, uključujući no ne ograničavajući se na one iz Uredbe (EU) br. 575/2013 i nacionalne odredbe kojima se prenosi Direktiva 2013/36/EU. Ti mehanizmi trebaju uključivati najmanje:

- a. posebne postupke za zaprimanje izvješća o kršenjima i daljnje praćenje, primjerice poseban odjel, jedinica ili funkcija za zviždanje;
- b. odgovarajuću zaštitu kako je navedena u odjeljku 13.;
- c. zaštitu osobnih podataka fizičkih osoba koje prijavljuju kršenje i fizičkih osoba koje su navodno odgovorne za kršenje u skladu s Direktivom 95/46/EZ i
- d. jasne postupke kako su utvrđeni u stavku 123.

125. Ne dovodeći u pitanje mogućnost izvješćivanja o kršenjima s pomoću mehanizama nadležnih tijela, nadležna tijela mogu poticati radnike da prvo pokušaju upotrijebiti i nastoje upotrebljavati postupke unutarnjeg upozoravanja svoje institucije.

Glava V. – Okvir i mehanizmi unutarnje kontrole

15 Okvir unutarnje kontrole

126. Institucije trebaju razviti i održavati kulturu kojom se potiče pozitivan stav prema kontroli rizika i usklađenosti unutar institucije te robustan i sveobuhvatan okvir unutarnje kontrole. U tom okviru poslovne linije institucija trebaju biti odgovorne za upravljanje rizicima koji nastaju tijekom provedbe aktivnosti i trebaju imati uspostavljene kontrole čiji je cilj osigurati usklađenost s unutarnjim i vanjskim zahtjevima. U tom okviru institucije trebaju imati kontrolne funkcije s odgovarajućim i dostatnim ovlastima, uporištem i pristupom upravljačkom tijelu radi ispunjavanja svoje misije te trebaju imati okvir upravljanja rizicima.

127. Okvir unutarnje kontrole predmetne institucije treba se prilagoditi posebnostima poslovanja svake institucije zasebno, njezinoj složenosti i povezanim rizicima pritom uzimajući u obzir grupni kontekst. Predmetne institucije trebaju organizirati razmjenu potrebnih informacija tako da osiguraju da svako upravljačko tijelo, poslovna linija i unutarnja jedinica, uključujući sve kontrolne funkcije, mogu obavljati svoje dužnosti. To podrazumijeva, primjerice,

neophodnu razmjenu odgovarajućih informacija između poslovnih linija i funkcije praćenja usklađenosti na razini grupe te između osoba odgovornih za rad kontrolnih funkcija na razini grupe i upravljačkog tijela institucije.

128. Okvir unutarnje kontrole treba obuhvatiti cijelu organizaciju, uključujući odgovornosti i zadaće upravljačkog tijela, i aktivnosti svih poslovnih linija i unutarnjih jedinica, uključujući kontrolne funkcije, eksternalizirane aktivnosti i distribucijske kanale.

129. Okvir unutarnje kontrole institucije treba osigurati:

- a. učinkovito i djelotvorno poslovanje;
- b. razborito vođenje poslovanja;
- c. prikladno utvrđivanje, mjerenje i smanjenje rizika;
- d. pouzdanost financijskih i nefinancijskih informacija o kojima se izvješćuje na unutarnjoj i vanjskoj razini;
- e. dobre administrativne i računovodstvene postupke te
- f. usklađenost sa zakonima, propisima, nadzornim zahtjevima te unutarnjim politikama, postupcima, pravilima i odlukama institucije.

16 Provedba okvira unutarnje kontrole

130. Upravljačko tijelo treba biti odgovorno za uspostavu i praćenje prikladnosti i učinkovitosti okvira, postupaka i mehanizama unutarnje kontrole te za nadzor svih poslovnih linija i unutarnjih jedinica, uključujući kontrolne funkcije (kao što su funkcija upravljanja rizicima, funkcija praćenja usklađenosti i funkcija unutarnje revizije). Institucije trebaju uspostaviti, održavati i redovito ažurirati prikladne pisane politike, mehanizme i postupke unutarnje kontrole koje treba odobriti upravljačko tijelo.

131. Institucija treba imati jasan, transparentan i dokumentiran proces odlučivanja te jasnu raspodjelu odgovornosti i ovlasti unutar okvira unutarnje kontrole, uključujući njezine poslovne linije, unutarnje jedinice i kontrolne funkcije.

132. Institucije trebaju obavijestiti sve radnike o tim politikama, mehanizmima i postupcima te svim njihovim značajnim promjenama.

133. Pri provedbi okvira unutarnje kontrole institucije trebaju uspostaviti prikladno razdvajanje dužnosti, npr. povjeravanjem sukobljenih aktivnosti u obradi transakcija ili pružanju usluga različitim osobama ili povjeravanjem nadzornih i izvještajnih odgovornosti za sukobljene

aktivnosti različitim osobama, te uspostaviti informacijske prepreke, npr. fizičkim odvajanjem određenih odjela.

134. Kontrolne funkcije trebaju provjeriti provode li se ispravno politike, mehanizmi i postupci utvrđeni okvirom unutarnje kontrole u okviru njihovih područja nadležnosti.
135. Kontrolne funkcije trebaju redovito podnositi upravljačkom tijelu pisana izvješća o utvrđenim velikim nedostacima. Ta izvješća trebaju u pogledu svakog utvrđenog novog velikog nedostatka uključivati bitne uključene rizike, procjenu učinka, preporuke i korektivne mjere koje se trebaju poduzeti. Upravljačko tijelo treba pravodobno i učinkovito poduzeti daljnje korake na temelju nalaza kontrolnih funkcija te treba zahtijevati odgovarajuće korektivne mjere. Treba se uspostaviti formalni postupak poduzimanja daljnjeg praćenja na temelju nalaza i poduzetih korektivnih mjera.

17 Okvir upravljanja rizicima

136. U sklopu sveobuhvatnog okvira unutarnje kontrole institucije trebaju imati holistički okvir upravljanja rizicima na razini institucije koji se primjenjuje u svim poslovnim linijama i unutarnjim jedinicama, uključujući kontrolne funkcije, i kojim se u potpunosti prepoznaje gospodarska priroda njezine cjelokupne izloženosti rizicima. Okvirom upravljanja rizicima treba omogućiti instituciji da donosi odluke o preuzimanju rizika na temelju potpune informiranosti. Okvirom upravljanja rizicima treba obuhvatiti bilančne i izvanbilančne rizike te stvarne rizike i buduće rizike kojima bi institucija mogla biti izložena. Rizike treba procjenjivati odozdo prema gore i odozgo prema dolje unutar poslovnih linija i među njima uporabom dosljedne terminologije i kompatibilnih metodologija u cijeloj instituciji i na konsolidiranoj ili potkonsolidiranoj razini. Okvirom upravljanja rizicima trebaju biti obuhvaćeni svi bitni rizici uz odgovarajuće razmatranje financijskih i nefinancijskih rizika, uključujući kreditni, tržišni, koncentracijski, operativni, IT, reputacijski, pravni i strateški rizik te rizike likvidnosti, ponašanja i usklađenosti.
137. Okvir upravljanja rizicima institucije treba uključivati politike, postupke, ograničenja rizika i kontrole rizika kojima se osigurava prikladno, pravodobno i neprekidno utvrđivanje, mjerenje ili procjena, praćenje i smanjenje rizika te upravljanje i izvješćivanje o njima na razini poslovne linije, razini institucije i konsolidiranoj ili potkonsolidiranoj razini.
138. U okviru upravljanja rizicima institucije trebaju se pružiti posebne smjernice o provedbi njezinih strategija. Tim se smjernicama, gdje je prikladno, trebaju utvrditi i održavati unutarnja ograničenja dosljedna sklonosti preuzimanju rizika institucije i razmjerna njezinom dobrom radu, financijskoj snazi, kapitalnoj osnovi i strateškim ciljevima. Profil rizičnosti institucije treba se održavati unutar tih uspostavljenih ograničenja. Okvirom upravljanja rizicima treba osigurati da postoji definirani postupak za upozoravanje na prekoračenja ograničenja rizika i njihovo rješavanje odgovarajućim postupkom daljnjeg praćenja.

139. Okvir upravljanja rizicima treba podvrgavati neovisnoj unutarnjoj provjeri, npr. koju će provesti funkcija unutarnje revizije, i redovitoj ponovnoj provjeri njegove usklađenosti sa sklonošću preuzimanju rizika institucije pritom uzimajući u obzir informacije dobivene od funkcije upravljanja rizicima i, ako je osnovan, odbora za rizike. Čimbenici koji bi se trebali razmotriti uključuju unutarnja i vanjska kretanja (uključujući promjene u bilanci i prihodima), povećanje složenosti poslovanja, profila rizičnosti ili operativne strukture institucije, geografsko širenje, spajanja i pripajanja te uvođenje novih proizvoda ili poslovnih linija.
140. Pri utvrđivanju i mjerenju ili procjeni rizika institucija treba razviti odgovarajuće metodologije, uključujući alate koji se odnose na budućnost i one koji se odnose na prošlost. Metodologijama treba omogućiti agregiranje izloženosti rizicima diljem poslovnih linija i pružanje potpore u utvrđivanju koncentracija rizika. Alati trebaju uključivati procjenu stvarnog profila rizičnosti u odnosu na sklonost preuzimanju rizika institucije te utvrđivanje i procjenu potencijalnih i stresnih izloženosti rizicima u odnosu na sposobnost podnošenja rizika institucije u različitim pretpostavljenim nepovoljnim okolnostima. Alatima se trebaju pružiti informacije o svim promjenama profila rizičnosti koje bi mogle biti potrebne. Institucije trebaju donijeti odgovarajuće konzervativne pretpostavke pri sastavljanju stresnih scenarija.
141. Institucije trebaju uzeti u obzir da rezultati kvantitativnih metodologija procjene, uključujući testiranje otpornosti na stres, uvelike ovise o ograničenjima i pretpostavkama modela (uključujući težinu i trajanje šoka i osnovne rizike). Na primjer, modeli u kojima se utvrde vrlo visoki povрати od ekonomskog kapitala možda proizlaze iz slabosti u modelima (npr. isključivanje određenih bitnih rizika) umjesto iz izvanredne strategije ili izvrsne provedbe strategije od strane institucije. Utvrđivanje razine preuzetog rizika stoga se ne treba temeljiti samo na kvantitativnim informacijama ili ishodima modela nego treba uključivati i kvalitativni pristup (uključujući stručnu prosudbu i kritičku analizu). Bitna kretanja i podaci u makroekonomskom okruženju trebaju se izričito razmotriti kako bi se utvrdio njihov učinak na izloženost i portfelje.
142. Krajnja odgovornost za procjenu rizika leži isključivo u rukama institucije koja stoga treba kritički procijeniti rizike i suzdržati se od oslanjanja isključivo na vanjske procjene. Na primjer, institucija treba potvrditi kupljeni model rizika i prilagoditi ga vlastitim okolnostima kako bi se osiguralo da se modelom precizno i sveobuhvatno bilježi i analizira rizik.
143. Institucije trebaju biti potpuno svjesne ograničenja modela i metrike te upotrebljavati ne samo kvantitativne nego i kvalitativne alate za procjenu rizika (uključujući stručnu prosudbu i kritičku analizu).
144. Osim vlastitih procjena institucije mogu upotrijebiti i vanjske procjene rizika (uključujući vanjski kreditni rejting ili modele rizika kupljene izvan institucije). Institucije trebaju biti potpuno svjesne točnog opsega tih procjena i njihovih ograničenja.
145. Trebaju se uspostaviti redoviti i transparentni mehanizmi izvješćivanja kako bi se upravljačkom tijelu, njegovu odboru za rizike, ako je osnovan, i svim relevantnim jedinicama u instituciji

pravodobno dostavljala precizna, sažeta, razumljiva i smisljena izvješća te kako bi prethodno navedeni mogli dijeliti bitne informacije o utvrđivanju, mjerenju ili procjeni i praćenju rizika te upravljanju njima. Okvir izvješćivanja treba dobro utvrditi i dokumentirati.

146. Učinkovita komunikacija i svijest o rizicima te strategija upravljanja rizicima ključne su za cjelokupan postupak upravljanja rizicima, uključujući provjeru i proces odlučivanja, i pomažu u sprečavanju donošenja odluka koje bi nesvjesno mogle povećati rizik. Učinkovito izvješćivanje o riziku uključuje dobro unutarnje razmatranje strategije upravljanja rizicima i bitnih podataka o riziku (npr. izloženosti i ključni pokazatelji rizika) te obavješćivanje o njima po horizontalnoj liniji unutar institucije i vertikalnoj liniji u upravnoj hijerarhiji.

18 Novi proizvodi i značajne promjene²⁴

147. Institucija treba imati uspostavljenu dobro dokumentiranu politiku odobrenja novih proizvoda (NPAP) koju je odobrilo upravljačko tijelo, a koja se odnosi na razvoj novih i značajne promjene postojećih tržišta, proizvoda i usluga te izvanredne transakcije. Usto se politikom trebaju obuhvatiti i značajne promjene povezanih postupaka (npr. novi sustavi eksternalizacije) i sustava (npr. postupci IT-promjena). NPAP treba osigurati dosljednost odobrenih proizvoda i promjena sa strategijom upravljanja rizicima i sklonošću preuzimanju rizika institucije te odgovarajućim ograničenjima odnosno treba osigurati provedbu potrebnih izmjena.
148. Značajne promjene ili izvanredne transakcije mogu uključivati spajanja i pripajanja, uključujući moguće posljedice provedbe nedovoljno temeljite dubinske analize kojom se ne uspiju utvrditi rizici i odgovornosti nakon spajanja, uspostavu struktura (npr. novih društava kćeri ili društava posebne namjene), nove proizvode, promjene sustava ili okvira ili postupaka upravljanja rizicima i promjene u organizaciji institucije.
149. Institucija treba imati posebne postupke za procjenu usklađenosti s tim politikama pritom uzimajući u obzir informacije dobivene od funkcije upravljanja rizicima. To treba uključivati sustavnu prethodnu procjenu i dokumentirano mišljenje funkcije praćenja usklađenosti za nove proizvode ili značajne promjene postojećih proizvoda.
150. NPAP-om institucije trebaju se obuhvatiti sva razmatranja koja se trebaju uzeti u obzir prije odlučivanja o ulasku na nova tržišta, trgovanju novim proizvodima, pokretanju novih usluga ili izvršavanju značajnih promjena postojećih proizvoda ili usluga. NPAP treba uključivati i definicije pojmova „novi proizvod/tržište/djelatnost” i „značajne promjene” koje će se upotrebljavati u organizaciji i unutarnjim funkcijama koje će biti uključene u proces odlučivanja.
151. NPAP-om se trebaju utvrditi glavna pitanja koja se moraju riješiti prije donošenja odluke. Njima se moraju obuhvatiti regulatorna usklađenost, računovodstvo, modeli utvrđivanja cijena, učinak na profil rizičnosti, adekvatnost kapitala i profitabilnost, dostupnost odgovarajućih

²⁴ Vidjeti i smjernice EBA-e o zahtjevima u pogledu nadzora i upravljanja za proizvođače i distributere proizvoda za poslovanje sa stanovništvom dostupne na <https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products>.

resursa u odjelu ugovaranja transakcija, odjelu pozadinskih poslova riznice i koordinacijskom odjelu te dostupnost odgovarajućih unutarnjih alata i stručnosti za razumijevanje i praćenje povezanih rizika. U odluci o pokretanju nove aktivnosti trebaju se jasno navesti poslovne jedinice i pojedinačne osobe odgovorne za nju. Ne smije se poduzimati nova aktivnost sve dok nisu dostupni odgovarajući resursi za razumijevanje povezanih rizika i upravljanje njima.

152. Funkcija upravljanja rizicima i funkcija praćenja usklađenosti trebaju biti uključene u odobranje novih proizvoda ili značajnih promjena postojećih proizvoda, postupaka i sustava. Njihov doprinos treba uključivati potpunu i objektivnu procjenu rizika nastalih novim aktivnostima u različitim scenarijima, procjenu svih mogućih nedostataka u okviru upravljanja rizicima i okviru unutarnje kontrole institucije te procjenu sposobnosti institucije da učinkovito upravlja svim novim rizicima. Funkcija upravljanja rizicima treba imati i jasan pregled uvođenja novih proizvoda (ili značajnih promjena postojećih proizvoda, postupaka i sustava) diljem različitih poslovnih linija i portfelja kao i ovlast da zahtijeva podvrgavanje promjena postojećih proizvoda formalnom postupku utvrđenom u NPAP-u.

19 Kontrolne funkcije

153. Kontrolne funkcije trebaju uključivati funkciju upravljanja rizicima (vidjeti odjeljak 20.), funkciju praćenja usklađenosti (vidjeti odjeljak 21.) i funkciju unutarnje revizije (vidjeti odjeljak 22.). Funkcija upravljanja rizicima i funkcija praćenja usklađenosti trebaju biti podložne provjeri koju provodi funkcija unutarnje revizije.
154. Operativni zadaci kontrolnih funkcija mogu se eksternalizirati konsolidirajućoj instituciji ili drugom subjektu unutar ili izvan grupe uz pristanak upravljačkih tijela predmetnih institucija pritom uzimajući u obzir kriterije razmjernosti navedene u glavi I. Čak i kada se operativni zadaci unutarnje kontrole djelomično ili potpuno eksternaliziraju, osoba odgovorna za rad predmetne kontrolne funkcije i upravljačko tijelo i dalje snose odgovornost za te aktivnosti i za održavanje kontrolne funkcije unutar institucije.

19.1 Osobe odgovorne za rad kontrolnih funkcija

155. Položaj osobe odgovorne za rad kontrolnih funkcija treba se uspostaviti na odgovarajućoj hijerarhijskoj razini kako bi se osobi odgovornoj za rad kontrolne funkcije osigurala dostatne ovlasti i uporište za ispunjavanje njezinih odgovornosti. Ne dovodeći u pitanje cjelokupnu odgovornost upravljačkog tijela, osobe odgovorne za rad kontrolnih funkcija trebaju biti neovisne od poslovnih linija ili jedinica koje nadziru. U tu svrhu osobe odgovorne za rad funkcija upravljanja rizicima, praćenja usklađenosti i unutarnje revizije trebaju izvješćivati upravljačko tijelo i izravno mu odgovarati, a upravljačko tijelo treba provjeravati rezultate njihova rada.
156. Osobama odgovornim za rad kontrolnih funkcija po potrebi treba omogućiti pristup upravljačkom tijelu u nadzornoj funkciji i njegovo izvješćivanje kako bi iskazali zabrinutost i upozorili nadzornu funkciju, gdje je prikladno, o određenim kretanjima koji utječu ili bi mogli

utjecati na instituciju. To ne smije spriječiti osobe odgovorne za rad kontrolne funkcije u izvješćivanju po redovitim linijama izvješćivanja.

157. Institucije trebaju imati uspostavljen dokumentirani postupak imenovanja na položaj osobe odgovorne za rad kontrolne funkcije te postupak povlačenja njezinih odgovornosti. U svakom slučaju osobe odgovorne za rad kontrolnih funkcija ne bi se trebale, a u skladu s člankom 76. stavkom 5. Direktive 2013/36/EU osoba odgovorna za rad funkcije upravljanja rizicima ne smije se, ukloniti bez prethodnog odobrenja upravljačkog tijela u nadzornoj funkciji. U značajnim institucijama treba odmah obavijestiti nadležna tijela o odobrenju i glavnim razlozima za uklanjanje osobe odgovorne za rad kontrolnih funkcija.

19.2 Neovisnost kontrolnih funkcija

158. Kako bi se kontrolne funkcije smatrale neovisnima, trebaju se ispuniti sljedeći uvjeti:

- a. njihovi radnici ne smiju izvršavati operativne zadaće koji spadaju u opseg aktivnosti koje kontrolne funkcije trebaju pratiti i nadzirati;
- b. organizacijski su odvojene od aktivnosti koje trebaju pratiti i nadzirati;
- c. ne dovodeći u pitanje cjelokupnu odgovornost članova upravljačkog tijela institucije, osoba odgovorna za rad kontrolne funkcije ne smije biti podređena osobi koja je odgovorna za upravljanje aktivnostima koje kontrolna funkcija prati i nadzire te
- d. primici radnika kontrolnih funkcija ne smiju biti povezani s rezultatima aktivnosti koje kontrolna funkcija prati i nadzire te ne smije biti vjerojatno da će na neki drugi način ugroziti njihovu objektivnost²⁵.

19.3 Udruživanje kontrolnih funkcija

159. Uzimajući u obzir kriterije razmjernosti utvrđene u glavi I., funkcija upravljanja rizicima i funkcija praćenja usklađenosti mogu se udružiti. Funkcija unutarnje revizije ne smije se udružiti s drugom kontrolnom funkcijom.

19.4 Resursi kontrolnih funkcija

160. Kontrolne funkcije trebaju imati dovoljno resursa. Trebaju imati dovoljan broj kvalificiranih radnika (na razini matičnog društva i na razini društva kćeri). Kvalificiranost radnika treba se trajno održavati pa radnici po potrebi trebaju proći osposobljavanje.

161. Kontrolne funkcije trebaju na raspolaganju imati odgovarajuće IT-sustave i podršku te pristup unutarnjim i vanjskim informacijama potrebnima za ispunjavanje svojih odgovornosti. Trebaju

²⁵ Vidjeti i smjernice EBA-e o dobrim politikama primitaka dostupne na <https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies>.

imati pristup svim potrebnim informacijama o svim poslovnim linijama i relevantnim rizičnim društvima kćerima, osobito onima koja mogu potencijalno stvoriti značajne rizike za institucije.

20 Funkcija upravljanja rizicima

162. Institucije trebaju uspostaviti funkciju upravljanja rizicima (RMF) koja pokriva cijelu instituciju. RMF treba imati dostatne ovlasti, uporište i resurse, pritom uzimajući u obzir kriterije razmjernosti navedene u glavi I., kako bi proveo politike rizika i okvir upravljanja rizicima kako je utvrđen u odjeljku 17.
163. RMF po potrebi treba imati izravan pristup upravljačkom tijelu u nadzornoj funkciji i njegovim odborima, ako su osnovani, uključujući osobito odbor za rizike.
164. RMF treba imati pristup svim poslovnim linijama i drugim unutarnjim jedinicama koje bi mogle stvoriti rizik te relevantnim društvima kćerima i pridruženim društvima.
165. Radnici RMF-a trebaju imati dovoljno znanja, vještina i iskustva u vezi s tehnikama i postupcima upravljanja rizicima te tržištima i proizvodima i treba imati pristup redovitom osposobljavanju.
166. RMF treba biti neovisan od poslovnih linija i jedinica čijim rizicima upravlja, no ne smije se sprječavati njihova interakcija. Interakcija između operativnih funkcija i RMF-a trebala bi pomoći u postizanju ciljeva svih radnika institucije odgovornih za upravljanje rizicima.
167. RMF treba biti središnja organizacijska značajka institucije, a njezina struktura treba biti takva da može provoditi politike rizika i upravljati okvirom upravljanja rizicima. RMF treba imati ključnu ulogu u osiguranju da institucija ima uspostavljene učinkovite postupke upravljanja rizicima. RMF treba biti aktivno uključen u donošenje svih značajnih odluka povezanih s upravljanjem rizicima.
168. Značajne institucije mogu razmotriti uspostavu posebnih RMF-ova za svaku značajnu poslovnu liniju. No treba postojati i središnji RMF, uključujući grupni RMF u konsolidirajućoj instituciji, kako bi se pružio holistički pristup svim rizicima na razini institucije i na razini grupe te kako bi se osiguralo postupanje u skladu sa strategijom upravljanja rizicima.
169. RMF treba pružiti bitne neovisne informacije, analize i stručne prosudbe o izloženosti rizicima i savjete o prijedlozima i odlukama o rizicima koje donose poslovne linije ili unutarnje jedinice te treba obavješćivati upravljačko tijelo o tome jesu li oni dosljedni sa sklonošću preuzimanju rizika i strategijom upravljanja rizicima institucije. RMF može preporučiti poboljšanja okvira upravljanja rizicima i korektivne mjere za ispravljanje kršenja politika i postupaka te prekoračenja ograničenja rizika.

20.1 Uloga funkcije upravljanja rizicima u strategiji upravljanja rizicima i odlukama o rizicima

170. RMF se treba u ranoj fazi aktivno uključiti u razradu strategije upravljanja rizicima institucije i osiguranje da institucija ima uspostavljene učinkovite postupke upravljanja rizicima. RMF treba pružiti upravljačkom tijelu sve bitne informacije povezane s rizikom koje će mu omogućiti određivanje razine sklonosti preuzimanju rizika institucije. RMF treba procijeniti robusnost i održivost strategije upravljanja rizicima i sklonosti preuzimanju rizika. Treba osigurati da se sklonost preuzimanju rizika na odgovarajući način pretoči u specifična ograničenja rizika. RMF treba procijeniti i strategije upravljanja rizicima poslovnih jedinica, uključujući ciljeve koje predlože poslovne jedinice, te se treba uključiti prije nego što upravljačko tijelo donese odluku o strategijama upravljanja rizicima. Ciljevi trebaju biti realistični i dosljedni sa strategijom upravljanja rizicima institucije.
171. RMF-ovo sudjelovanje u procesima odlučivanja trebalo bi osigurati da se razmatranja rizika uzmu u obzir na odgovarajući način. No odgovornost za donesene odluke trebaju i dalje snositi poslovne i unutarnje jedinice te u konačnici upravljačko tijelo.

20.2 Uloga funkcije upravljanja rizicima u značajnim promjenama

172. U skladu s odjeljkom 18., prije donošenja odluka o značajnim promjenama ili izvanrednim transakcijama, RMF se treba uključiti u procjenu učinka takvih promjena i izvanrednih transakcija na cjelokupan rizik institucije i grupe te treba izravno izvijestiti upravljačko tijelo o svojim nalazima prije nego što se donese odluka.
173. RMF treba procijeniti kako utvrđeni rizici mogu utjecati na sposobnost institucije ili grupe da upravljaju svojim profilom rizičnosti, likvidnošću i dobrom kapitalnom osnovom u normalnim i nepovoljnim okolnostima.

20.3 Uloga funkcije upravljanja rizicima u utvrđivanju, mjerenju, procjeni, smanjenju i praćenju rizika te upravljanju i izvješćivanju o njima

174. RMF treba osigurati da se svi rizici utvrde, procijene, izmjere i prate, da se njima upravlja i da se o njima propisno izvješćuju nadležne jedinice u instituciji.
175. RMF treba osigurati da se utvrđivanje i procjena ne temelje samo na kvantitativnim informacijama ili ishodima modela te treba uzeti u obzir i kvalitativne pristupe. RMF treba osigurati stalnu informiranost upravljačkog tijela o pretpostavkama upotrijebljenima u modelima i analizi rizika te o mogućim nedostacima modela i analize rizika.

176. RMF treba osigurati da se provjeravaju transakcije s povezanim stranama te da se utvrde i primjereno procijene rizici koje one donose instituciji.
177. RMF treba osigurati da poslovne jedinice učinkovito prate sve utvrđene rizike.
178. RMF treba redovito pratiti stvarni profil rizičnosti institucije i temeljito ga analizirati u odnosu na strateške ciljeve i sklonost preuzimanju rizika institucije kako bi se upravljačkom tijelu u upravljačkoj funkciji omogućilo donošenje odluka, a upravljačkom tijelu u nadzornoj funkciji propitivanje.
179. RMF treba analizirati kretanja i prepoznati nove rizike ili rizike u nastajanju i povećanja rizika nastala promjenama okolnosti i uvjeta. Treba i redovito provjeravati stvarne ishode rizika u odnosu na prethodne procjene (tj. retroaktivno testiranje) kako bi se procijenila i poboljšala točnost i učinkovitost postupka upravljanja rizicima.
180. RMF treba procijeniti moguće načine smanjenja rizika. U izvješćivanje upravljačkog tijela trebaju biti uključene predložene, odgovarajuće mjere za smanjenje rizika.

20.4 Uloga funkcije upravljanja rizicima u neodobrenim izloženostima

181. RMF treba neovisno procijeniti kršenja sklonosti preuzimanju rizika ili prekoračenja ograničenja rizika (uključujući utvrđivanje uzroka te provedbu pravne i ekonomske analize stvarnog troška zatvaranja, smanjenja ili zaštite od izloženosti u odnosu na potencijalni trošak njezina zadržavanja). RMF treba obavijestiti predmetne poslovne jedinice i upravljačko tijelo te preporučiti moguće ispravke. RMF treba izravno izvijestiti upravljačko tijelo u nadzornoj funkciji kada je kršenje značajno ne dovodeći u pitanje RMF-ovu obvezu izvješćivanja drugih unutarnjih funkcija i odbora.
182. RMF treba imati ključnu ulogu u osiguranju da se odluka o njegovim preporukama donese na odgovarajućoj razini, da relevantne poslovne jedinice postupaju u skladu s njome i da se o njoj izvijesti upravljačko tijelo i, gdje je osnovan, odbor za rizike.

20.5 Osoba odgovorna za rad funkcije upravljanja rizicima

183. Osoba odgovorna za rad RMF-a treba biti odgovorna za pružanje sveobuhvatnih i razumljivih informacija o rizicima i savjetovanje upravljačkog tijela, čime tom tijelu pomaže u razumijevanju cjelokupnog profila rizičnosti institucije. Isto vrijedi i za osobu odgovornu za rad RMF-a matične institucije u pogledu konsolidiranog položaja.
184. Osoba odgovorna za rad RMF-a treba biti dovoljno stručna, neovisna i imati dovoljno visok položaj u hijerarhiji da propituje odluke koje utječu na izloženost institucije rizicima. Kada osoba odgovorna za rad RMF-a nije član upravljačkog tijela, značajne institucije trebaju imenovati neovisnu osobu odgovornu za rad RMF-a koja nije odgovorna za druge funkcije i koja izravno odgovara upravljačkom tijelu. Kada nije primjereno imenovati osobu koja je

posvećena samo ulozi osobe odgovorne za rad RMF-a, pritom uzimajući u obzir načelo razmjernosti kako je utvrđeno u glavi I., ta funkcija može se udružiti s osobom odgovornom za rad funkcije praćenja usklađenosti ili je može obavljati druga osoba na višem položaju pod uvjetom da ne postoji sukob interesa između udruženih funkcija. Ta osoba u svakom slučaju treba imati dostatne ovlasti, uporište i neovisnost (npr. voditelj pravnih poslova).

185. Osoba odgovorna za rad RMF-a treba biti sposobna propitivati odluke rukovodstva institucije i njezina upravljačkog tijela, a razlozi prigovora trebaju se službeno dokumentirati. Ako institucija želi dodijeliti osobi odgovornoj za rad RMF-a pravo veta na odluke (npr. odluku o kreditu ili ulaganju ili postavljanje ograničenja) donesene na razinama nižim od upravljačkog tijela, treba odrediti opseg tog prava veta, eskalacijske ili žalbene postupke i način na koji će upravljačko tijelo biti uključeno.
186. Institucije trebaju uspostaviti ojačani postupak odobrenja odluka za koja je osoba odgovorna za rad RMF-a izrazila negativno mišljenje. Upravljačko tijelo u nadzornoj funkciji treba biti sposobno izravno komunicirati s osobom odgovornom za rad RMF-a o ključnim pitanjima rizika, uključujući kretanja koja možda nisu dosljedna sa sklonošću preuzimanju rizika i strategijom upravljanja rizicima institucije.

21 Funkcija praćenja usklađenosti

187. Institucije trebaju uspostaviti stalnu i učinkovitu funkciju praćenja usklađenosti koja će upravljati rizicima povezanim s usklađenosti te trebaju imenovati osobu odgovornu za tu funkciju za cijelu instituciju (službenik za praćenje usklađenosti ili osoba odgovorna za rad praćenja usklađenosti).
188. Kada nije primjereno imenovati osobu koja je posvećena samo ulozi osobe odgovorne za rad funkcije praćenja usklađenosti, pritom uzimajući u obzir načelo razmjernosti kako je utvrđeno u glavi I., ta funkcija može se udružiti s osobom odgovornom za rad RMF-a ili je može obavljati druga osoba na višem položaju (npr. voditelj pravnih poslova) pod uvjetom da ne postoji sukob interesa između udruženih funkcija.
189. Funkcija praćenja usklađenosti, uključujući osobu odgovornu za rad te funkcije, treba biti neovisna od poslovnih linija i unutarnjih jedinica koje nadzire te imati dostatne ovlasti, uporište i resurse. Uzimajući u obzir kriterije razmjernosti utvrđene u glavi I., toj funkciji može pomagati RMF ili se ona može udružiti s RMF-om ili drugom odgovarajućom funkcijom, npr. odjelom za pravna pitanja ili ljudske resurse.
190. Radnici odgovorni za praćenje usklađenosti treba imati dovoljno znanja, vještina i iskustva u vezi s usklađenošću i povezanim postupcima te treba imati pristup redovitom osposobljavanju.
191. Upravljačko tijelo u nadzornoj funkciji treba nadzirati provedbu dobro dokumentirane politike usklađenosti o kojoj se moraju obavijestiti svi radnici. Institucije trebaju uspostaviti postupak za redovitu procjenu izmjena zakona i propisa primjenjivih na njihove aktivnosti.

192. Funkcija praćenja usklađenosti treba savjetovati upravljačko tijelo o mjerama koje se moraju poduzeti kako bi se osigurala usklađenost s primjenjivim zakonima, pravilima, propisima i standardima te treba procijeniti mogući učinak promjena u pravnom ili regulatornom okruženju na aktivnosti i okvir praćenja usklađenosti institucije.
193. Funkcija praćenja usklađenosti treba osigurati provedbu praćenja usklađenosti u okviru strukturiranog i dobro utvrđenog programa praćenja usklađenosti te treba osigurati pridržavanje politike usklađenosti. Funkcija praćenja usklađenosti treba izvješćivati upravljačko tijelo i po potrebi komunicirati s RMF-om o rizicima povezanim s usklađenošću institucije i upravljanju tim rizicima. Funkcija praćenja usklađenosti i RMF trebaju po potrebi surađivati i razmjenjivati informacije kako bi mogli izvršiti svoje zadaće. Upravljačko tijelo i RMF trebaju uzeti u obzir nalaze funkcije praćenja usklađenosti u procesu odlučivanja.
194. U skladu s odjeljkom 18. ovih smjernica, funkcija praćenja usklađenosti, u bliskoj suradnji s RMF-om i jedinicom za pravne poslove, treba i provjeriti jesu li novi proizvodi i novi postupci u skladu s važećim pravnim okvirom i, po potrebi, sa svim poznatim nadolazećim izmjenama zakonodavstva, propisa i nadzornih zahtjeva.
195. Institucije trebaju poduzeti odgovarajuće mjere protiv unutarnjih ili vanjskih prijevара i kršenja discipline (npr. kršenje unutarnjih postupaka, prekoračenje ograničenja rizika).
196. Institucije trebaju osigurati da njihova društva kćeri i podružnice poduzmu korake kojima će osigurati usklađenost svojeg poslovanja s lokalnim zakonima i propisima. Ako lokalni zakoni i propisi otežavaju primjenu strožih postupaka i sustava za praćenje usklađenosti koje provodi grupa, osobito ako sprečavaju otkrivanje i razmjenu potrebnih informacija među subjektima unutar grupe, društva kćeri i podružnice trebaju o tome obavijestiti službenika za praćenje usklađenosti ili osobu odgovornu za rad funkcije praćenja usklađenosti konsolidirajuće institucije.

22 Funkcija unutarnje revizije

197. Institucije trebaju uspostaviti neovisnu i učinkovitu funkciju unutarnje revizije (IAF), pritom uzimajući u obzir kriterije razmjernosti utvrđene u glavi I., te trebaju imenovati osobu odgovornu za tu funkciju za cijelu instituciju. IAF treba biti neovisan i treba imati dostatne ovlasti, uporište i resurse. Institucije osobito trebaju osigurati da su kvalifikacije radnika IAF-a i resursi IAF-a, osobito revizorski alati i metode analize rizika, primjereni veličini i lokacijama institucije te vrstama, opsegu i složenosti rizika povezanih s poslovnim modelom, aktivnostima, kulturom rizika institucije i njezinom sklonosti preuzimanju rizika.
198. IAF treba biti neovisan od aktivnosti nad kojima se obavlja revizija. Stoga se ne smije udružiti s drugim funkcijama.
199. IAF treba primjenom pristupa koji se temelji na procjeni rizika obaviti neovisnu provjeru i izraziti objektivno uvjerenje o usklađenosti svih aktivnosti i jedinica institucije, uključujući

eksternaliziranih aktivnosti, s politikama i postupcima institucije te vanjskim zahtjevima. U opseg rada IAF-a trebaju ulaziti svi subjekti unutar grupe.

200. IAF ne smije biti uključen u izradu, odabir, uspostavu i uporabu specifičnih politika, mehanizama i postupaka unutarnje kontrole te ograničenja rizika. No to ne bi trebalo spriječiti upravljačko tijelo u nadzornoj funkciji da traži povratne informacije od unutarnje revizije o pitanjima povezanim s rizikom, unutarnjim kontrolama i usklađenošću s primjenjivim pravilima.
201. IAF treba procijeniti je li okvir unutarnje kontrole institucije utvrđen u odjeljku 15. i učinkovit i djelotvoran. IAF osobito treba procijeniti:
- a. prikladnost okvira upravljanja institucije;
 - b. jesu li postojeće politike i postupci prikladni i u skladu s pravnim i regulatornim zahtjevima te sklonošću preuzimanju rizika i strategijom upravljanja rizicima institucije;
 - c. usklađenost postupaka s mjerodavnim zakonima i propisima te odlukama upravljačkog tijela;
 - d. jesu li postupci ispravno i učinkovito provedeni (npr. usklađenost transakcija, razina stvarno nastalih rizika itd.) i
 - e. prikladnost, kvalitetu i učinkovitost provedenih kontrola i izvješćivanja koje obavljaju poslovne jedinice te funkcija upravljanja rizicima i funkcija praćenja usklađenosti.
202. IAF treba osobito provjeriti cjelovitost postupaka kojima se osigurava pouzdanost metoda i tehnika institucije te pretpostavke i izvore informacija upotrijebljene u njezinim internim modelima (npr. modeliranje rizika i računovodstveno mjerenje). Treba procijeniti i kvalitetu i uporabu alata za kvalitativno utvrđivanje i procjenu rizika te poduzetih mjera za smanjenje rizika.
203. IAF treba imati neometan pristup svojoj evidenciji, dokumentima, informacijama i objektima cijele institucije. To uključuje pristup informacijskim sustavima upravljanja te zapisnicima svih odbora i tijela koja donose odluke.
204. IAF se treba pridržavati nacionalnih i međunarodnih profesionalnih standarda. Primjer profesionalnih standarda na koje se to odnosi jesu standardi Instituta internih revizora.
205. Unutarnja revizija treba se provoditi u skladu s planom revizije i detaljnim programom revizije u kojem se primjenjuje pristup koji se temelji na procjeni rizika.
206. Plan unutarnje revizije treba se sastaviti jednom godišnje na temelju godišnjih ciljeva unutarnje revizije i kontrole. Upravljačko tijelo treba odobriti plan unutarnje revizije.

207. Odgovarajuća razina rukovodstva mora provesti formalni postupak daljnjeg praćenja na temelju svih preporuka iz revizije kako bi se osiguralo njihovo učinkovito i pravodobno rješavanje te se izvijestilo o tome.

Glava VI. – Upravljanje kontinuitetom poslovanja

208. Institucije trebaju uspostaviti dobar plan upravljanja kontinuitetom poslovanja kako bi bile sposobne neprekidno poslovati i ograničiti gubitke u slučaju ozbiljnog prekida poslovanja.

209. Institucije mogu uspostaviti posebnu, neovisnu funkciju za kontinuitet poslovanja, npr. u okviru RMF-a²⁶.

210. Poslovanje institucije oslanja se na nekoliko ključnih resursa (npr. IT-sustave, uključujući usluge u oblaku, komunikacijske sustave i objekte). Svrha je upravljanja kontinuitetom poslovanja smanjiti operativne, financijske, pravne, reputacijske i druge značajne posljedice nastale katastrofom ili produženom nedostupnosti tih resursa i posljedičnim prekidom svakodnevnog poslovanja institucije. Ostale mjere upravljanja rizicima mogu biti usmjerene na smanjenje mogućnosti pojave takvih incidenata ili prijenosa njihova financijskog učinka na treće strane (npr. osiguranjem).

211. Kako bi utvrdila dobar plan upravljanja kontinuitetom poslovanja, institucija treba pažljivo analizirati svoju izloženost ozbiljnim prekidima poslovanja i procijeniti (kvantitativno i kvalitativno) njihov potencijalni učinak uporabom unutarnje i/ili vanjske analize podataka i scenarija. Tom analizom trebaju se obuhvatiti sve poslovne linije i unutarnje jedinice, uključujući RMF, te se treba uzeti u obzir njihova međuovisnost. Rezultati analize trebaju pridonijeti utvrđivanju prioriteta i ciljeva institucije u pogledu oporavka.

212. Na temelju prethodno navedene analize institucija treba utvrditi:

- a. planove postupanja u kriznim situacijama i plan kontinuiteta poslovanja kako bi se osiguralo da institucija prikladno reagira na hitne situacije i da može osigurati funkcioniranje svojih najvažnijih poslovnih aktivnosti ako dođe do prekida svakodnevnog poslovanja i
- b. planove oporavka za ključne resurse kako bi se instituciji omogućio oporavak svakodnevnog poslovanja u odgovarajućem roku. Sav rezidualni rizik od mogućih prekida poslovanja treba biti dosljedan sa sklonošću preuzimanju rizika institucije.

213. Plan postupanja u kriznim situacijama, plan kontinuiteta poslovanja i planovi oporavka trebaju se dokumentirati i pažljivo provoditi. Dokumentacija treba biti dostupna svim poslovnim linijama, unutarnjim jedinicama i RMF-u te treba biti pohranjena na sustavima koji su fizički odvojeni i lako dostupni u slučaju kriznih situacija. Treba se pružiti odgovarajuće osposobljavanje. Planove treba redovito testirati i ažurirati. Svi izazovi ili neuspjesi koji se

²⁶ Vidjeti i članak 312. Uredbe (EU) br. 575/2013.

pojave u testiranjima trebaju se dokumentirati i analizirati, a planovi se sukladno tome trebaju preispitati.

Glava VII. – Transparentnost

214. Sve relevantne radnike u cijeloj instituciji treba obavijestiti o strategijama, politikama i postupcima. Radnici institucije trebaju razumjeti politike i postupke koji se odnose na njihove dužnosti i odgovornosti te ih se trebaju pridržavati.

215. Stoga upravljačko tijelo treba jasno i dosljedno obavješćivati relevantne radnike o strategijama i politikama institucije te o njihovim izmjenama, najmanje u mjeri u kojoj je to potrebno za izvršavanje njihovih dužnosti. To se može obaviti pisanim smjernicama, priručnicima ili drugim sredstvima.

216. Kada nadležna tijela na temelju članka 106. stavka 2. Direktive 2013/36/EU od matičnih društava zahtijevaju godišnju objavu opisa njihove pravne strukture te upravljačke i organizacijske strukture grupe institucija, informacijama se trebaju obuhvatiti svi subjekti unutar strukture grupe kako je definirana u Direktivi 2013/34/EU²⁷ i podijeliti po zemlji.

217. Ta objava treba sadržavati najmanje:

- a. pregled unutarnje organizacije institucije i strukture grupe kako je definirana u Direktivi 2013/34/EU i njezinim izmjenama, uključujući glavne linije izvješćivanja i odgovornosti;
- b. sve značajne izmjene od prethodne objave i datum značajne promjene;
- c. nove pravne, upravljačke ili organizacijske strukture;
- d. informacije o strukturi, organizaciji i članovima upravljačkog tijela, uključujući broj njezinih članova i broj neovisnih članova te podatke o spolu i trajanju mandata svakog člana upravljačkog tijela;
- e. ključne odgovornosti upravljačkog tijela;
- f. popis odbora upravljačkog tijela u nadzornoj funkciji i njihov sastav;
- g. pregled politike upravljanja sukobima interesa koji je primjenjiv na institucije i upravljačko tijelo;
- h. pregled okvira unutarnje kontrole i

²⁷ Direktiva 2013/34/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o godišnjim financijskim izvještajima, konsolidiranim financijskim izvještajima i povezanim izvješćima za određene vrste poduzeća, o izmjeni Direktive 2006/43/EZ Europskog parlamenta i Vijeća i o stavljanju izvan snage direktiva Vijeća 78/660/EEZ i 83/349/EEZ (SL L 182, 29.6.2013., str. 19)

- i. pregled okvira upravljanja kontinuitetom poslovanja.

Prilog I. – Aspekti koje treba uzeti u obzir pri razvoju politike internog upravljanja

U skladu s glavom III., pri evidentiranju politika i sustava internog upravljanja institucije trebaju uzeti u obzir aspekte u nastavku.

1. Struktura dioničara
2. Struktura grupe ako je primjenjivo (pravna i funkcionalna struktura)
3. Sastav i funkcioniranje upravljačkog tijela
 - a) kriteriji odabira
 - b) broj, trajanje mandata, rotacija, dob
 - c) neovisni članovi upravljačkog tijela
 - d) izvršni članovi upravljačkog tijela
 - e) neizvršni članovi upravljačkog tijela
 - f) unutarnja raspodjela zadaća ako je primjenjivo
4. Upravljačka struktura i organizacijska shema (s učinkom na grupu ako je primjenjivo)
 - a) specijalizirani odbori
 - i. sastav
 - ii. funkcioniranje
 - b) izvršni odbor ako postoji
 - i. sastav
 - ii. funkcioniranje
5. Nositelji ključnih funkcija
 - a) osoba odgovorna za rad funkcije upravljanja rizicima
 - b) osoba odgovorna za rad funkcije praćenja usklađenosti
 - c) osoba odgovorna za rad funkcije unutarnje revizije
 - d) glavni financijski direktor
 - e) ostali nositelji ključnih funkcija
6. Okvir unutarnje kontrole
 - a) opis svake funkcije, uključujući njezinu organizaciju, resurse, uporište i ovlasti

- b) opis okvira upravljanja rizicima, uključujući strategiju upravljanja rizicima
- 7. Organizacijska struktura (s učinkom na grupu ako je primjenjivo)
 - a) operativna struktura, poslovne linije i raspodjela nadležnosti i odgovornosti
 - b) eksternalizacija
 - c) raspon proizvoda i usluga
 - d) geografski opseg poslovanja
 - e) besplatno pružanje usluga
 - f) podružnice
 - g) društva kćeri, zajednički pothvati itd.
 - h) uporaba izvanteritorijalnih centara
- 8. Kodeks ponašanja i ponašanje (s učinkom na grupu ako je primjenjivo)
 - a) strateški ciljevi i vrijednosti društva
 - b) unutarnji kodeksi i propisi, preventivna politika
 - c) politika upravljanja sukobima interesa
 - d) zviždanje
- 9. Status politike internog upravljanja s datumom
 - a) razvoj
 - b) posljednja izmjena
 - c) posljednja procjena
 - d) odobrenje upravljačkog tijela.