EBA/GL/2021/05

2 juli 2021

Richtsnoeren

inzake interne governance

1. Nalevings- en rapportageverplichtingen

Status van deze richtsnoeren

1. Deze richtsnoeren zijn uitgebracht op grond van artikel 16 van Verordening (EU) nr. 1093/2010 [1]. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 moeten bevoegde autoriteiten en financiële instellingen, met inbegrip van instellingen, zich tot het uiterste inspannen om aan de richtsnoeren te voldoen.

2. Richtsnoeren geven weer wat in de opvatting van EBA passende toezichtpraktijken binnen het Europees Systeem voor financieel toezicht zijn en hoe het recht van de Unie op een specifiek gebied dient te worden toegepast. Bevoegde autoriteiten als bedoeld in artikel 4, lid 2, van Verordening (EU) nr. 1093/2010 voor wie richtsnoeren gelden, dienen hieraan te voldoen door deze op passende wijze in hun praktijken te integreren (bijv. door hun wettelijk kader of hun toezichtprocessen aan te passen), ook wanneer richtsnoeren primair tot instellingen zijn gericht.

Rapportageverplichtingen

3. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 stellen bevoegde autoriteiten de EBA er vóór (05.12.2021) van in kennis of zij aan deze richtsnoeren voldoen of voornemens zijn deze op te volgen, of, indien dit niet het geval is, wat de redenen van de niet-naleving zijn. Bevoegde autoriteiten die bij het verstrijken van de termijn niet hebben gereageerd, worden geacht niet te hebben voldaan aan de richtsnoeren. Kennisgevingen worden ingediend door het formulier op de EBA-website te versturen naar onder vermelding van “EBA/GL/2021/05”. Kennisgevingen worden ingediend door personen die bevoegd zijn om namens hun bevoegde autoriteit te melden of zij aan de richtsnoeren voldoen. Elke verandering in de status van de naleving dient eveneens aan EBA te worden gemeld.

4. Kennisgevingen worden overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 2093/2010 op de website van EBA bekendgemaakt.

[1] Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12).

2. Onderwerp, toepassingsgebied en definities

Onderwerp

5. Deze richtsnoeren geven een nadere specificatie van de regelingen, procedures en mechanismen voor interne governance die instellingen die onderworpen zijn aan Richtlijn 2013/36/EU [2] en beleggingsondernemingen die onderworpen zijn aan titel VII van Richtlijn 2013/36/EU bij de toepassing van artikel 1, leden 2 en 5, van Verordening 2019/2033/EU ten uitvoer moeten leggen overeenkomstig artikel 74, lid 1, van Richtlijn 2013/36/EU ter waarborging van hun doeltreffend en prudent bestuur.

Geadresseerden

Deze richtsnoeren zijn gericht tot bevoegde autoriteiten zoals gedefinieerd in artikel 4, punt 2, onder i), van Verordening (EU) 1093/2010 en tot financiële instellingen zoals gedefinieerd in artikel 4, lid 1, van Verordening (EU) 1093/2010 die hetzij instellingen zijn voor de toepassing van Richtlijn 2013/36/EU zoals gedefinieerd in artikel 3, lid 1, punt 3, van Richtlijn 2013/36/EU in samenhang met artikel 3, lid 3, van die richtlijn, of beleggingsondernemingen die onderworpen zijn aan titel VII van Richtlijn 2013/36/EU voor de toepassing van artikel 1, leden 2 en 5, van Verordening 2019/2033/EU ("instellingen").

Toepassingsgebied

6. Deze richtsnoeren gelden voor governanceregelingen van instellingen, met inbegrip van hun organisatiestructuur en de bijbehorende verantwoordelijkheidslijnen, procedures voor de detectie, het beheer, de bewaking en de rapportage van alle risico's[3] waaraan zij blootstaan of bloot kunnen komen te staan, en het kader voor interne controle.

7. De richtsnoeren beogen betrekking te hebben op alle bestaande bestuursmodellen zonder een bepaald model voor te staan. De richtsnoeren laten de algemene bevoegdheidsverdeling overeenkomstig nationaal vennootschapsrecht onverlet. Zij dienen dan ook ongeacht het gebruikte bestuursmodel (monistisch en/of dualistisch bestuursmodel en/of een ander model) te worden toegepast in de lidstaten. Het leidinggevend orgaan, als gedefinieerd in

[2] Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen en beleggingsondernemingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van de Richtlijnen 2006/48/EG en 2006/49/EG (PB L 176 van 27.6.2013, blz. 338).

[3] Waar in deze richtsnoeren wordt verwezen naar risico's, wordt ook verwezen naar witwassen van geld en financiering van terrorisme.

artikel 3, lid 1, punten 7 en 8, van Richtlijn 2013/36/EU, dient te worden opgevat als een orgaan met leidinggevende (uitvoerende) en toezichthoudende (niet-uitvoerende) functies[4].

8. De termen 'leidinggevend orgaan in zijn bestuursfunctie' en 'leidinggevend orgaan in zijn toezichtfunctie' worden in deze richtsnoeren gebruikt zonder te refereren aan een specifieke governancestructuur, en verwijzingen naar de leidinggevende (uitvoerende) of toezichthoudende (niet-uitvoerende) functie dienen te worden opgevat als geldend voor de organen of leden van het leidinggevend orgaan die verantwoordelijk zijn voor die functie overeenkomstig het nationale recht. Bij de tenuitvoerlegging van deze richtsnoeren houden bevoegde autoriteiten rekening met hun nationaal vennootschapsrecht en specificeren zij, waar noodzakelijk, op welk orgaan of op welke leden van het leidinggevend orgaan die functies van toepassing zijn.

9. In lidstaten waarin het leidinggevend orgaan de uitvoerende functies geheel of gedeeltelijk delegeert aan een persoon of een intern uitvoerend orgaan (bijvoorbeeld aan een chief executive officer (CEO), managementteam of bestuur), dienen de personen die die uitvoerende functies op basis van die delegering uitvoeren, te worden beschouwd als vormden zij de bestuursfunctie van het leidinggevend orgaan. In deze richtsnoeren vallen, in geval van verwijzing naar het leidinggevend orgaan in zijn bestuursfunctie, daar ook de leden van het uitvoerend orgaan of de CEO onder, zoals gedefinieerd in deze richtsnoeren, ook al zijn zij niet voorgesteld of benoemd als formele leden van het bestuurslichaam of de bestuurslichamen van de instelling op grond van het nationale recht.

10. In lidstaten waar bepaalde verantwoordelijkheden rechtstreeks worden uitgeoefend door aandeelhouders, leden of eigenaren van de instelling in plaats van door het leidinggevend orgaan, dienen instellingen te waarborgen dat dergelijke verantwoordelijkheden en bijbehorende besluiten zoveel mogelijk in overeenstemming zijn met de richtsnoeren die gelden voor het leidinggevend orgaan.

11. De definities van CEO, chief financial officer (CFO) en medewerker met een sleutelfunctie die in deze richtsnoeren worden gebruikt, zijn louter functioneel en zijn niet bedoeld om de benoeming van deze functionarissen of de totstandbrenging van dergelijke functies op te leggen, tenzij dit is voorgeschreven door relevante EU- of nationale wetgeving.

12. Instellingen dienen te voldoen aan deze richtsnoeren en bevoegde autoriteiten dienen ervoor te zorgen dat instellingen voldoen aan deze richtsnoeren op een individuele, gesubconsolideerde en geconsolideerde basis overeenkomstig het toepassingsniveau dat is vastgelegd in artikel 109 van Richtlijn 2013/36/EU.

[4] Zie ook overweging 56 van Richtlijn 2013/36/EU.

Definities

13. Tenzij anders aangegeven hebben de termen die in Richtlijn 2013/36/EU en in Verordening (EU) nr. 575/2013 worden gebruikt en gedefinieerd, in deze richtsnoeren dezelfde betekenis. In deze richtsnoeren gelden bovendien de volgende definities:

Risicobereidheid	het totale risiconiveau en de soorten risico's die een instelling binnen haar risicodraagkracht en overeenkomstig haar bedrijfsmodel bereid is te nemen om haar strategische doelen te bereiken.
Risicodraagkracht	het maximale risiconiveau dat een instelling in staat is op zich te nemen gegeven haar kapitaalbasis, haar capaciteiten op het gebied van risicobeheer en -beheersing, en haar wettelijke beperkingen.
Risicocultuur	de normen, de attitudes en het gedrag van een instelling met betrekking tot risicobewustzijn, het nemen van risico's en risicobeheer, en de controlemaatregelen die besluiten over risico's vormgeven. De risicocultuur beïnvloedt de besluiten van leidinggevenden en werknemers tijdens de dagelijkse activiteiten en is van invloed op de risico's die zij aangaan.
Personeel	alle werknemers van een instelling en haar dochterondernemingen die onder de consolidatie vallen, met inbegrip van dochterondernemingen die niet zijn onderworpen aan Richtlijn 2013/36/EU, en alle leden van het leidinggevend orgaan in zijn bestuursfunctie en in zijn toezichtfunctie.
Chief executive officer (CEO)	de persoon die verantwoordelijk is voor het beheren en aansturen van het geheel aan bedrijfsactiviteiten van een instelling.
Chief financial officer (CFO)	de persoon die algemeen verantwoordelijk is voor het beheer van elk van de volgende activiteiten: beheer van financiële middelen, financiële planning en financiële verslaglegging.
Hoofden interne controlefuncties	de personen op het hoogste hiërarchische niveau die belast zijn met het daadwerkelijke beheer van de dagelijkse activiteiten van de onafhankelijke risicobeheersfunctie, de nalevingsfunctie en de interne auditfunctie.
Medewerkers met een sleutelfunctie	personen die een aanzienlijke invloed hebben op de leiding over de instelling, maar die geen lid van het leidinggevend orgaan zijn en ook niet de CEO zijn. Daartoe behoren onder meer de hoofden van interne controlefuncties en de CFO, als die geen lid van het leidinggevend orgaan zijn, en andere medewerkers met een sleutelfunctie, wanneer die door instellingen met behulp van een op risico gebaseerde aanpak zijn geïdentificeerd.

	Andere medewerkers met een sleutelfunctie kunnen zijn: hoofden van belangrijke bedrijfsonderdelen, vestigingen in de Europese Economische Ruimte/Europese Vrijhandelsassociatie, dochterondernemingen in derde landen en andere interne functies.
Prudentiële consolidatie	de toepassing van de prudentiële voorschriften als vastgelegd in Richtlijn 2013/36/EU en Verordening (EU) nr. 575/2013 op geconsolideerde of gesubconsolideerde basis, overeenkomstig deel één, titel II, hoofdstuk 2, van Verordening (EU) nr. 575/2013[5].
Loonkloof tussen mannen en vrouwen	het verschil tussen het gemiddelde bruto-uurloon van mannen en dat van vrouwen, uitgedrukt als percentage van het gemiddelde bruto-uurloon van mannen.
Consoliderende instelling	een instelling die verplicht is aan de prudentiële vereisten te voldoen op basis van de geconsolideerde situatie, overeenkomstig deel één, titel II, hoofdstuk 2, van Verordening (EU) nr. 575/2013.
Significante instellingen	instellingen als bedoeld in artikel 131 van Richtlijn 2013/36/EU (mondiaal systeemrelevante instellingen (MSI's) en andere systeemrelevante instellingen (ASI's)), alsmede eventuele andere instellingen als bepaald door de bevoegde autoriteit of het nationale recht op basis van een beoordeling van de omvang en de interne organisatie van de instellingen en de aard, omvang en complexiteit van hun activiteiten.
Beursgenoteerde instelling	een instelling waarvan de financiële instrumenten in een of meer lidstaten zijn toegelaten tot handel op een gereglementeerde markt of op een multilaterale handelsfaciliteit zoals gedefinieerd in artikel 4, lid 1, punten 21 en 22, van Richtlijn 2014/65/EU[6].
Aandeelhouder	een persoon die aandelen in een instelling bezit, of, afhankelijk van de rechtsvorm van een instelling, andere eigenaren of leden van de instelling.
Bestuursfunctie	een functie als lid van het leidinggevend orgaan van een instelling of een andere rechtspersoon.

[5] Zie ook de technische reguleringsnormen inzake prudentiële consolidatie op: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2021/973355/Final%20Report%20Draft%20RTS%20methods%20of%20consolidation.pdf

[6] Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU (PB L 173 van 12.6.2014, blz. 349).

3. Uitvoering

Ingangsdatum

14. Deze bijgewerkte richtsnoeren gelden met ingang van 31 december 2021.

Intrekking

15. De EBA-richtsnoeren inzake interne governance (EBA/GL/2017/11) van 26 september 2017 worden per 31 december 2021 ingetrokken.

4. Richtsnoeren

Titel I – Evenredigheid

16. Het evenredigheidsbeginsel dat is vastgelegd in artikel 74, lid 2, van Richtlijn 2013/36/EU heeft als doel te waarborgen dat regelingen voor interne governance consistent zijn met het individuele risicoprofiel en bedrijfsmodel van de instelling, zodat de doelstellingen van de regelgevingsvereisten en -bepalingen doeltreffend worden bereikt.

17. Instellingen dienen, wanneer zij regelingen voor interne governance ontwikkelen en ten uitvoer leggen, rekening te houden met hun omvang en interne organisatie, en met de aard, schaal en complexiteit van hun activiteiten. Significante instellingen dienen geavanceerdere governanceregelingen te hebben, terwijl kleine en minder complexe instellingen eenvoudiger governanceregelingen ten uitvoer kunnen leggen. Instellingen dienen er evenwel rekening mee te houden dat de omvang of het systeembelang van een instelling op zichzelf niet per se indicatief is voor de mate waarin die instelling aan risico's blootstaat.

18. Ten behoeve van de toepassing van het evenredigheidsbeginsel en om een passende tenuitvoerlegging van de regelgevingsvereisten en deze richtsnoeren te waarborgen, dienen instellingen en bevoegde autoriteiten rekening te houden met alle onderstaande aspecten:

    a. de omvang in termen van het balanstotaal van de instelling en haar dochterondernemingen die onder de prudentiële consolidatie vallen;

    b. de geografische aanwezigheid van de instelling en de omvang van haar werkzaamheden in elk rechtsgebied;

    c. de rechtsvorm van de instelling, evenals de vraag of de instelling deel uitmaakt van een groep, en zo ja, de voor de groep uitgevoerde evenredigheidsbeoordeling;

    d. of de instelling een beursgenoteerde instelling is;

    e. of de instelling toestemming heeft interne modellen te gebruiken voor het meten van de kapitaalvereisten (bijv. de interneratingbenadering);

    f. het type toegestane activiteiten en diensten dat de instelling verricht (zie bijvoorbeeld ook bijlage I bij Richtlijn 2013/36/EU en bijlage I bij Richtlijn 2014/65/EU);

    g. het onderliggende bedrijfsmodel en de onderliggende bedrijfsstrategie; de aard en complexiteit van de bedrijfsactiviteiten, en de organisatiestructuur van de instelling;

h. de risicostrategie, de risicobereidheid en het werkelijke risicoprofiel van de instelling, waarbij ook rekening wordt gehouden met het resultaat van de SREP-kapitaal- en SREP-liquiditeitsbeoordelingen;

i. de eigendoms- en financieringsstructuur van de instelling;

j. het type cliënten (bijv. detailhandel, bedrijven, mkb/kmo's, institutionele cliënten, overheden) en de complexiteit van de producten of contracten;

k. de uitbestede functies en distributiekanalen;

l. de bestaande IT-systemen, met inbegrip van continuïteitssystemen en uitbestedingsfuncties op dit gebied, en

m. of de instelling valt onder de definitie van een kleine en niet-complexe instelling of een grote instelling in artikel 4, lid 1, punten 145 en 146 van Verordening (EU) nr. 575/2013.

Titel II – Rol en samenstelling van het leidinggevend orgaan en comités

1 Rol en verantwoordelijkheden van het leidinggevend orgaan

19. Overeenkomstig artikel 88, lid 1, van Richtlijn 2013/36/EU draagt het leidinggevend orgaan de uiteindelijke en algemene verantwoordelijkheid voor de instelling en stelt het governanceregelingen op, houdt het daar toezicht op en legt het verantwoording af voor de uitvoering ervan binnen de instelling; deze regelingen garanderen een doeltreffend en prudent bestuur van een instelling.

20. De taken van het leidinggevend orgaan dienen duidelijk omschreven te zijn, waarbij een onderscheid wordt gemaakt tussen de taken van de bestuursfunctie (uitvoerend) en de toezichthoudende functie (niet-uitvoerend). De verantwoordelijkheden en taken van het leidinggevend orgaan dienen te worden omschreven in een schriftelijk document en naar behoren te zijn goedgekeurd door het leidinggevend orgaan. Alle leden van het leidinggevend orgaan dienen volledig op de hoogte te zijn van de structuur en verantwoordelijkheden van het leidinggevend orgaan, en van de taakverdeling tussen verschillende functies van het leidinggevend orgaan en zijn comités.

21. Er dient een doeltreffende interactie te zijn tussen het leidinggevend orgaan in zijn toezichtfunctie en het leidinggevend orgaan in zijn bestuursfunctie. Beide functies behoren elkaar voldoende informatie te verstrekken om hun respectieve taken te kunnen uitvoeren. Met het oog op passende controlemechanismen dient de besluitvorming binnen het leidinggevend orgaan niet te worden gedomineerd door één lid of een kleine groep leden.

22. Tot de verantwoordelijkheden van het leidinggevend orgaan dienen te behoren: de vaststelling, de goedkeuring en het toezicht op de uitvoering van

    a. de algemene bedrijfsstrategie en de belangrijkste beleidsmaatregelen van de instelling binnen het toepasselijke wet- en regelgevingskader, rekening houdend met de financiële belangen en solvabiliteit van de instelling op de lange termijn;

    b. de algehele risicostrategie, de risicobereidheid van de instelling en haar kader voor risicobeheer en maatregelen die ervoor moeten zorgen dat het leidinggevend orgaan voldoende tijd besteedt aan kwesties omtrent risico's en risicobeheer;

    c. een toereikend en doeltreffend kader voor interne governance en interne controle, zoals gedefinieerd in titel V, dat:

        i. een heldere organisatiestructuur omvat evenals goed functionerende onafhankelijke interne risicobeheers-, nalevings- en auditfuncties met voldoende gezag, status en middelen om hun functies te vervullen;

        ii. de naleving waarborgt van de toepasselijke regelgevingsvereisten in verband met het voorkomen van het witwassen van geld en terrorismefinanciering;

    d. de hoeveelheid, typen en verdeling van intern kapitaal en toetsingsvermogen om de risico's van de instelling voldoende te dekken;

    e. doelen voor het liquiditeitsbeheer van de instelling;

    f. een beloningsbeleid dat in overeenstemming is met de beginselen die worden uiteengezet in de artikelen 92 tot en met 95 van Richtlijn 2013/36/EU en de EBA-richtsnoeren betreffende een degelijk beloningsbeleid krachtens artikel 74, lid 3, en artikel 75, lid 2, van Richtlijn 2013/36/EU[7];

    g. regelingen die ervoor moeten zorgen dat de individuele en collectieve geschiktheidsbeoordelingen van het leidinggevend orgaan doeltreffend worden uitgevoerd, dat de samenstelling en het opvolgingsplan van het leidinggevend orgaan passend zijn, en dat het leidinggevend orgaan zijn functies doeltreffend vervult[8];

    h. een selectie- en geschiktheidsbeoordelingsproces voor medewerkers met een sleutelfunctie[9];

[7] EBA-richtsnoeren betreffende een beheerst beloningsbeleid

[8] Zie ook de gezamenlijke ESMA- en EBA-richtsnoeren voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie.

[9] Zie ook de gezamenlijk ESMA- en EBA-richtsnoeren voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie.

i. regelingen die ervoor moeten zorgen dat het intern functioneren van elk ingesteld comité van het leidinggevend orgaan gewaarborgd is, door een specifieke beschrijving te geven van:

    i. de rol, samenstelling en taken van elk comité;

    ii. de passende informatiestroom, met inbegrip van de documentatie van aanbevelingen en conclusies, en rapportagelijnen tussen elk comité en het leidinggevend orgaan, bevoegde autoriteiten en andere partijen;

j. een risicocultuur overeenkomstig hoofdstuk 9 van deze richtsnoeren, waarin aandacht wordt geschonken aan het risicobewustzijn en het risicogedrag van de instelling;

k. een bedrijfscultuur en waarden overeenkomstig hoofdstuk 10, die verantwoordelijk en ethisch gedrag bevorderen, met inbegrip van een gedragscode of soortgelijk instrument;

l. een beleid inzake belangenconflicten op institutioneel niveau overeenkomstig hoofdstuk 11 en voor personeel overeenkomstig hoofdstuk 12; en

m. regelingen die zijn gericht op het waarborgen van de integriteit van de systemen voor boekhoudkundige en financiële verslaglegging, met inbegrip van de financiële en operationele controle en de naleving van de wetgeving en de toepasselijke normen.

23. Bij het vaststellen, goedkeuren en toezicht houden op de uitvoering van de in punt 22 opgesomde aspecten dient het leidinggevend orgaan te streven naar een bedrijfsmodel en governanceregelingen, met inbegrip van een risicobeheerkader, waarin met alle risico's rekening wordt gehouden. Bij het inventariseren van alle risico's waaraan zij zijn blootgesteld, dienen instellingen alle relevante risicofactoren in aanmerking te nemen, met inbegrip van milieutechnische, maatschappelijke en governancegerelateerde risicofactoren. Instellingen moeten er op bedacht zijn dat die laatste risicofactoren tot verhoogde prudentiële risico's kunnen leiden, bijv. via risicofactoren in verband met de transitie naar een duurzame economie of met externe fysieke klimaatgerelateerde gebeurtenissen die nadelige gevolgen kunnen hebben voor debiteuren, de markt, liquiditeit of operationele risico's, maar ook tot verhoogde reputatierisico's, bijv. via maatschappelijke of governancegerelateerde risicofactoren, zoals in verband met uitbestedingsregelingen[10]. Voorbeelden van dergelijke risico's zijn juridische (verbintenisrechtelijke of arbeidsrechtelijke) risico's, risico's in verband met mogelijke mensenrechtenschendingen of andere ESG-risicofactoren die van invloed kunnen zijn op het land waar een dienstverlener is gevestigd en op het vermogen van die dienstverlener om het overeengekomen niveau van de dienstverlening te waarborgen.

[10] Zie het EBA-verslag over het beheer van en toezicht op ESG-risico's, uitgebracht overeenkomstig artikel 98, lid 8, van de RKV, voor een beschrijving van de visie van EBA op ESG-risico's, transmissiekanalen en aanbevelingen voor regelingen, procedures, mechanismen en strategieën die de instellingen ten uitvoer moeten leggen om ESG-risico's te bepalen, te beoordelen en te beheren.

24. Het leidinggevend orgaan moet toezicht houden op het proces van het bekendmaken van gegevens en het communiceren met externe belanghebbenden en bevoegde autoriteiten.

25. Alle leden van het leidinggevend orgaan behoren op de hoogte te zijn van de algemene bedrijfsactiviteiten, de financiële situatie en de risicosituatie van de instelling, waarbij rekening wordt gehouden met het economische klimaat, en van besluiten die zijn genomen die een belangrijke impact hebben op de activiteiten van de instelling.

26. Een lid van het leidinggevend orgaan kan verantwoordelijk zijn voor een interne controlefunctie zoals vermeld in titel V, paragraaf 19.1, mits het lid geen andere mandaten heeft die de interne controleactiviteiten van het lid en de onafhankelijkheid van de interne controlefunctie in opspraak zouden brengen.

27. Het leidinggevend orgaan dient eventuele geïdentificeerde zwakke punten in de tenuitvoerlegging van processen, strategieën en beleid met betrekking tot de in de punten 22 en 23 genoemde verantwoordelijkheden te bewaken, periodiek te evalueren en aan te pakken. Het kader voor interne governance en de tenuitvoerlegging daarvan dienen periodiek te worden getoetst en geactualiseerd, rekening houdend met het evenredigheidsbeginsel, zoals verder toegelicht in titel I. Wanneer een instelling te maken krijgt met belangrijke veranderingen, dient een grondiger toetsing te worden uitgevoerd.

2 De bestuursfunctie van het leidinggevend orgaan

28. Het leidinggevend orgaan in zijn bestuursfunctie dient actief betrokken te zijn bij de activiteiten van een instelling en besluiten te nemen op grond van goede kennis van zaken.

29. Het leidinggevend orgaan in zijn bestuursfunctie behoort verantwoordelijk te zijn voor de tenuitvoerlegging van de strategieën die het leidinggevend orgaan heeft vastgesteld en dient de tenuitvoerlegging en passendheid van die strategieën regelmatig te bespreken met het leidinggevend orgaan in zijn toezichtfunctie. De operationele tenuitvoerlegging kan door de directie van de instelling worden verricht.

30. Het leidinggevend orgaan in zijn bestuursfunctie dient voorstellen, toelichtingen en ontvangen informatie op constructieve wijze ter discussie te stellen en deze kritisch te beoordelen wanneer het een oordeel velt en besluiten neemt. Het leidinggevend orgaan in zijn bestuursfunctie dient aan het leidinggevend orgaan in zijn toezichtfunctie uitvoerig verslag uit te brengen van, en dit orgaan indien nodig zonder onnodig uitstel te informeren over, de relevante elementen voor de beoordeling van een situatie, de risico's en ontwikkelingen die van invloed zijn of kunnen zijn op de instelling, bijv. belangrijke besluiten inzake bedrijfsactiviteiten en genomen risico's, de evaluatie van het economische en bedrijfsklimaat van de instelling, haar liquiditeit en solide kapitaalbasis, en de beoordeling van haar belangrijke risicoblootstellingen.

31. Onverminderd de verplichting om Richtlijn 2015/849/EU om te zetten in nationaal recht dient het leidinggevend orgaan overeenkomstig de vereisten van artikel 46, lid 4, van Richtlijn

2015/849/EU (de antiwitwasrichtlijn) te bepalen wie van haar leden verantwoordelijk is voor de uitvoering van de wettelijke en bestuursrechtelijke bepalingen die nodig zijn voor de naleving van deze richtlijn, met inbegrip van de overeenkomstige AML/CFT-beleidsvoorschriften en -procedures binnen de instelling en op het niveau van het leidinggevend orgaan[11].

3 Toezichthoudende functie van het leidinggevend orgaan

32. De rol van de leden van het leidinggevend orgaan in zijn toezichtfunctie dient mede uit monitoring en een constructieve maar kritische opstelling ten aanzien van de strategie van de instelling te bestaan.

33. Onverminderd het nationale recht dient het leidinggevend orgaan in zijn toezichtfunctie onafhankelijke leden te bevatten zoals bepaald in paragraaf 9.3 van de gemeenschappelijke ESMA- en EBA-richtsnoeren voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie uit hoofde van Richtlijn 2013/36/EU en Richtlijn 2014/65/EU.

34. Onverminderd de verantwoordelijkheden die hem zijn toegekend overeenkomstig het toepasselijke nationale vennootschapsrecht, dient het leidinggevend orgaan in zijn toezichtfunctie:

    a. toe te zien en controle uit te oefenen op de bestuurlijke besluitvorming en acties en doeltreffend toezicht uit te oefenen op het leidinggevend orgaan in zijn bestuursfunctie, zoals het toezicht houden op en het toetsen van zijn individuele en collectieve prestaties en van de tenuitvoerlegging van de strategie en doelstellingen van de instelling;

    b. voorstellen en informatie van leden van het leidinggevend orgaan in zijn bestuursfunctie, evenals zijn besluiten, ter discussie te stellen en kritisch te evalueren;

    c. rekening houdend met het evenredigheidsbeginsel zoals uiteengezet in titel I, naar behoren de taken en rol van het risico-, benoemings- en beloningscomité te vervullen, wanneer dergelijke comités niet zijn opgericht;

    d. de doeltreffendheid van het kader voor interne governance van de instelling te waarborgen en periodiek te beoordelen en passende stappen te ondernemen om eventuele vastgestelde tekortkomingen aan te pakken;

    e. erop toe te zien en te monitoren dat de strategische doelstellingen, de organisatiestructuur en de risicostrategie van de instelling, haar risicobereidheid en

[11] Het leidinggevend orgaan blijft als collegiaal orgaan in zijn geheel verantwoordelijk.

kader voor risicobeheer, evenals ander beleid (bijv. beloningsbeleid) en het kader met betrekking tot openbaarmaking, consistent worden toegepast;

f. erop toe te zien dat de risicocultuur van de instelling consistent wordt toegepast;

g. erop toe te zien dat een gedragscode of een soortgelijke code en doeltreffend beleid voor het identificeren, beheren en beperken van feitelijke en potentiële belangenconflicten ten uitvoer wordt gelegd en wordt gehandhaafd;

h. toe te zien op de integriteit van financiële informatie en verslaglegging, en het kader voor interne controle, met inbegrip van een doeltreffend en solide kader voor risicobeheersing;

i. te waarborgen dat de hoofden van interne controlefuncties onafhankelijk kunnen handelen en, ongeacht de verantwoordelijkheid om te rapporteren aan andere interne organen, bedrijfsonderdelen of -eenheden, hun bezorgdheid kenbaar kunnen maken en het leidinggevend orgaan in zijn toezichtfunctie zo nodig rechtstreeks kunnen waarschuwen, wanneer ongunstige risico-ontwikkelingen een negatieve invloed op de instelling hebben of kunnen hebben; en

j. toe te zien op de tenuitvoerlegging van het interne-auditplan, nadat eerst de risico- en auditcomités erbij zijn betrokken, indien dergelijke comités zijn opgericht.

4 De rol van de voorzitter van het leidinggevend orgaan

35. De voorzitter van het leidinggevend orgaan behoort leiding te geven aan het leidinggevend orgaan, bij te dragen aan een doeltreffende informatiestroom binnen het leidinggevend orgaan en tussen het leidinggevend orgaan en zijn comités, indien die zijn opgericht, en verantwoordelijk te zijn voor het algehele doeltreffende functioneren.

36. De voorzitter dient een open en kritische discussie aan te moedigen en te bevorderen en ervoor te zorgen dat afwijkende meningen in het besluitvormingsproces kunnen worden geuit en bespreekbaar zijn.

37. Als algemeen principe geldt dat de voorzitter van het leidinggevend orgaan een niet-uitvoerend lid dient te zijn. Wanneer het de voorzitter is toegestaan uitvoerende taken op zich te nemen, dient de instelling maatregelen te treffen om een eventueel nadelig effect op de controlemechanismen van de instelling te verminderen (bijv. door een leidend lid van de raad van bestuur of een senior onafhankelijk lid van de raad van bestuur aan te wijzen, of door een groter aantal niet-uitvoerende leden in het leidinggevend orgaan in zijn toezichtfunctie op te nemen). Met name dient, overeenkomstig artikel 88, lid 1, onder e), van Richtlijn 2013/36/EU, de voorzitter van het leidinggevend orgaan in zijn toezichtfunctie van een instelling, niet tegelijkertijd de functie van CEO binnen dezelfde instelling te bekleden, tenzij dat door de instelling is gerechtvaardigd en door de bevoegde autoriteiten is toegestaan.

38. De voorzitter dient de agenda's van vergaderingen vast te stellen en ervoor te zorgen dat strategische kwesties met voorrang worden besproken. Hij of zij dient te waarborgen dat besluiten van het leidinggevend orgaan worden genomen op grond van goede kennis van zaken en dat documenten en informatie ruim vóór de vergadering worden ontvangen.

39. De voorzitter van het leidinggevend orgaan dient bij te dragen aan een duidelijke verdeling van taken tussen leden van het leidinggevend orgaan en aan een doeltreffende informatiestroom tussen hen, teneinde de leden van het leidinggevend orgaan in zijn toezichtfunctie in staat te stellen een constructieve bijdrage te leveren aan discussies en om een op goede informatie gefundeerde stem uit te brengen.

5 Comités van het leidinggevend orgaan in zijn toezichtfunctie

5.1 Instellen van comités

40. Overeenkomstig artikel 109, lid 1, van Richtlijn 2013/36/EU in samenhang met de artikelen 76, lid 3, 88, lid 2, en 95, lid 1, van Richtlijn 2013/36/EU, stellen alle instellingen die zelf significant zijn, rekening houdend met het individuele, gesubconsolideerde en geconsolideerde niveau, risico-, benoemings- [12] en beloningscomités [13] in om het leidinggevend orgaan in zijn toezichtfunctie te adviseren en om de besluiten die dit orgaan moet nemen, voor te bereiden. Niet-significante instellingen, ook wanneer zij onder de prudentiële consolidatie vallen van een instelling die significant is in een gesubconsolideerde of geconsolideerde situatie, zijn niet verplicht deze comités in te stellen.

41. Wanneer geen risico- of benoemingscomité is ingesteld, dienen de verwijzingen in deze richtsnoeren naar deze comités te worden opgevat als zijnde van toepassing op het leidinggevend orgaan in zijn toezichtfunctie, rekening houdend met het evenredigheidsbeginsel zoals uiteengezet in titel I.

42. Instellingen kunnen, rekening houdend met de criteria die worden uiteengezet in titel I van deze richtsnoeren, andere comités instellen (bijv. comités ter bestrijding van witwaspraktijken of terrorismefinanciering (AML/CTF), en comités op het gebied van ethiek, gedrag of naleving).

43. Instellingen dienen te zorgen voor een duidelijke toewijzing en verdeling van plichten en taken tussen gespecialiseerde comités van het leidinggevend orgaan.

44. Elk comité dient te beschikken over een schriftelijk mandaat (waarin ook zijn verantwoordelijkheden zijn vastgelegd) van het leidinggevend orgaan in zijn toezichtfunctie, en stelt passende werkprocedures vast.

[12] Zie ook de gemeenschappelijke ESMA- en EBA-richtsnoeren voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie uit hoofde van Richtlijn 2013/36/EU en Richtlijn 2014/65/EU.

[13] Raadpleeg voor meer informatie aangaande het beloningscomité de EBA-richtsnoeren betreffende een beheerst beloningsbeleid.

45. Comités behoren de toezichthoudende functie op specifieke gebieden te ondersteunen en de ontwikkeling en uitvoering van een solide kader voor interne governance te bevorderen. Het delegeren van taken aan comités ontslaat het leidinggevend orgaan in zijn toezichtfunctie geenszins van zijn verplichting om collectief zijn taken en verantwoordelijkheden te vervullen.

5.2 Samenstelling van comités[14]

46. Alle comités dienen te worden voorgezeten door een niet-uitvoerend lid van het leidinggevend orgaan dat in staat is een objectief oordeel te vellen.

47. Onafhankelijke leden[15] van het leidinggevend orgaan in zijn toezichtfunctie dienen actief betrokken te zijn bij comités.

48. Wanneer overeenkomstig Richtlijn 2013/36/EU of het nationale recht comités moeten worden ingesteld, dienen deze uit ten minste drie leden te bestaan.

49. Instellingen dienen ervoor te zorgen, rekening houdend met de omvang van het leidinggevend orgaan en het aantal onafhankelijke leden van het leidinggevend orgaan in zijn toezichtfunctie, dat comités niet worden samengesteld uit een groep leden die samen al een ander comité vormen.

50. Instellingen dienen erop te letten dat voorzitters en leden van comités incidenteel rouleren, waarbij zij rekening dienen te houden met de specifieke ervaring, kennis en vaardigheden die, individueel of collectief, vereist zijn voor deze comités.

51. De risico- en benoemingscomités dienen te bestaan uit niet-uitvoerende leden van het leidinggevend orgaan in zijn toezichtfunctie van de betrokken instelling. Het auditcomité dient te worden samengesteld op de wijze beschreven in artikel 41 van Richtlijn 2006/43/EG[16]. Het beloningscomité dient te worden samengesteld op de wijze beschreven in paragraaf 2.4.1 van de EBA-richtsnoeren betreffende een beheerst beloningsbeleid[17].

52. In MSI's en ASI's behoort de meerderheid van de leden van het benoemingscomité onafhankelijk te zijn en dit comité te worden voorgezeten door een onafhankelijk lid. In andere significante instellingen, als door bevoegde autoriteiten of het nationale recht bepaald, dient het benoemingscomité voldoende onafhankelijke leden te hebben; dergelijke

[14] Dit hoofdstuk dient te worden gelezen in samenhang met de gemeenschappelijke ESMA- en EBA-richtsnoeren voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie uit hoofde van Richtlijn 2013/36/EU en Richtlijn 2014/65/EU.

[15] Zoals gedefinieerd in paragraaf 9.3 van de gemeenschappelijke ESMA- en EBA-richtsnoeren voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie uit hoofde van Richtlijn 2013/36/EU en Richtlijn 2014/65/EU.

[16] Richtlijn 2006/43/EG van het Europees Parlement en de Raad van 17 mei 2006 betreffende de wettelijke controles van jaarrekeningen en geconsolideerde jaarrekeningen, tot wijziging van de Richtlijnen 78/660/EEG en 83/349/EEG van de Raad en houdende intrekking van Richtlijn 84/253/EEG van de Raad (PB L 157 van 9.6.2006, blz. 87), laatstelijk gewijzigd bij Richtlijn 2014/56/EU van het Europees Parlement en de Raad van 16 april 2014.

[17] Richtsnoeren betreffende een beheerst beloningsbeleid overeenkomstig artikel 74, lid 3, en artikel 75, lid 2, van Richtlijn 2013/36/EU en openbaarmaking overeenkomstig artikel 450 van Verordening (EU) nr. 575/2013 (EBA/GL/2015/22).

instellingen kunnen het eveneens als een goede praktijk beschouwen een voorzitter van het benoemingscomité te hebben die onafhankelijk is.

53. Leden van het benoemingscomité dienen, zowel individueel als gezamenlijk, over voldoende kennis, vaardigheden en deskundigheid op het gebied van het selectieproces en geschiktheidsvereisten zoals uiteengezet in Richtlijn 2013/36/EU te beschikken.

54. In MSI's en ASI's behoort de meerderheid van de leden van het risicocomité onafhankelijk te zijn. In MSI's en ASI's dient het risicocomité te worden voorgezeten door een onafhankelijk lid. In andere significante instellingen, als door bevoegde autoriteiten of het nationale recht bepaald, dient het risicocomité voldoende onafhankelijke leden te hebben en dient dit comité waar mogelijk te worden voorgezeten door een onafhankelijk lid. De voorzitter van het risicocomité dient in geen enkele instelling tevens de voorzitter van het leidinggevend orgaan of de voorzitter van enig ander comité zijn.

55. Leden van het risicocomité dienen, zowel individueel als gezamenlijk, over voldoende kennis, vaardigheden en deskundigheid op het gebied van risicobeheer- en -beheersingspraktijken te beschikken.

5.3 Processen van comités

56. Comités dienen regelmatig verslag uit te brengen aan het leidinggevend orgaan in zijn toezichtfunctie.

57. Er dient een passende wisselwerking te zijn tussen comités. Met inachtneming van punt 49 kan een dergelijke wisselwerking de vorm aannemen van wederzijdse vertegenwoordiging zodat de voorzitter of een lid van een comité ook lid kan zijn van een ander comité.

58. Leden van comités dienen actief deel te nemen aan open en kritische discussies, tijdens welke afwijkende meningen op een constructieve manier worden besproken.

59. Comités behoren de agenda's van comitévergaderingen vast te leggen, evenals de belangrijkste resultaten en conclusies van die vergaderingen.

60. Het risicocomité en het benoemingscomité dienen er in ieder geval voor te zorgen dat zij:

    a. toegang hebben tot alle relevante informatie en gegevens die nodig zijn om hun taak te verrichten, met inbegrip van informatie en gegevens die afkomstig zijn van relevante bedrijfs- en controlefuncties (zoals de afdelingen juridische zaken, financiën, personeelszaken, IT, interne controle, risico en naleving, waaronder ook informatie over naleving van de AML/CTF-voorschriften en geaggregeerde informatie over meldingen van verdachte transacties en de risicofactoren witwassen en terrorismefinanciering);

    b. regelmatig rapporten, ad-hocinformatie, mededelingen en adviezen van hoofden interne controlefuncties ontvangen met betrekking tot het actuele risicoprofiel van de

instelling, haar risicocultuur en haar risicolimieten, evenals aangaande eventuele belangrijke inbreuken [18] die mogelijk hebben plaatsgevonden, met gedetailleerde informatie over en aanbevelingen voor corrigerende maatregelen die zijn genomen, moeten worden genomen of worden voorgesteld, en dat zij de inhoud, het format en de frequentie van de risicoinformatie die aan hen wordt gerapporteerd, onderwerpen aan periodieke evaluatie en besluitvorming, en

c. waar nodig zorgen voor voldoende betrokkenheid van de interne controlefuncties en andere relevante functies (personeelszaken, juridische zaken, financiën) binnen de respectieve deskundigheidsgebieden en/of advies van externe deskundigen inwinnen.

5.4 Taken van het risicocomité

61. Indien een risicocomité is ingesteld, dient dit ten minste:

a. het leidinggevend orgaan in zijn toezichtfunctie te adviseren en ondersteunen voor wat betreft het toezicht op de algemene feitelijke en toekomstige risicostrategie en risicobereidheid van de instelling, waarbij het rekening houdt met alle soorten risico's, teneinde ervoor te zorgen dat deze in lijn zijn met de bedrijfsstrategie, de doelstellingen en de bedrijfscultuur en -waarden van de instelling;

b. het leidinggevend orgaan in zijn toezichtfunctie bij te staan in de uitoefening van het toezicht op de uitvoering van de risicostrategie van de instelling en de limieten die daarvoor zijn vastgesteld;

c. toe te zien op de tenuitvoerlegging van de strategieën voor kapitaal- en liquiditeitsbeheer evenals voor alle andere relevante risico's van een instelling, zoals markt-, krediet-, operationele (met inbegrip van juridische en IT-risico's) en reputatierisico's, om hun toereikendheid in het licht van de vastgestelde risicobereidheid en -strategie te beoordelen;

d. het leidinggevend orgaan in zijn toezichtfunctie aanbevelingen te doen inzake noodzakelijke aanpassingen van de risicostrategie die onder meer voortvloeien uit veranderingen in het bedrijfsmodel van de instelling, marktontwikkelingen of aanbevelingen die worden gedaan door de risicobeheerfunctie;

e. advies te verstrekken inzake de aanstelling van externe adviseurs die het toezichthoudend orgaan mogelijk inzet voor advies of assistentie;

[18] Wat betreft ernstige inbreuken op het gebied van AML/CTF, zie ook de uit hoofde van artikel 117, lid 6, van Richtlijn 2013/36/EU uit te brengen richtsnoeren met de nadere regelingen betreffende de wijze van samenwerking en informatie-uitwisseling tussen de in lid 5 van dit artikel bedoelde autoriteiten, met name met betrekking tot grensoverschrijdende groepen en in de context van het vaststellen van ernstige schendingen van de regels ter voorkoming van het witwassen van geld.

f. een aantal mogelijke scenario's te toetsen, waaronder stressscenario's, om te beoordelen hoe het risicoprofiel van de instelling zou reageren op externe en interne gebeurtenissen;

g. toe te zien op de afstemming tussen alle belangrijke aan cliënten aangeboden financiële producten en diensten en het bedrijfsmodel en de risicostrategie van de instelling[19]. Het risicocomité dient de risico's die samenhangen met de aangeboden financiële producten en diensten te beoordelen en rekening te houden met de afstemming van de prijzen die aan de producten worden toegekend en de winst die met deze producten en diensten wordt behaald; en

h. de aanbevelingen van interne of externe auditors te beoordelen en een vervolg te geven aan de passende tenuitvoerlegging van genomen maatregelen.

62. Het risicocomité dient samen te werken met andere comités waarvan de activiteiten gevolgen kunnen hebben voor de risicostrategie (bijv. audit- en beloningscomités) en op regelmatige basis te communiceren met de interne controlefuncties van de instelling, met name de risicobeheerfunctie.

63. Wanneer er een risicocomité is ingesteld, onderzoekt dit, onverminderd de taken van het beloningscomité, of de prikkels die uitgaan van het beloningsbeleid en de beloningspraktijken rekening houden met het risico, het kapitaal, de liquiditeit en de waarschijnlijkheid en de spreiding in de tijd van winsten van de instelling.

5.5 Taken van het auditcomité

64. Overeenkomstig Richtlijn 2006/43/EG[20] dient het auditcomité, indien dit is ingesteld, onder meer:

a. toe te zien op de doeltreffendheid van de interne kwaliteitscontrole- en risicobeheersystemen van de instelling en, indien toepasselijk, van haar interne auditfunctie, ten aanzien van de financiële verslaglegging van de gecontroleerde instelling, zonder inbreuk te maken op haar onafhankelijkheid;

b. toe te zien op de vaststelling door de instelling van de grondslagen voor financiële verslaglegging;

c. toe te zien op het financiële verslagleggingsproces en aanbevelingen te doen met het oog op het waarborgen van haar integriteit;

[19] Zie ook de EBA-richtsnoeren inzake producttoezicht- en -governanceregelingen voor retailbanken, beschikbaar op .

[20] Richtlijn 2006/43/EG van het Europees Parlement en de Raad van 17 mei 2006 betreffende de wettelijke controles van jaarrekeningen en geconsolideerde jaarrekeningen, tot wijziging van de Richtlijnen 78/660/EEG en 83/349/EEG van de Raad en houdende intrekking van Richtlijn 84/253/EEG van de Raad (PB L 157 van 9.6.2006, blz. 87), laatstelijk gewijzigd bij Richtlijn 2014/56/EU van het Europees Parlement en de Raad van 16 april 2014.

d. de onafhankelijkheid van de wettelijke auditors of de auditkantoren te evalueren en monitoren in overeenstemming met de artikelen 22, 22 bis, 22 ter, 24 bis en 24 ter van Richtlijn 2006/43/EU en artikel 6 van Verordening (EU) nr. 537/2014[21], en met name de passendheid van de levering van niet-controlediensten aan de gecontroleerde instelling overeenkomstig artikel 5 van die verordening;

e. toezicht te houden op de wettelijke controle van de enkelvoudige en geconsolideerde jaarrekeningen, met name de uitvoering daarvan, rekening houdend met eventuele bevindingen en conclusies van de bevoegde autoriteit uit hoofde van artikel 26, lid 6, van Verordening (EU) nr. 537/2014;

f. de verantwoordelijkheid te dragen voor de procedure voor de selectie van externe wettelijke auditor(s) of auditkantoren en aanbevelingen te doen voor hun benoeming, vergoeding en ontslag, met het oog op goedkeuring daarvan door het bevoegde orgaan van de instelling (overeenkomstig artikel 16 van Verordening (EU) nr. 537/2014, behoudens wanneer artikel 16, lid 8, van Verordening (EU) nr. 537/2014 van toepassing is);

g. de reikwijdte van de controle en de frequentie van de wettelijke controle van de jaarrekening of de geconsolideerde jaarrekening te beoordelen;

h. overeenkomstig artikel 39, lid 6, onder a), van Richtlijn 2006/43/EU, het leidinggevende of toezichthoudende orgaan van de gecontroleerde entiteit in kennis te stellen van het resultaat van de wettelijke controle en toe te lichten op welke wijze de wettelijke controle heeft bijgedragen aan de integriteit van de financiële verslaglegging en welke rol het auditcomité in dat proces heeft gespeeld; en

i. auditverslagen in ontvangst te nemen en er rekening mee te houden.

5.6 Gecombineerde comités

65. Overeenkomstig artikel 76, lid 3, van Richtlijn 2013/36/EU kunnen bevoegde autoriteiten instellingen die niet significant worden geacht, toestaan het risicocomité, indien ingesteld, met het auditcomité als bedoeld in artikel 39 van Richtlijn 2006/43/EG te combineren.

66. Wanneer risico- en benoemingscomités zijn ingesteld in niet-significante instellingen, kunnen deze worden gecombineerd. Als dat gebeurt, dienen deze instellingen vast te leggen om welke redenen ze ervoor hebben gekozen de comités te combineren en hoe ze met deze aanpak de doelstellingen van de comités verwezenlijken.

[21] Verordening (EU) nr. 537/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende specifieke eisen voor de wettelijke controles van entiteiten van openbaar belang en tot intrekking van Besluit 2005/909/EG van de Commissie (PB L 158 van 27.5.2014, blz. 77).

67. Instellingen zorgen er te allen tijde voor dat de leden van een gecombineerd comité, individueel en collectief, de noodzakelijke kennis, vaardigheden en deskundigheid bezitten om de taken die het gecombineerde comité dient uit te voeren, volledig te begrijpen[22].

Titel III – Kader voor governance

6 Organisatiekader en -structuur

6.1 Organisatiekader

68. Het leidinggevend orgaan van een instelling dient te zorgen voor een passende en transparante organisatie- en operationele structuur voor die instelling en dient daar een schriftelijke beschrijving van te hebben. Deze structuur dient te getuigen van en bevorderend te zijn voor een doeltreffend en prudent beheer van de instelling op individueel, gesubconsolideerd en geconsolideerd niveau. Het leidinggevend orgaan dient ervoor te zorgen dat de interne controlefuncties onafhankelijk zijn van de bedrijfsonderdelen die zij controleren, wat onder meer inhoudt dat er een adequate scheiding van taken is, en dat zij over de passende financiële en personele middelen en bevoegdheden beschikken om hun taak naar behoren te vervullen. De rapportagelijnen en de toewijzing van verantwoordelijkheden binnen een instelling, met name die tussen medewerkers met een sleutelfunctie, behoren helder, welomschreven, samenhangend en afdwingbaar, en adequaat gedocumenteerd te zijn. De documentatie dient wanneer nodig te worden bijgewerkt.

69. De structuur van de instelling dient het vermogen van het leidinggevend orgaan om de risico's van de instelling of groep te overzien en doeltreffend te beheren of het vermogen van de bevoegde autoriteit om doeltreffend toezicht te houden op de instelling, niet te belemmeren.

70. Het leidinggevend orgaan dient te beoordelen of en hoe belangrijke veranderingen in de structuur van de groep (bijv. de oprichting van nieuwe dochterondernemingen, fusies en overnames, het afstoten of de liquidatie van delen van de groep, of externe ontwikkelingen) de deugdelijkheid van het organisatiekader van de instelling beïnvloeden. Wanneer zwakke punten worden vastgesteld, dient het leidinggevend orgaan eventueel noodzakelijke aanpassingen snel door te voeren.

6.2 Ken uw structuur

71. Het leidinggevend orgaan dient de juridische, organisatie- en operationele structuur van de instelling ten volle te kennen en te begrijpen ("ken uw structuur") en ervoor te zorgen dat die structuur aansluit op de goedgekeurde bedrijfs- en risicostrategie en risicobereidheid en door haar kader voor risicobeheer wordt gedekt.

[22] Zie ook de gemeenschappelijke ESMA- en EBA-richtsnoeren voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie uit hoofde van Richtlijn 2013/36/EU en Richtlijn 2014/65/EU.

72. Het leidinggevend orgaan dient verantwoordelijk te zijn voor de goedkeuring van deugdelijke strategieën en beleid voor de vaststelling van nieuwe structuren. Wanneer een instelling binnen haar groep een groot aantal rechtspersonen opricht, dienen hun aantal en in het bijzonder de onderlinge verbindingen en transacties tussen hen geen knelpunten te vormen bij het ontwerp van haar interne governance en voor het doeltreffende beheer van en toezicht op de risico's van de groep als geheel. Het leidinggevend orgaan dient ervoor te zorgen dat de structuur van een instelling en, in voorkomend geval, de structuren binnen een groep, rekening houdend met de criteria die zijn vastgelegd in hoofdstuk 7, duidelijk, doeltreffend en transparant zijn voor het personeel, de aandeelhouders en andere belanghebbenden van de instelling en voor de bevoegde autoriteit.

73. Het leidinggevend orgaan dient sturing te geven aan de structuur van de instelling alsmede aan haar ontwikkeling en beperkingen, en ervoor te zorgen dat de structuur gerechtvaardigd, efficiënt en niet nodeloos complex is.

74. Het leidinggevend orgaan van een consoliderende instelling dient niet alleen de juridische, organisatie- en operationele structuur van de groep te kennen, maar ook het doel en de activiteiten van haar verschillende entiteiten alsmede hun onderlinge verbanden en betrekkingen. Daartoe behoort ook inzicht in operationele risico's die specifiek zijn voor de groep en in blootstellingen binnen de groep, evenals in de wijze waarop financierings-, kapitaal-, liquiditeits- en risicoprofielen van de groep onder normale en ongunstige omstandigheden kunnen worden beïnvloed. Het leidinggevend orgaan dient ervoor te zorgen dat de instelling tijdig informatie over de groep kan verstrekken wat betreft het type, de kenmerken, het organisatieschema, de eigendomsstructuur en de bedrijfsactiviteiten van iedere rechtspersoon, en dat de instellingen binnen de groep voldoen aan alle rapportagevereisten van de toezichthouder op een individuele, gesubconsolideerde en geconsolideerde basis.

75. Het leidinggevend orgaan van een consoliderende instelling dient ervoor te zorgen dat de verschillende entiteiten van de groep (met inbegrip van de consoliderende instelling zelf) voldoende informatie ontvangen, zodat zij een duidelijk beeld hebben van de algemene doelstellingen, de strategieën en het risicoprofiel van de groep en van de manier waarop de betrokken groepsentiteit is ingebed in de structuur en operationele werking van de groep. Dergelijke informatie en herzieningen daarvan dienen te worden gedocumenteerd en beschikbaar te worden gesteld aan de betrokken relevante functies, waaronder het leidinggevend orgaan, bedrijfsonderdelen en interne controlefuncties. De leden van het leidinggevend orgaan van een consoliderende instelling dienen ervoor te zorgen dat ze op de hoogte blijven van de risico's die de structuur van de groep met zich meebrengt, rekening houdend met de criteria die zijn vastgelegd in hoofdstuk 7 van de richtsnoeren. Dat betekent onder andere dat zij:

    a. informatie ontvangen over belangrijke risicobronnen;

b. periodieke rapporten ontvangen met een beoordeling van de algemene structuur van de instelling en van de verenigbaarheid van activiteiten van de afzonderlijke entiteiten met de goedgekeurde groepsbrede strategie; en

c. periodieke rapporten ontvangen over terreinen waarop het regelgevingskader moet worden nageleefd op individueel, gesubconsolideerd en geconsolideerd niveau.

6.3 Complexe structuren en activiteiten die niet standaard en niet transparant zijn

76. Instellingen dienen het opzetten van complexe en potentieel niet-transparante structuren te vermijden. Instellingen dienen bij hun besluitvorming rekening te houden met de resultaten van een risicobeoordeling aan de hand waarvan wordt vastgesteld of dergelijke structuren zouden kunnen worden gebruikt voor het witwassen van geld, het financieren van terrorisme of andere financiële misdrijven, en met de respectieve controles en het toepasselijke rechtskader[23]. Daartoe dienen instellingen ten minste rekening te houden met:

a. de mate waarin het rechtsgebied waarin de structuur wordt opgezet daadwerkelijk voldoet aan EU- en internationale normen inzake belastingtransparantie en de bestrijding van het witwassen van geld en de financiering van terrorisme[24];

b. de mate waarin de structuur een duidelijk economisch en rechtmatig doel dient;

c. de mate waarin de structuur zou kunnen worden gebruikt om de identiteit van de uiteindelijk gerechtigde verborgen te houden;

d. de mate waarin het verzoek van de cliënt dat mogelijk tot het opzetten van een structuur zal leiden, aanleiding geeft tot zorg;

e. of de structuur passend toezicht door het leidinggevend orgaan van de instelling of het vermogen van de instelling om de bijbehorende risico's te beheren in de weg zou staan; en

f. of de structuur een obstakel vormt voor doeltreffend toezicht door bevoegde autoriteiten.

77. In ieder geval dienen instellingen geen ondoorzichtige of nodeloos complexe structuren op te zetten die geen duidelijke economische reden of juridisch doel hebben, en evenmin structuren die aanleiding zouden kunnen vormen tot zorg dat ze mogelijk worden opgezet voor een doel dat verband houdt met financiële misdrijven.

[23] Voor nadere gegevens over de beoordeling van landspecifieke risico's en de risico's in verband met individuele producten en cliënten dienen instellingen ook de gemeenschappelijke richtsnoeren inzake de risicofactoren witwaspraktijken en terrorismefinanciering (EBA GL JC/2017/37) te raadplegen, die momenteel worden herzien.

[24] Zie ook:

78. Wanneer dergelijke structuren worden opgezet, dient het leidinggevend orgaan ervoor te zorgen dat het deze structuren, hun doel en de specifieke risico's die ermee samenhangen, begrijpt en dat de interne controlefuncties er op passende wijze bij worden betrokken. Dergelijke structuren dienen alleen te worden goedgekeurd en gehandhaafd als hun doel duidelijk vastgesteld en begrepen is, en wanneer het leidinggevend orgaan er zeker van is dat alle belangrijke risico's, met inbegrip van reputatierisico's, zijn vastgesteld, dat alle risico's doeltreffend kunnen worden beheerd en op passende wijze gerapporteerd, en dat doeltreffend toezicht is gewaarborgd. Hoe complexer en ondoorzichtiger de organisatie- en operationele structuur en hoe groter de risico's, des te intensiever dient het toezicht erop te zijn.

79. Instellingen dienen hun besluiten te documenteren en in staat te zijn om hun besluiten te rechtvaardigen ten opzichte van bevoegde autoriteiten.

80. Het leidinggevend orgaan dient ervoor te zorgen dat passende maatregelen worden genomen om de risico's van activiteiten binnen dergelijke structuren te vermijden of beperken. Dit houdt onder meer in dat:

    a. de instelling adequaat beleid en adequate procedures en gedocumenteerde processen (bijv. toepasselijke limieten en informatiestromen) heeft ingevoerd voor het overwegen, naleven, goedkeuren en risicobeheer van dergelijke activiteiten, rekening houdend met de gevolgen voor de organisatie- en operationele structuur van de groep, haar risicoprofiel en reputatierisico;

    b. informatie over deze activiteiten en de risico's daarvan toegankelijk is voor de consoliderende instelling en interne en externe auditors en wordt gerapporteerd aan het leidinggevend orgaan in zijn toezichtfunctie en aan de bevoegde autoriteit die een vergunning heeft verleend; en

    c. de instelling op gezette tijden beoordeelt of het nog steeds noodzakelijk is om dergelijke structuren te handhaven.

81. Deze structuren en activiteiten, evenals de mate waarin deze in overeenstemming zijn met de wet en professionele normen, dienen periodiek aan een onderzoek te worden onderworpen door de interne auditfunctie, waarbij een op risico's gebaseerde benadering wordt gehanteerd.

82. Instellingen dienen dezelfde risicobeheermaatregelen te nemen als voor de eigen bedrijfsactiviteiten van de instelling wanneer zij activiteiten uitvoeren voor cliënten die niet standaard en niet transparant zijn (bijv. cliënten helpen met het opzetten van vehikels in offshore rechtsgebieden, het optuigen van complexe structuren, het financieren van transacties voor hen, of de verlening van trusteediensten) en die soortgelijke uitdagingen voor de interne governance inhouden en grote operationele en reputatierisico's met zich brengen. Instellingen dienen met name te analyseren waarom een cliënt een bepaalde structuur wil opzetten.

7 Organisatiekader in de context van een groep

83. Overeenkomstig artikel 109, lid 2, van Richtlijn 2013/36/EU dienen moederondernemingen en dochterondernemingen die onder die richtlijn vallen, ervoor te zorgen dat regelingen, processen en mechanismen voor interne governance samenhang vertonen en goed geïntegreerd zijn op geconsolideerde of gesubconsolideerde basis. Met het oog hierop dienen moederondernemingen en dochterondernemingen die onder de prudentiële consolidatie vallen, dergelijke regelingen, processen en mechanismen in hun niet onder Richtlijn 2013/36/EU vallende dochterondernemingen toe te passen, met inbegrip van dochterondernemingen die in derde landen, waaronder in offshore financiële centra, zijn opgericht, om te zorgen voor solide governanceregelingen op een geconsolideerde en gesubconsolideerde basis. Wat betreft de beloningsvereisten gelden er enkele uitzonderingen overeenkomstig artikel 109, leden 4 en 5[25]. Bevoegde functies binnen de consoliderende instelling en haar dochterondernemingen dienen onderling contact te hebben en waar nuttig informatie uit te wisselen. De regelingen, processen en mechanismen voor governance dienen te waarborgen dat de consoliderende instelling voldoende gegevens en informatie tot haar beschikking heeft en in staat is het groepsbrede risicoprofiel te beoordelen, zoals omschreven in paragraaf 6.2.

84. Het leidinggevend orgaan van een dochteronderneming die onder Richtlijn 2013/36/EU valt, dient het groepsbrede governancebeleid dat op het geconsolideerde en gesubconsolideerde niveau is vastgesteld, goed te keuren en op individueel niveau uit te voeren, op een wijze die voldoet aan alle specifieke vereisten van EU- en nationale wetgeving.

85. Op geconsolideerd en gesubconsolideerd niveau dient de consoliderende instelling ervoor te zorgen dat het in titel V genoemde groepsbrede governancebeleid en interne controlekader worden nageleefd door alle instellingen en andere entiteiten die onder de prudentiële consolidatie vallen, met inbegrip van hun dochterondernemingen die zelf niet onder Richtlijn 2013/36/EU vallen. Bij de tenuitvoerlegging van governancebeleid dient de consoliderende instelling ervoor te zorgen dat solide governanceregelingen zijn ingevoerd voor elke dochteronderneming en specifieke regelingen, processen en mechanismen te overwegen wanneer bedrijfsactiviteiten niet in afzonderlijke rechtspersonen zijn georganiseerd, maar binnen een matrix van bedrijfsonderdelen die meer rechtspersonen omvat.

86. Een consoliderende instelling moet rekening houden met de belangen van al haar dochterondernemingen. Ook moet zij nadenken over hoe strategieën en beleid op de lange termijn bijdragen aan het belang van elke dochteronderneming en van de groep als geheel.

87. Moederondernemingen en hun dochterondernemingen dienen ervoor te zorgen dat de instellingen en entiteiten binnen de groep voldoen aan alle specifieke regelgevingsvereisten in elk relevant rechtsgebied.

[25] Gelieve ook de EBA-richtsnoeren betreffende een beheerst beloningsbeleid te raadplegen.

88. De consoliderende instelling dient ervoor te zorgen dat dochterondernemingen die in derde landen zijn gevestigd, en die onder de prudentiële consolidatie vallen, governanceregelingen, processen en mechanismen hebben ingevoerd die stroken met het groepsbrede governancebeleid en voldoen aan de vereisten van de artikelen 74 tot en met 96 van Richtlijn 2013/36/EU en aan deze richtsnoeren, zolang dit niet onrechtmatig is volgens de wetten van het derde land.

89. De governancevereisten van Richtlijn 2013/36/EU en de bepalingen van deze richtsnoeren gelden voor instellingen, ook als dit dochterondernemingen van een moederonderneming in een derde land zijn. Wanneer een dochteronderneming in de EU van een moederonderneming in een derde land een consoliderende instelling is, omvat de prudentiële consolidatie niet het niveau van de in een derde land gevestigde moederonderneming en andere rechtstreekse dochterondernemingen van die moederonderneming. De consoliderende instelling dient ervoor te zorgen dat in haar eigen governancebeleid rekening wordt gehouden met het groepsbrede governancebeleid van de moederonderneming in een derde land, voor zover dat niet in strijd is met de vereisten van relevante EU-wetgeving, waaronder Richtlijn 2013/36/EU en de nadere specificaties in deze richtsnoeren.

90. Bij het vaststellen van beleid en het documenteren van governanceregelingen dienen instellingen rekening te houden met de aspecten die worden genoemd in bijlage I bij de richtsnoeren. Ofschoon beleid en documentatie in afzonderlijke documenten mogen worden opgenomen, dienen instellingen te overwegen deze te combineren of ze op te nemen in één enkel kaderdocument voor governance.

8 Uitbestedingsbeleid[26]

91. Het leidinggevend orgaan dient het uitbestedingsbeleid van een instelling goed te keuren, regelmatig te herzien en bij te werken, waarbij het ervoor dient te zorgen dat de benodigde wijzigingen tijdig ten uitvoer worden gelegd.

92. In het uitbestedingsbeleid dient rekening te worden gehouden met het uitbestedingseffect op de bedrijfsactiviteiten van een instelling en de daarmee gepaard gaande risico's (zoals operationele risico's, waaronder juridische en IT-risico's, reputatie- en concentratierisico's). Het beleid dient de rapportage- en controleregelingen te bevatten die van de aanvang tot de beëindiging van een uitbestedingscontract dienen te worden uitgevoerd (waaronder de uitwerking van het zakelijk motief voor uitbesteding, het aangaan van een uitbestedingscontract, de uitvoering van het contract tot aan de vervaldatum, noodplannen en exitstrategieën). Een instelling blijft volledig verantwoordelijk voor alle uitbestede diensten en activiteiten en hieruit voortvloeiende managementbesluiten. In het beleidsdocument inzake uitbesteding dient dus duidelijk te worden vastgelegd dat

[26] Zie ook: EBA-richtsnoeren inzake uitbesteding, beschikbaar op:

uitbesteding de instelling niet ontslaat van haar wettelijke verplichtingen en verantwoordelijkheden jegens haar cliënten.

93. In het beleidsdocument dient te worden vastgelegd dat uitbestedingsregelingen een doelmatig toezicht ter plekke en op afstand niet mogen belemmeren en niet mogen indruisen tegen beperkingen inzake toezicht op het gebied van diensten en activiteiten. Het beleid dient ook van toepassing te zijn op uitbesteding binnen de groep (bijv. diensten die worden verstrekt door een afzonderlijke rechtspersoon binnen de groep van een instelling) en rekening te houden met eventuele specifieke omstandigheden binnen de groep.

Titel IV – Risicocultuur en gedragsregels

9 Risicocultuur

94. Een solide, zorgvuldige en consistente risicocultuur dient een belangrijk element te zijn van doeltreffend risicobeheer van instellingen en dient instellingen in staat te stellen gedegen en geïnformeerde besluiten te nemen.

95. Instellingen dienen een geïntegreerde en organisatiebrede risicocultuur te ontwikkelen die berust op volledig inzicht in en een holistisch perspectief op de risico's die zij lopen en de manier waarop zij deze risico's beheren met inachtneming van de risicobereidheid van de instelling.

96. Instellingen dienen een risicocultuur te ontwikkelen aan de hand van beleid, communicatie en opleiding van personeel inzake de activiteiten, de strategie en het risicoprofiel van instellingen, en hun communicatie en personeelsopleiding af te stemmen op de verantwoordelijkheden van het personeel als het gaat om het nemen en beheren van risico's.

97. Personeelsleden dienen zich volledig bewust te zijn van hun verantwoordelijkheden op het gebied van risicobeheer. Risicobeheer behoort niet uitsluitend een taak van risicospecialisten of werknemers in een interne controlefunctie te zijn. De verantwoordelijkheid voor het dagelijks risicobeheer in overeenstemming met het beleid, de procedures en controles van de instelling, rekening houdend met de risicobereidheid en -draagkracht van de instelling dient in hoofdzaak bij de bedrijfseenheden te berusten, waarbij het leidinggevend orgaan toezicht uitoefent.

98. Een sterke risicocultuur dient het volgende te omvatten, zonder daartoe beperkt te zijn:

    a. Toon aan de top: het leidinggevend orgaan is verantwoordelijk voor het vaststellen en communiceren van de kernwaarden en verwachtingen van de instelling. De leden dienen deze waarden in hun gedrag tot uiting te brengen. Het bestuur van instellingen, waaronder de medewerkers met een sleutelfunctie, dient bij te dragen aan de interne communicatie van kernwaarden en verwachtingen naar het personeel. Personeelsleden dienen in overeenstemming met alle toepasselijke wet- en regelgeving te handelen en direct melding te doen van waargenomen niet-naleving

binnen of buiten de instelling (bijv. aan de bevoegde autoriteit middels een klokkenluidersprocedure). Het leidinggevend orgaan dient voortdurend de risicocultuur van de instelling te bevorderen, bewaken en beoordelen; rekening te houden met het effect van de risicocultuur op de financiële stabiliteit, het risicoprofiel en de solide governance van de instelling; en waar nodig wijzigingen door te voeren.

b. Verantwoording: relevante personeelsleden op alle niveaus dienen de kernwaarden van de instelling en, voor zover noodzakelijk voor hun functie, haar risicobereidheid en risicodraagkracht te kennen en te begrijpen. Zij dienen in staat te zijn om hun functies uit te oefenen en zich ervan bewust te zijn dat ze verantwoording dienen af te leggen voor hun acties ten aanzien van het risicogedrag van de instelling.

c. Doeltreffende communicatie en kritiek: een goede risicocultuur dient een klimaat van open communicatie en het daadwerkelijk ter discussie stellen van zaken waarin besluitvormingsprocessen de aanzet vormen tot een brede reeks standpunten, te bevorderen, de gelegenheid te bieden bestaande praktijken te toetsen, een constructieve kritische houding onder het personeel aan te wakkeren, en een open en constructieve betrokkenheid in de hele organisatie te bevorderen.

d. Stimulansen: passende stimulansen dienen een essentiële rol te spelen in het afstemmen van risicogedrag op het risicoprofiel van de instelling en haar langetermijnbelangen[27].

10 Ondernemingswaarden en gedragscode

99. Het leidinggevend orgaan dient hoge ethische en beroepsnormen te ontwikkelen, vast te stellen, in acht te nemen en te bevorderen, rekening houdend met de specifieke behoeften en kenmerken van de instelling, en dient de tenuitvoerlegging van dergelijke normen te waarborgen (door middel van een gedragscode of soortgelijk instrument). Het dient ook toe te zien op naleving van deze normen door het personeel. Het leidinggevend orgaan kan, indien van toepassing, de groepsbrede normen of gemeenschappelijke normen die verenigingen of andere relevante organisaties hebben uitgebracht, vaststellen en ten uitvoer leggen.

100. Instellingen dienen te waarborgen dat er geen sprake is van discriminatie van personeelsleden op basis van geslacht, ras, huidskleur, etnische of sociale afkomst, genetische kenmerken, taal, godsdienst of levensovertuiging, politieke of andere overtuigingen, het behoren tot een nationale minderheid, eigendom, geboorte, invaliditeit, leeftijd of seksuele geaardheid.

101. Het beleid van instellingen dient genderneutraal te zijn. Dit betreft, maar is niet beperkt tot, het beleid ten aanzien van beloning, werving, loopbaanontwikkeling en opvolging, toegang tot opleiding en mogelijkheden om te solliciteren naar interne vacatures. Instellingen

[27] Zie ook de EBA-richtsnoeren betreffende een beheerst beloningsbeleid overeenkomstig artikel 74, lid 3, en artikel 75, lid 2, van Richtlijn 2013/36/EU en openbaarmaking overeenkomstig artikel 450 van Verordening (EU) nr. 575/2013 (EBA/GL/2015/22), beschikbaar op .

waarborgen gelijke kansen[28] voor alle personeelsleden ongeacht hun geslacht, en ook ten aanzien van loopbaanperspectieven, en streven naar verbetering van de vertegenwoordiging van het geslacht dat in het leidinggevend orgaan en in de groep personeelsleden met leidinggevende verantwoordelijkheden zoals gedefinieerd in de Gedelegeerde Verordening van de Commissie (technische reguleringsnormen inzake geïdentificeerde personeelsleden) ondervertegenwoordigd is[29]. Instellen houden bij hoe de loonkloof tussen mannen en vrouwen zich specifiek onder geïdentificeerde personeelsleden (met uitzondering van leden van het leidinggevend orgaan), onder leden van het leidinggevend orgaan in zijn bestuursfunctie, onder leden van het leidinggevend orgaan in zijn toezichtfunctie en onder andere personeelsleden ontwikkelt. Instellingen hebben een beleid gericht op herintegratie van hun personeelsleden na moederschaps-, vaderschaps- of ouderschapsverlof.

102. De ten uitvoer gelegde normen dienen zich te richten op het versterken van de robuuste governanceregelingen van de instelling en op het terugdringen van de risico's waaraan de instelling is blootgesteld, met name operationele en reputatierisico's, die een aanzienlijke ongunstige impact op de winstgevendheid en duurzaamheid van een instelling kunnen hebben als gevolg van boetes, proceskosten, door bevoegde autoriteiten opgelegde beperkingen, andere financiële en strafrechtelijke sancties en het verlies aan merkwaarde en consumentenvertrouwen.

103. Het leidinggevend orgaan dient een helder en gedocumenteerd beleid te voeren over hoe aan deze normen dient te worden voldaan. Dit beleid dient:

a. personeelsleden eraan te herinneren dat alle activiteiten van de instelling moeten worden verricht overeenkomstig de toepasselijke wetgeving en de ondernemingswaarden van de instelling;

b. risicobewustzijn te bevorderen door middel van een sterke risicocultuur overeenkomstig hoofdstuk 9 van de richtsnoeren, waarin de verwachting van het leidinggevend orgaan tot uiting wordt gebracht dat activiteiten de vastgestelde risicobereidheid en door de instelling vastgestelde limieten en de respectieve verantwoordelijkheden van personeelsleden niet zullen overschrijden;

c. beginselen uiteen te zetten aangaande en voorbeelden te verstrekken van toelaatbaar en ontoelaatbaar gedrag dat met name samenhangt met opgave van onjuiste financiële gegevens en financieel wangedrag, economische en financiële misdrijven waaronder, maar niet beperkt tot, fraude, witwassen van geld en terrorismefinanciering, anti-trustpraktijken, financiële sancties, omkoping en corruptie, marktmanipulatie, misleidende verkopen en andere schendingen van wetgeving inzake consumentenbescherming, en fiscale misdrijven, hetzij rechtstreeks

[28] Zie ook Richtlijn 2006/54/EG van het Europees Parlement en de Raad van 5 juli 2006 betreffende de toepassing van het beginsel van gelijke kansen en gelijke behandeling van mannen en vrouwen in arbeid en beroep

[29] Zie ook de EBA-richtsnoeren betreffende genderneutraal beloningsbeleid

hetzij onrechtstreeks gepleegd, zoals door middel van onrechtmatige of verboden dividendarbitrageregelingen;

d. aan te geven dat van personeelsleden niet alleen wordt verwacht dat zij de wettelijke en regelgevingsvereisten en het interne beleid naleven, maar ook dat zij zich eerlijk en integer gedragen en hun taken uitvoeren met de nodige bekwaamheid, zorgvuldigheid en toewijding; en

e. ervoor te zorgen dat personeelsleden zich bewust zijn van de potentiële interne en externe disciplinaire maatregelen, gerechtelijke procedures en sancties die kunnen volgen op wangedrag en onaanvaardbaar gedrag.

104. Instellingen dienen de naleving van dergelijke normen te controleren en te zorgen voor bewustzijn bij personeelsleden, bijv. door het verstrekken van opleiding. Instellingen dienen vast te stellen welke functie verantwoordelijk is voor het toezicht op naleving van de gedragscode of een soortgelijk instrument en voor het beoordelen van schendingen daarvan, en een procedure vast te stellen voor het omgaan met niet-nalevingskwesties. De resultaten dienen periodiek te worden gerapporteerd aan het leidinggevend orgaan.

11 Beleid inzake belangenconflicten op het niveau van de instelling

105. Het leidinggevend orgaan dient verantwoordelijk te zijn voor de vaststelling, de goedkeuring en het toezicht op de tenuitvoerlegging en de handhaving van doeltreffend beleid voor het identificeren, beoordelen, beheren en beperken of voorkomen van feitelijke en potentiële belangenconflicten op het niveau van de instelling, bijv. als gevolg van de verschillende activiteiten en rollen van de instelling, van verschillende instellingen die onder de prudentiële consolidatie vallen of van verschillende bedrijfsonderdelen of -eenheden binnen een instelling, of met betrekking tot externe belanghebbenden.

106. Instellingen dienen, binnen hun organisatorische en administratieve regelingen, adequate maatregelen te nemen om te voorkomen dat belangenconflicten de belangen van hun cliënten negatief beïnvloeden.

107. De maatregelen van instellingen om belangenconflicten te beheren of, indien van toepassing, te beperken, dienen te worden gedocumenteerd en onder meer te bestaan uit:

a. een passende scheiding van taken, waarbij conflicterende activiteiten binnen de verwerking van transacties of bij het verlenen van diensten, alsmede toezichts- en rapportageverantwoordelijkheden in verband met conflicterende activiteiten aan verschillende personen worden toegewezen;

b. het instellen van informatiebarrières, bijv. de fysieke afscheiding van bepaalde bedrijfsonderdelen of -eenheden.

12 Beleid inzake belangenconflicten voor personeelsleden[30]

108. Het leidinggevend orgaan dient verantwoordelijk te zijn voor de vaststelling, de goedkeuring en het toezicht op de tenuitvoerlegging en de handhaving van doeltreffend beleid voor het identificeren, beoordelen, beheren en beperken of voorkomen van feitelijke en potentiële conflicten tussen de belangen van de instelling en de particuliere belangen van personeelsleden, met inbegrip van leden van het leidinggevend orgaan, die de vervulling van hun taken en verantwoordelijkheden negatief zouden kunnen beïnvloeden. Een consoliderende instelling dient rekening te houden met belangen binnen een groepsbreed beleid inzake belangenconflicten op een geconsolideerde of gesubconsolideerde basis.

109. Het beleid dient erop gericht te zijn belangenconflicten van personeelsleden te identificeren, met inbegrip van conflicten met de belangen van hun naaste familieleden. Instellingen dienen er rekening mee te houden dat belangenconflicten niet alleen kunnen ontstaan als gevolg van bestaande persoonlijke of professionele relaties, maar ook van dergelijke relaties uit het verleden. Wanneer belangenconflicten ontstaan, dienen instellingen te beoordelen hoe zwaarwegend deze zijn en besluiten te nemen over beperkende maatregelen, en die indien nodig uit te voeren.

110. Wat betreft belangenconflicten die het gevolg zijn van relaties uit het verleden, dienen instellingen een passende periode vast te stellen waarvoor zij willen dat personeelsleden dergelijke belangenconflicten melden, op basis van het feit dat deze nog steeds van invloed kunnen zijn op het gedrag van personeelsleden en hun aandeel in de besluitvorming.

111. Het beleid dient in ieder geval betrekking te hebben op de volgende situaties of relaties waarin belangenconflicten kunnen ontstaan:

a. economische belangen (bijv. aandelen, andere eigendomsrechten en lidmaatschappen, financiële holdings en andere economische belangen in commerciële cliënten, intellectuele-eigendomsrechten, leningen die door de instelling zijn verstrekt aan een onderneming die in handen is van een personeelslid, lidmaatschap van een orgaan of eigendom van een orgaan of entiteit met conflicterende belangen);

b. persoonlijke of professionele relaties met de bezitters van gekwalificeerde deelnemingen in de instelling;

c. persoonlijke of professionele relaties met personeelsleden van de instellingen of entiteiten die onder de prudentiële consolidatie vallen (bijv. familiaire relaties);

d. een andere baan en een eerdere baan uit het recente verleden (bijv. vijf jaar);

[30] Dit hoofdstuk dient te worden gelezen in samenhang met de gemeenschappelijke ESMA- en EBA-richtsnoeren voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie uit hoofde van Richtlijn 2013/36/EU en Richtlijn 2014/65/EU.

e. persoonlijke of professionele relaties met relevante externe belanghebbenden (bijv. banden hebben met belangrijke leveranciers, adviesbedrijven of andere dienstverleners); en

f. politieke invloed of politieke relaties.

112. Niettemin dienen instellingen er rekening mee te houden dat het feit dat iemand aandeelhouder van een instelling is of particuliere rekeningen of leningen heeft bij, of gebruikmaakt van andere diensten van een instelling, niet tot een situatie dient te leiden waarin personeelsleden worden geacht een belangenconflict te hebben als zij binnen een toepasselijke 'de minimis'-drempel blijven.

113. In het beleid dienen de procedures te worden vastgelegd voor rapportage en communicatie met de functie die verantwoordelijk is in het kader van het beleid. Personeelsleden dienen verplicht te zijn elke aangelegenheid die kan leiden of heeft geleid tot een belangenconflict, direct intern bekend te maken.

114. Het beleid dient onderscheid te maken tussen belangenconflicten die voortduren en permanent dienen te worden beheerd, en belangenconflicten die onverwacht optreden ten aanzien van één enkele gebeurtenis (bijv. een transactie, de selectie van een dienstverlener, enz.) en die gewoonlijk met een eenmalige maatregel kunnen worden beheerd. In alle gevallen dient het belang van de instelling centraal te staan in de genomen besluiten.

115. In het beleid dienen de procedures, maatregelen, documentatie-onderdelen en verantwoordelijkheden uiteen te worden gezet voor de identificatie en voorkoming van belangenconflicten, voor de beoordeling van het belang ervan en voor het nemen van beperkende maatregelen. Daartoe dienen onder meer de volgende procedures, onderdelen, verantwoordelijkheden en maatregelen te behoren:

a. conflicterende activiteiten of transacties toewijzen aan verschillende personen;

b. voorkomen dat personeelsleden die ook buiten de instelling actief zijn, ongepaste invloed verkrijgen binnen de instelling met betrekking tot deze andere activiteiten;

c. vastleggen dat de leden van het leidinggevend orgaan de verantwoordelijkheid hebben zich te onthouden van stemming bij aangelegenheden waarin een lid een belangenconflict heeft of kan hebben, of wanneer de objectiviteit of het vermogen van het lid om taken naar behoren uit te oefenen anderszins in het geding kan komen;

d. voorkomen dat leden van het leidinggevend orgaan bestuursfuncties hebben bij concurrerende instellingen, tenzij dat instellingen zijn die tot hetzelfde institutioneel protectiestelsel behoren, als bedoeld in artikel 113, lid 7, van Verordening (EU) nr. 575/2013, kredietinstellingen die blijvend zijn aangesloten bij een centraal orgaan, als bedoeld in artikel 10 van Verordening (EU) nr. 575/2013, of instellingen die onder de prudentiële consolidatie vallen.

116. Het beleid dient in ieder geval betrekking te hebben op belangenconflicten op het niveau van het leidinggevend orgaan en voldoende leidraden te bieden voor de identificatie en het beheer van belangenconflicten die het vermogen van leden van het leidinggevend orgaan tot het nemen van objectieve en onpartijdige beslissingen die erop gericht zijn de belangen van de instelling optimaal te behartigen, zouden kunnen belemmeren. Instellingen dienen er rekening mee te houden dat belangenconflicten van invloed kunnen zijn op de onafhankelijkheid van geest van leden van het leidinggevend orgaan[31].

117. Bij hun inspanningen om vastgestelde belangenconflicten van leden van het leidinggevend orgaan te beperken, dienen instellingen de getroffen maatregelen te documenteren en daarbij ook te beargumenteren hoe die maatregelen objectieve beslissingen helpen waarborgen.

118. Feitelijke of potentiële belangenconflicten die zijn aangemeld bij de verantwoordelijke functie binnen de instelling dienen naar behoren te worden beoordeeld en beheerd. Als een belangenconflict is vastgesteld, dient de instelling de genomen beslissing te documenteren, met name wanneer het belangenconflict en de bijbehorende risico's zijn aanvaard, en als het is aanvaard, de manier waarop dit belangenconflict afdoende is beperkt of weggenomen.

119. Alle feitelijke en potentiële belangenconflicten op het niveau van het leidinggevend orgaan, individueel en collectief, dienen naar behoren te worden gedocumenteerd en te worden gecommuniceerd naar het leidinggevend orgaan, waarna dit orgaan ze bespreekt, er een besluit over neemt en ze naar behoren beheert.

12.1 Beleid inzake belangenconflicten in het kader van leningen en andere transacties met leden van het leidinggevend orgaan en hun verbonden partijen

120. Als onderdeel van hun beleid inzake belangenconflicten voor personeelsleden (hoofdstuk 12) en het beheer van belangenconflicten van leden van het leidinggevend orgaan zoals uiteengezet in punt 117 dient het leidinggevend orgaan een kader op te zetten voor het in kaart brengen en beheren van belangenconflicten in de context van het verstrekken van leningen en het aangaan van andere transacties (bijv. factoring, leasing, vermogenstransacties enz.) met leden van het leidinggevend orgaan en hun verbonden partijen.

121. Onverminderd de nationale omzetting van Richtlijn 2013/36/EU[32] om kunnen instellingen aanvullende categorieën van verbonden partijen aanwijzen waarop zij hun kader voor belangenconflicten inzake leningen en andere transacties geheel of gedeeltelijk van toepassing verklaren.

[31] Zie ook de gemeenschappelijke ESMA- en EBA-richtsnoeren voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie uit hoofde van Richtlijn 2013/36/EU en Richtlijn 2014/65/EU.

[32] Zie ook kernbeginsel voor een effectief bankentoezicht nr. 20.

122. Het kader voor belangenconflicten dient te waarborgen dat beslissingen betreffende het verstrekken van leningen en het aangaan van andere transacties met leden van het leidinggevend orgaan en hun verbonden partijen objectief, zonder ongepaste beïnvloeding door belangenconflicten en in principe conform het zakelijkheidsbeginsel worden genomen.

123. Het leidinggevend orgaan dient de toepasselijke besluitvormingsprocessen op te zetten inzake het verstrekken van leningen aan en het aangaan van andere transacties met leden van het leidinggevend orgaan en hun verbonden partijen. Binnen dat kader kan onderscheid worden gemaakt tussen enerzijds standaard zakelijke transacties[33] die worden aangegaan in het kader van de normale bedrijfsuitoefening en conform de reguliere marktvoorwaarden, en anderzijds leningen aan en transacties met personeelsleden onder voorwaarden die voor alle personeelsleden gelden. Verder kan in het kader voor belangenconflicten en het besluitvormingsproces ook onderscheid worden gemaakt tussen belangrijke en niet-belangrijke leningen en andere transacties, verschillende soorten leningen en andere transacties en het niveau van de feitelijke of potentiële belangenconflicten die zij kunnen doen ontstaan.

124. Als onderdeel van het kader voor belangenconflicten dient het leidinggevend orgaan passende drempelwaarden te hanteren (bijv. per producttype of afhankelijk van de voorwaarden) die het bedrag aangeven waarboven de lening of andere transactie met een lid van het leidinggevend orgaan of een verbonden partij altijd goedkeuring van het leidinggevend orgaan behoeft. Beslissingen inzake belangrijke leningen of andere belangrijke transacties met leden van het leidinggevend orgaan die niet conform reguliere marktvoorwaarden worden verstrekt of verricht, maar onder voorwaarden die voor alle personeelsleden gelden, dienen altijd door het leidinggevend orgaan te worden genomen.

125. Het lid van het leidinggevend orgaan dat voordeel heeft van een dergelijke belangrijke lening of belangrijke andere transactie of het met de tegenpartij verbonden lid, dient niet bij de besluitvorming betrokken te zijn.

126. Alvorens een beslissing te nemen over een lening of andere transactie met leden van het leidinggevend orgaan of hun verbonden partijen, dient de instelling het risico waaraan zij als gevolg van die transactie mogelijk wordt blootgesteld, te beoordelen.

127. Waar leningen worden verstrekt in de vorm van een kredietlijn (bijv. een rekening-courantkrediet), dienen zowel de initiële beslissing als wijzigingen daarvan te worden gedocumenteerd. Het gebruik van dergelijke overeengekomen kredietfaciliteiten binnen de overeengekomen limieten dient niet te worden beschouwd als een nieuwe beslissing inzake een lening aan een lid van het leidinggevend orgaan of zijn/haar verbonden partij. Wanneer een wijziging van een kredietlijn als wezenlijk moet worden aangemerkt uit hoofde van het beleid van de instelling, dient een nieuwe beoordeling te worden verricht en een nieuwe beslissing te worden genomen.

[33] Onder zakelijke transacties wordt onder meer verstaan leningen en andere transacties (bijv. leasing, factoring, diensten in verband met beursintroducties, fusies en overnames, en de koop en verkoop van eigendommen).

128. Teneinde naleving te waarborgen van hun beleid inzake belangenconflicten, dienen instellingen erop toe te zien dat alle relevante interne controleprocedures volledig van toepassing zijn op leningen aan en andere transacties met leden van het leidinggevend orgaan of hun verbonden partijen, en dat er op het niveau van het leidinggevend orgaan in zijn toezichtfunctie een passend toezichtkader is ingericht.

12.2 Documentatie van leningen aan leden van het leidinggevend orgaan en hun verbonden partijen en aanvullende informatie

129. Voor de toepassing van artikel 88, lid 1, van Richtlijn 2013/36/EU dienen instellingen gegevens over leningen[34] aan leden van het leidinggevend orgaan en hun verbonden partijen naar behoren te documenteren, met vermelding van in ieder geval:

a. de naam van de debiteur en diens status (d.w.z., lid van het leidinggevend orgaan of een verbonden partij) en, voor leningen aan een verbonden partij, het lid van het leidinggevend orgaan aan wie die partij is verbonden en de aard van de relatie met de verbonden partij;

b. het soort lening/de aard van de lening en het bedrag;

c. de voorwaarden die op de lening van toepassing zijn;

d. de datum waarop de lening is goedgekeurd;

e. de naam van de persoon die of de naam en samenstelling van het orgaan dat de beslissing tot goedkeuring van de lening heeft genomen en de desbetreffende voorwaarden;

f. of de lening wel of niet conform marktvoorwaarden is verstrekt; en

g. of de lening wel of niet is verstrekt onder voorwaarden die voor alle personeelsleden gelden.

130. Instellingen dienen te waarborgen dat voor alle leningen aan leden van het leidinggevend orgaan en hun verbonden partijen volledige en actuele documentatie beschikbaar is en dat zij op verzoek de volledige documentatie onverwijld in een passend format aan de bevoegde autoriteiten ter beschikking kunnen stellen.

131. Bij leningen van meer dan 200 000 EUR aan leden van het leidinggevend orgaan of hun verbonden partijen dient de instelling in staat te zijn om op verzoek de volgende aanvullende informatie ter beschikking te stellen van de bevoegde autoriteit:

a. het percentage van de lening en het percentage van de som van alle uitstaande bedragen van leningen aan dezelfde debiteur, vergeleken met:

i. de som van haar tier 1-kapitaal en tier 2-kapitaal, en

[34] Zie ook de EBA-richtsnoeren inzake de initiëring van leningen, beschikbaar op:

ii. het tier 1-kernkapitaal van de instelling;

b. of de lening deel uitmaakt van een grote risicoblootstelling[35], en

c. het relatieve gewicht van het totaalbedrag van alle uitstaande leningen aan dezelfde debiteur, berekend als percentage door het totale uitstaande bedrag te delen door het totaalbedrag van alle uitstaande leningen aan leden van het leidinggevend orgaan en hun verbonden partijen.

13 Interne meldingsprocedures

132. Instellingen dienen passend intern beleid en passende interne meldingsprocedures in te voeren om personeelsleden in staat te stellen potentiële of feitelijke inbreuken op regelgevings- of interne vereisten, waaronder, zonder daartoe beperkt te zijn, die van Verordening (EU) nr. 575/2013 en nationale bepalingen tot omzetting van Richtlijn 2013/36/EU, of op regelingen voor interne governance, via een specifiek, onafhankelijk en zelfstandig kanaal te kunnen melden. Het dient voor personeelsleden die een inbreuk melden niet noodzakelijk te zijn daarvan bewijs te leveren; zij dienen er echter zo zeker van te zijn dat er voldoende reden is om een onderzoek te starten. Daarnaast dienen instellingen passende processen en procedures in te richten die waarborgen dat zij voldoen aan hun verplichtingen uit hoofde van de nationale tenuitvoerlegging van Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden.

133. Om belangenconflicten te voorkomen dienen personeelsleden inbreuken te kunnen melden buiten de reguliere rapportagelijnen om (bijv. via de compliance officer, de interne auditor of een onafhankelijke interne klokkenluidersprocedure). De meldingsprocedures dienen de bescherming te waarborgen van de persoonsgegevens van zowel de persoon die de inbreuk meldt als de natuurlijke persoon die voor de inbreuk verantwoordelijk zou zijn, in overeenstemming met Verordening (EU) 2016/679[36] (AVG).

134. De meldingsprocedures dienen beschikbaar te worden gesteld aan alle personeelsleden in een instelling.

135. Informatie die personeelsleden via de meldingsprocedures hebben verstrekt, dient, in voorkomend geval, beschikbaar te worden gesteld aan het leidinggevend orgaan en andere verantwoordelijke functies die in het interne meldingsbeleid zijn gedefinieerd. Wanneer het personeelslid dat een inbreuk meldt, dit verlangt, dient de informatie anoniem te worden verstrekt aan het leidinggevend orgaan en andere verantwoordelijke functies. Instellingen kunnen ook voorzien in een klokkenluidersprocedure die het mogelijk maakt informatie anoniem in te dienen.

[35] Zie ook deel IV van Verordening (EU) nr. 575/2013 en in het bijzonder artikel 392.

[36] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening persoonsgegevens).

136. Instellingen dienen ervoor te zorgen dat de persoon die de inbreuk meldt, afdoende wordt beschermd tegen eventuele negatieve gevolgen, zoals vergelding, discriminatie of andere soorten onbillijke behandeling. De instelling dient ervoor te zorgen dat geen enkele persoon die onder controle van de instelling valt, zich inlaat met represailles tegen een persoon die een inbreuk heeft gemeld, en dient passende maatregelen te nemen tegen degenen die verantwoordelijk zijn voor dergelijke represailles.

137. Instellingen dienen eveneens personen over wie meldingen worden gedaan te beschermen tegen eventuele negatieve effecten, mocht uit het onderzoek geen bewijs naar voren komen dat maatregelen tegen die persoon rechtvaardigt. Indien wel maatregelen worden genomen, dient de instelling deze op zodanige wijze te nemen dat de betrokken persoon beschermd wordt tegen onbedoelde negatieve effecten die het doel van de maatregel overstijgen.

138. Interne meldingsprocedures dienen met name:

a. te worden gedocumenteerd (bijv. handleidingen voor personeel);

b. heldere regels te verschaffen die waarborgen dat informatie over de persoon die de melding doet en de persoon op wie de melding betrekking heeft, en over de inbreuk, vertrouwelijk wordt behandeld, overeenkomstig Verordening (EU) 2016/679, tenzij bekendmaking volgens het nationale recht wordt vereist in het kader van nader onderzoek of een daaropvolgende gerechtelijke procedure;

c. personeelsleden te beschermen die vrezen dat er represailles tegen hen zullen worden genomen omdat ze te melden inbreuken openbaar hebben gemaakt;

d. te waarborgen dat de gemelde potentiële of feitelijke inbreuken worden beoordeeld en geëscaleerd, waaronder zo nodig naar de relevante bevoegde autoriteit of wetshandhavingdienst;

e. indien mogelijk te waarborgen dat personeelsleden die potentiële of feitelijke inbreuken hebben gemeld, een bevestiging krijgen dat hun informatie is ontvangen;

f. ervoor te zorgen dat het resultaat van een onderzoek naar een gemelde inbreuk wordt gevolgd; en

g. te waarborgen dat de gegevens goed worden bewaard.

14 Melding van inbreuken aan bevoegde autoriteiten

139. Bevoegde autoriteiten dienen doeltreffende en betrouwbare mechanismen in te stellen om personeelsleden van instellingen in staat te stellen relevante potentiële of feitelijke inbreuken op regelgevingsvereisten aan bevoegde autoriteiten te melden, waaronder, zonder

daartoe beperkt te zijn, die van Verordening (EU) nr. 575/2013 en nationale bepalingen tot omzetting van Richtlijn 2013/36/EU. Deze mechanismen bevatten ten minste:

a. specifieke procedures voor het in ontvangst nemen en behandelen van meldingen van inbreuken, bijvoorbeeld een speciaal daartoe ingestelde klokkenluidersafdeling, -eenheid of -functie;

b. passende bescherming als bedoeld in hoofdstuk 13;

c. bescherming van de persoonsgegevens van zowel de natuurlijke persoon die de inbreuk meldt als de natuurlijke persoon die voor de inbreuk verantwoordelijk zou zijn, in overeenstemming met Verordening (EU) 2016/679; en

d. heldere procedures zoals beschreven in hoofdstuk 13.

140. Onverminderd de mogelijkheid inbreuken te melden via de mechanismen van bevoegde autoriteiten, kunnen bevoegde autoriteiten personeelsleden aanmoedigen eerst te proberen de interne meldingsprocedures van hun instellingen te gebruiken.

Titel V – Kader en mechanismen voor interne controle

15 Het kader voor interne controle

141. Instellingen dienen een cultuur te ontwikkelen en te handhaven die een positieve houding jegens risicobeheersing en naleving binnen de instelling aanmoedigt, evenals een robuust en alomvattend kader voor interne controle. Krachtens dit kader dienen de bedrijfsonderdelen van instellingen verantwoordelijk te zijn voor het beheren van de risico's die zij lopen bij het uitvoeren van hun activiteiten en dienen zij over controles te beschikken die de naleving van interne en externe vereisten waarborgen. Als onderdeel van dit kader dienen instellingen te beschikken over interne controlefuncties met passend en voldoende gezag, status en toegang tot het leidinggevend orgaan om hun taak te vervullen, evenals over een risicobeheerkader.

142. Het kader voor interne controle van instellingen dient op individuele basis te worden aangepast aan het specifieke karakter van hun activiteiten, hun complexiteit en de bijbehorende risico's, rekening houdend met de groepscontext. Instellingen dienen de uitwisseling van de benodigde informatie te organiseren op een wijze die waarborgt dat elk leidinggevend orgaan, elk bedrijfsonderdeel en elke interne eenheid, waaronder elke interne controlefunctie, in staat is zijn/haar taken uit te voeren. Dit betekent bijvoorbeeld een noodzakelijke uitwisseling van adequate informatie tussen de bedrijfsonderdelen, de nalevingsfunctie en de AML/CTF-nalevingsfunctie als dat een afzonderlijke interne controlefunctie is, op groepsniveau en tussen de hoofden van de interne controlefuncties op groepsniveau en het leidinggevend orgaan van de instelling.

143. Instellingen dienen ervoor te zorgen dat zij beschikken over passende processen en procedures die waarborgen zij voldoen aan hun verplichtingen in verband met het bestrijden van witwassen van geld en terrorismefinanciering. Instellingen dienen de mate waarin zij zijn blootgesteld aan het risico dat zij worden gebruikt voor witwassen of terrorismefinanciering te beoordelen en dienen zo nodig maatregelen te nemen om die risico's en hun daarmee verband houdende operationele risico's en reputatierisico's te beperken. Instellingen dienen maatregelen te nemen om te waarborgen dat hun personeelsleden zich bewust zijn van het risico van witwassen en terrorismefinanciering en van de gevolgen daarvan voor de instelling en de integriteit van financiële systeem.

144. Het kader voor interne controle dient betrekking te hebben op de hele organisatie, met inbegrip van de verantwoordelijkheden en taken van het leidinggevend orgaan, en de activiteiten van alle bedrijfsonderdelen en interne eenheden, waaronder interne controlefuncties, uitbestede activiteiten en distributiekanalen.

145. Het kader voor interne controle van een instelling dient het volgende te waarborgen:

a. doeltreffende en efficiënte activiteiten;

b. behoedzame bedrijfsvoering;

c. adequate identificatie, meting en beperking van risico's;

d. de betrouwbaarheid van financiële en niet-financiële informatie die zowel intern als extern wordt gerapporteerd;

e. solide administratieve en boekhoudkundige procedures; en

f. naleving van wetten, regelgeving, toezichtvereisten en het interne beleid, de procedures, de regels en de besluiten van de instelling.

16 Invoering van een kader voor interne controle

146. Het leidinggevend orgaan dient verantwoordelijk te zijn voor de totstandbrenging en monitoring van de adequaatheid en doeltreffendheid van het kader voor interne controle, zijn procedures en mechanismen, en voor het toezicht op alle bedrijfsonderdelen en interne eenheden, met inbegrip van interne controlefuncties (zoals risicobeheer, naleving, AML/CTF-naleving als dat een afzonderlijke controlefunctie is, en interne auditfuncties). Instellingen dienen door het leidinggevend orgaan goed te keuren adequaat schriftelijk beleid en adequate schriftelijke mechanismen en procedures voor interne controle op te stellen, deze te handhaven regelmatig bij te werken.

147. Een instelling dient te beschikken over een duidelijk, transparant en gedocumenteerd besluitvormingsproces en te zorgen voor een heldere toewijzing van verantwoordelijkheden

en bevoegdheden binnen haar kader voor interne controle, met inbegrip van haar bedrijfsonderdelen, interne eenheden en interne controlefuncties.

148. Instellingen dienen alle personeelsleden van dit beleid en van deze mechanismen en procedures op de hoogte te stellen, evenals van belangrijke wijzigingen daarop.

149. Bij de implementatie van het kader voor interne controle dienen instellingen een adequate scheiding van taken tot stand te brengen – waarbij bijvoorbeeld conflicterende activiteiten binnen de verwerking van transacties of bij het verlenen van diensten, alsmede toezichts- en rapportageverantwoordelijkheden in verband met conflicterende activiteiten aan verschillende personen worden toegewezen – en informatiebarrières op te stellen, bijvoorbeeld door middel van de fysieke scheiding van bepaalde afdelingen.

150. De interne controlefuncties dienen te controleren of het beleid, de mechanismen en de procedures die worden uiteengezet in het kader voor interne controle, correct ten uitvoer worden gelegd in hun respectieve bevoegdheidsgebieden.

151. Interne controlefuncties dienen regelmatig schriftelijk verslag uit te brengen aan het leidinggevend orgaan over grote vastgestelde gebreken. Deze verslagen dienen voor elk nieuw vastgesteld belangrijk gebrek de relevante betrokken risico's, een effectbeoordeling, aanbevelingen en te nemen corrigerende maatregelen te bevatten. Het leidinggevend orgaan dient de bevindingen van de interne controlefuncties tijdig en doeltreffend op te volgen en toereikende herstelacties te vereisen. Er dient een formele follow-upprocedure voor bevindingen en corrigerende maatregelen te worden opgesteld.

17 Het kader voor risicobeheer

152. Instellingen behoren als onderdeel van het algehele kader voor interne controle over een holistisch, instellingsbreed kader voor risicobeheer te beschikken dat zich uitstrekt over alle bedrijfsonderdelen en interne eenheden, met inbegrip van interne controlefuncties, waarin het economische belang van al haar risicoblootstellingen ten volle wordt erkend. Het kader voor risicobeheer dient de instelling in staat te stellen om geïnformeerde besluiten te nemen inzake het nemen van risico's. Het kader voor risicobeheer dient risico's binnen en buiten de balans te omvatten, evenals feitelijke risico's en toekomstige risico's waaraan de instelling mogelijk is, of kan worden, blootgesteld. Risico's dienen bottom-up en top-down te worden beoordeeld, binnen elk bedrijfsonderdeel en over alle bedrijfsonderdelen heen, waarbij gebruik wordt gemaakt van consistente terminologie en onderling verenigbare methodieken binnen de gehele instelling en op geconsolideerd en gesubconsolideerd niveau. Het kader voor risicobeheer omvat alle relevante risico's, waarbij zowel financiële als niet-financiële risico's op passende wijze in aanmerking worden genomen, met inbegrip van krediet-, markt-, liquiditeits-, concentratie-, operationele, IT-, reputatie-, juridische en gedragsrisico's, nalevingsrisico's in verband met AML/CTF en andere financiële misdrijven, ESG-risico's en strategische risico's.

153. Het kader voor risicobeheer van een instelling dient beleid, procedures, risicolimieten en risicocontroles te bevatten die zorgen voor adequate, tijdige en permanente identificatie, meting of beoordeling, monitoring, beheer, beperking en rapportage van de risico's op het niveau van het bedrijfsonderdeel, de instelling en op geconsolideerd of gesubconsolideerd niveau.

154. Dit kader dient specifieke sturing te geven aan de uitvoering van de strategieën van de instelling. Dit betekent dat zo nodig interne limieten dienen te worden vastgesteld en gehandhaafd die stroken met de risicobereidheid van de instelling, en overeenstemmen met het deugdelijk functioneren, de financiële kracht en de strategische doelstellingen van de instelling. Het risicoprofiel van een instelling dient binnen deze vastgestelde limieten te worden gehouden. Het kader voor risicobeheer behoort te waarborgen dat, wanneer risicolimieten worden overschreden, er een vaste procedure is om daar melding van te doen en er zorg wordt gedragen voor een passende follow-upprocedure.

155. Het kader voor risicobeheer dient te worden onderworpen aan onafhankelijk intern onderzoek, dat bijvoorbeeld wordt uitgevoerd door de interne auditfunctie, en regelmatig opnieuw te worden getoetst aan de risicobereidheid van de instelling, waarbij informatie wordt meegewogen afkomstig van de risicobeheerfunctie en, indien ingesteld, het risicocomité. In aanmerking te nemen factoren zijn onder meer interne en externe ontwikkelingen, veranderingen in de balans en inkomsten, eventuele toename van de complexiteit van de bedrijfsactiviteiten van de instelling, het risicoprofiel of de werkstructuur; geografische expansie; fusies en overnames; en de introductie van nieuwe producten of bedrijfsonderdelen.

156. Instellingen dienen passende methoden te ontwikkelen voor het identificeren, meten of beoordelen van risico's, waaronder zowel toekomstgerichte als retrospectieve instrumenten. Deze methoden dienen de mogelijkheid te bieden van aggregatie van risicoblootstellingen bij alle bedrijfsonderdelen en het identificeren van risicoconcentraties te ondersteunen. De instrumenten dienen het mogelijk te maken om het feitelijke risicoprofiel af te zetten tegen de risicobereidheid van de instelling, en om potentiële risicoblootstellingen en risicoblootstellingen in stresssituaties onder een reeks voorziene ongunstige omstandigheden te identificeren en te beoordelen met inachtneming van de risicodraagkracht van de instelling. De instrumenten dienen informatie te verstrekken over iedere eventueel benodigde aanpassing van het risicoprofiel. Instellingen dienen voldoende voorzichtige aannames te doen wanneer zij stressscenario's opstellen.

157. Instellingen dienen er rekening mee te houden dat de resultaten van kwantitatieve beoordelingsmethoden, waaronder stresstests, in hoge mate afhankelijk zijn van de beperkingen en aannames van de modellen (zoals ernst en duur van de schok en onderliggende risico's). Zo kan het gebeuren dat een zeer hoog rendement van economisch kapitaal zoals vastgesteld door modellen, eerder het resultaat is van een tekortkoming in die modellen (bijv. de uitsluiting van bepaalde relevante risico's) dan het gevolg van een excellente strategie of excellente uitvoering van een strategie van de zijde van de instelling.

De bepaling van het niveau van het genomen risico dient daarom niet alleen gebaseerd te zijn op kwantitatieve informatie of uitkomsten van modellen, maar dient ook een kwalitatieve benadering te omvatten (inclusief oordelen van deskundigen en kritische analyses). Er dient expliciet aandacht te worden besteed aan belangrijke trends en gegevens betreffende het macro-economische klimaat om hun potentiële effect op blootstellingen en portefeuilles in kaart te brengen.

158. De uiteindelijke verantwoordelijkheid voor risicobeoordeling berust uitsluitend bij de instelling, die haar risico's dus kritisch dient te evalueren en zich niet uitsluitend dient te verlaten op externe beoordelingen. Zo dient een instelling een ingekocht risicomodel te valideren en het vervolgens af te stemmen op haar individuele omstandigheden om ervoor te zorgen dat het model het risico accuraat en uitvoerig vastlegt en analyseert.

159. Instellingen dienen zich ten volle bewust te zijn van de beperkingen van modellen en cijfers en niet alleen kwantitatieve maar ook kwalitatieve instrumenten voor risicobeoordeling te gebruiken (inclusief oordelen van deskundigen en kritische analyses).

160. Instellingen kunnen, naast hun eigen beoordelingen, gebruikmaken van externe risicobeoordelingen (waaronder externe kredietratings of elders ingekochte risicomodellen). Instellingen dienen volledig op de hoogte te zijn van de precieze reikwijdte van dergelijke beoordelingen en hun beperkingen.

161. Er dienen mechanismen voor regelmatige en transparante rapportage te worden ingevoerd zodat het leidinggevend orgaan, zijn risicocomité, indien ingesteld, en alle relevante eenheden in een instelling op tijd accurate, beknopte, begrijpelijke en zinvolle rapporten ontvangen en zij belangrijke gegevens kunnen uitwisselen over de identificatie, meting of beoordeling, monitoring en het beheer van risico's. Het kader voor rapportage dient nauwkeurig omschreven en gedocumenteerd te worden.

162. Een doeltreffende communicatie en bewustzijn op het gebied van risico's en de risicostrategie is van cruciaal belang voor het gehele risicobeheerproces, met inbegrip van de beoordelings- en besluitvormingsprocessen, en helpt besluiten te voorkomen die het risico vergroten zonder dat men dat beseft. Een doeltreffende risicorapportage behelst dat risico's intern naar behoren in aanmerking worden genomen en dat er wordt gecommuniceerd over de risicostrategie en relevante risicogegevens (bijv. blootstellingen en belangrijke risico-indicatoren), zowel horizontaal door de instelling heen, als naar boven en naar beneden in de managementketen.

18 Nieuwe producten en ingrijpende wijzigingen[37]

163. Een instelling dient te beschikken over een duidelijk gedocumenteerd beleid voor de goedkeuring van nieuwe producten. In dit beleid, dat door het leidinggevend orgaan wordt

[37] Zie ook de EBA-richtsnoeren inzake producttoezicht- en -governanceregelingen voor ontwikkelaars en distributeurs van retailbankproducten, beschikbaar op .

goedgekeurd, dient te worden ingegaan op de ontwikkeling van nieuwe markten, producten en diensten, en ingrijpende wijzigingen van bestaande markten, evenals op buitengewone transacties. Het beleid dient daarnaast belangrijke veranderingen in daarmee verband houdende processen (bijv. nieuwe uitbestedingsregelingen) en systemen (bijv. IT-veranderingsprocessen) te omvatten. Het beleid voor de goedkeuring van nieuwe producten dient te waarborgen dat goedgekeurde producten en veranderingen in overeenstemming zijn met de risicostrategie en risicobereidheid van de instelling en de desbetreffende limieten, of dat benodigde herzieningen worden aangebracht.

164. Belangrijke veranderingen of buitengewone transacties kunnen fusies en overnames zijn, waaronder de mogelijke gevolgen van onvoldoende due diligence, waardoor risico's en verplichtingen na de fusie niet worden opgemerkt; de oprichting van structuren (bijv. nieuwe dochterondernemingen of single-purpose vehicles); nieuwe producten; wijzigingen in systemen of het kader of de procedures voor risicobeheer; en organisatorische veranderingen in de instelling.

165. Een instelling dient over specifieke procedures te beschikken voor de toetsing van de naleving van dit beleid, en dient daarbij rekening te houden met de input van de risicobeheerfunctie. Daartoe behoort ook een systematische voorafgaande beoordeling door en een onderbouwd standpunt van de nalevingsfunctie met betrekking tot nieuwe producten of ingrijpende wijzigingen van bestaande producten.

166. Het beleid voor de goedkeuring van nieuwe producten van een instelling dient alle afwegingen te omvatten die moeten worden gemaakt alvorens nieuwe markten worden betreden, in nieuwe producten wordt gehandeld, een nieuwe dienst wordt gelanceerd of bestaande producten of diensten ingrijpend worden gewijzigd. In dit beleid dient ook te worden vastgelegd welke definities van 'nieuw product', 'nieuwe markt', 'nieuwe bedrijfsactiviteiten' en 'ingrijpende wijzigingen' in de organisatie worden gebruikt en welke interne functies bij het besluitvormingsproces worden betrokken.

167. Dit beleid dient de belangrijkste thema's aan te geven die aan de orde moeten komen voordat een besluit wordt genomen. Hiertoe behoren naleving van de voorschriften, financiële verslaggeving, prijsbepalingsmodellen, het effect op het risicoprofiel, kapitaaltoereikendheid en rentabiliteit, de beschikbaarheid van adequate middelen voor front-, back- en middle-office en de beschikbaarheid van geschikte interne instrumenten en expertise om de gerelateerde risico's te begrijpen en te monitoren. De instellingen dienen bovendien, teneinde te voldoen aan hun verplichtingen uit hoofde van Richtlijn (EU) 2015/849, de aan het nieuwe product of de nieuwe handelspraktijk verbonden risico's op het gebied van witwassen en terrorismefinanciering in kaart te brengen, deze risico's te beoordelen en de te nemen maatregelen vast te stellen om ze te beperken. In het besluit om een nieuwe activiteit te initiëren dient duidelijk te worden aangegeven welke bedrijfseenheden en personen er verantwoordelijk voor zijn. Een nieuwe activiteit dient pas te worden opgestart als er voldoende hulpmiddelen beschikbaar zijn om de risico's die eraan verbonden zijn, te begrijpen en te beheersen.

168. De risicobeheerfunctie en de nalevingsfunctie dienen te worden betrokken bij de goedkeuring van nieuwe producten of bij ingrijpende wijzingen van bestaande producten, processen en systemen. Hun bijdrage dient onder andere te bestaan uit een volledige en objectieve beoordeling van risico's die uit nieuwe activiteiten voortvloeien onder verschillende scenario's, van potentiële tekortkomingen in de kaders voor risicobeheer en interne controle van de instelling, en van het vermogen van de instelling om nieuwe risico's doeltreffend te beheren. De risicobeheerfunctie dient ook een duidelijk overzicht te hebben van de uitrol van nieuwe producten (of van ingrijpende wijzigingen in bestaande producten, processen en systemen) binnen verschillende bedrijfsonderdelen en portefeuilles. Voorts dient hij of zij bevoegd te zijn om te vereisen dat wijzigingen van bestaande producten eerst behandeld worden in een formele procedure in het kader van het beleid voor de goedkeuring van nieuwe producten.

19 Interne controlefuncties

169. De interne controlefuncties dienen een risicobeheerfunctie (zie hoofdstuk 20), een nalevingsfunctie (zie hoofdstuk 21) en een interne auditfunctie (zie hoofdstuk 22) te omvatten. De risicobeheer- en de nalevingsfunctie dienen te worden gecontroleerd door de interne auditfunctie. De controlefuncties zijn er onder meer verantwoordelijk voor te waarborgen dat de AML/CFT-vereisten worden nageleefd.

170. De operationele taken van de interne controlefuncties kunnen, rekening houdend met de evenredigheidscriteria die worden genoemd in titel I, worden uitbesteed aan de consoliderende instelling of een andere entiteit binnen of buiten de groep met instemming van de leidinggevende organen van de betrokken instellingen. Zelfs wanneer operationele taken op het gebied van interne controle geheel of gedeeltelijk zijn uitbesteed, zijn het hoofd van de betrokken interne controlefunctie en het leidinggevend orgaan nog steeds verantwoordelijk voor deze activiteiten en voor de instandhouding van een interne controlefunctie binnen de instelling.

171. Onverminderd het nationale recht waarin Richtlijn 2015/849/EU wordt omgezet, dienen instellingen een personeelslid (bijv. het hoofd naleving) aan te wijzen dat verantwoordelijk is voor naleving, door de instelling, van de vereisten van die richtlijn en van haar eigen beleid en procedures. Instellingen kunnen een afzonderlijke AML/CTF-nalevingsfunctie instellen die als zelfstandige controlefunctie fungeert[38]. De voor AML/CTF verantwoordelijke dient zo nodig rechtstreeks te kunnen rapporteren aan het leidinggevend orgaan in zijn bestuursfunctie en zijn toezichtfunctie.

19.1 Hoofden van de interne controlefuncties

172. Hoofden van interne controlefuncties dienen op een zodanig hiërarchisch niveau te worden aangesteld dat zij het gezag en de status krijgen die nodig zijn om hun verantwoordelijkheden

[38] Raadpleeg ook de EBA-richtsnoeren inzake de AML/CTF-nalevingsfunctie (in ontwikkeling).

te vervullen. Niettegenstaande de algemene verantwoordelijkheid van het leidinggevend orgaan, dienen hoofden van interne controlefuncties onafhankelijk te zijn van de bedrijfsonderdelen of eenheden die zij controleren. Daartoe dienen de hoofden van de risicobeheer-, nalevings- en interne auditfuncties te rapporteren en rechtstreeks verantwoording af te leggen aan het leidinggevend orgaan, en dienen hun prestaties te worden getoetst door het leidinggevend orgaan.

173. Waar nodig kunnen de hoofden van internecontrolefuncties toegang krijgen tot en rechtstreeks rapporteren aan het leidinggevend orgaan in zijn toezichtfunctie om punten van zorg aan te kaarten en de toezichtfunctie, waar nodig, te waarschuwen wanneer specifieke ontwikkelingen gevolgen hebben of kunnen hebben voor de instelling. Dit dient de hoofden van interne controlefuncties er niet van te weerhouden eveneens te rapporteren binnen de reguliere rapportagelijnen.

174. Instellingen dienen te beschikken over gedocumenteerde processen voor de toewijzing van de functie van hoofd interne controlefunctie en voor de intrekking van zijn of haar verantwoordelijkheden. In ieder geval dienen de hoofden interne controlefuncties – en krachtens artikel 76, lid 5, van Richtlijn 2013/36/EU het hoofd van de risicobeheerfunctie – niet zonder voorafgaande goedkeuring van het leidinggevend orgaan in diens toezichtfunctie uit hun functie te worden verwijderd. In significante instellingen dienen bevoegde autoriteiten direct geïnformeerd te worden over de goedkeuring en de belangrijkste redenen voor de verwijdering van een hoofd van een interne controlefunctie uit zijn functie.

19.2 Onafhankelijkheid van interne controlefuncties

175. Om als onafhankelijk te worden aangemerkt, dienen de interne controlefuncties aan de volgende voorwaarden te voldoen:

a. hun personeelsleden verrichten geen operationele taken die vallen onder de activiteiten die de interne controlefuncties behoren te monitoren en controleren;

b. ze zijn organisatorisch gescheiden van de activiteiten die zij dienen te monitoren en controleren;

c. niettegenstaande de algemene verantwoordelijkheid van de leden van het leidinggevend orgaan voor de instelling, is het hoofd van een interne controlefunctie niet ondergeschikt aan een persoon die verantwoordelijk is voor het beheer van de activiteiten die de interne controlefunctie monitort en controleert;

d. de beloning van personeel van de interne controlefunctie mag niet gekoppeld zijn aan de prestaties van de activiteiten die door de interne controlefunctie worden

gemonitord en gecontroleerd, of anderszins zijn of haar objectiviteit denkelijk ondermijnen[39].

19.3 Combinatie van interne controlefuncties

176. Rekening houdend met de evenredigheidscriteria die worden genoemd in titel I, kunnen de risicobeheerfunctie en de nalevingsfunctie worden gecombineerd. De interne auditfunctie dient niet te worden gecombineerd met een andere interne controlefunctie.

19.4 Personele middelen van interne controlefuncties

177. Interne controlefuncties dienen over voldoende personele middelen te beschikken. Zij dienen te beschikken over een toereikend aantal gekwalificeerde personeelsleden (zowel bij het moederbedrijf als bij een dochteronderneming). Het personeel dient continu gekwalificeerd te blijven en zo nodig te worden opgeleid.

178. Interne controlefuncties dienen te beschikken over passende IT-systemen en ondersteuning en toegang te hebben tot de interne en externe informatie die nodig zijn om hun verantwoordelijkheden na te komen. Zij dienen toegang te hebben tot alle benodigde informatie over alle bedrijfsonderdelen en relevante risicodragende dochterondernemingen, met name die welke potentieel belangrijke risico's voor de instellingen kunnen voortbrengen.

20 Risicobeheerfunctie

179. Instellingen dienen een risicobeheerfunctie in te stellen die de hele instelling bestrijkt. De risicobeheerfunctie dient over voldoende gezag, status en middelen te beschikken, rekening houdend met de evenredigheidscriteria die worden genoemd in titel I, om het risicobeleid en het risicobeheerkader ten uitvoer te leggen zoals uiteengezet in hoofdstuk 17.

180. De risicobeheerfunctie dient, indien nodig, rechtstreeks toegang te hebben tot het leidinggevend orgaan in zijn toezichtfunctie en zijn comités, indien ingesteld, waaronder met name het risicocomité.

181. De risicobeheerfunctie dient toegang te hebben tot alle bedrijfsonderdelen en andere interne eenheden die potentieel risico's kunnen genereren, evenals tot relevante dochterondernemingen en gelieerde bedrijven.

182. Personeel binnen de risicobeheerfunctie dient over voldoende kennis, vaardigheden en ervaring te beschikken wat betreft risicobeheertechnieken en -procedures, markten en producten, en dient toegang te hebben tot regelmatige opleiding.

183. De risicobeheerfunctie dient onafhankelijk te zijn van de bedrijfsonderdelen en -eenheden waarvan zij de risico's controleert, maar dient niet belet te worden daarmee onderling contact

[39] Zie ook de EBA-richtsnoeren betreffende een beheerst beloningsbeleid, beschikbaar op .

te onderhouden. Een wisselwerking tussen de operationele functies en de risicobeheerfunctie dient bij te dragen aan het bereiken van de beoogde situatie waarin alle werknemers van de instelling verantwoordelijkheid dragen voor risicobeheer.

184. De risicobeheerfunctie dient organisatorisch centraal in de instelling te staan en zodanig ingericht te zijn dat risicobeleid kan worden uitgevoerd en het kader voor risicobeheer kan worden gecontroleerd . De risicobeheerfunctie dient een belangrijke rol te spelen bij de verwezenlijking van doeltreffende risicobeheerprocessen in de instelling. De risicobeheerfunctie dient actief betrokken te zijn bij alle belangrijke risicobeheerbesluiten.

185. Significante instellingen kunnen overwegen om voor elk relevant bedrijfsonderdeel een specifieke risicobeheerfunctie in te stellen. Er dient echter een centrale risicobeheerfunctie, waaronder een groepsrisicobeheerfunctie in de consoliderende instelling, te bestaan om te zorgen voor een instellings- en groepsbreed holistisch perspectief op alle risico's en om te waarborgen dat aan de risicostrategie wordt voldaan.

186. De risicobeheerfunctie dient belangrijke onafhankelijke informatie, alsmede analyses en deskundige oordelen over risicoblootstellingen te verstrekken. Daarnaast dient zij advies uit te brengen over voorstellen die zijn gedaan en risicobesluiten die zijn genomen door bedrijfsonderdelen of interne eenheden, en dient zij het leidinggevend orgaan ervan op de hoogte te stellen of de besluiten stroken met de risicostrategie en risicobereidheid van de instelling. De risicobeheerfunctie kan aanbevelingen doen voor de verbetering van het kader voor risicobeheer en voor corrigerende maatregelen in het geval van overtredingen van beleid, procedures en limieten.

20.1 De rol van de risicobeheerfunctie in de risicostrategie en -besluiten

187. De risicobeheerfunctie dient in een vroeg stadium actief te worden betrokken bij de uitwerking van de risicostrategie van de instelling en bij de verwezenlijking van doeltreffende risicobeheerprocessen in de instelling. De risicobeheerfunctie dient het leidinggevend orgaan alle relevante risicogerelateerde informatie te verschaffen op basis waarvan dit orgaan de risicobereidheid van de instelling kan vaststellen. De risicobeheerfunctie dient de degelijkheid en duurzaamheid van de risicostrategie en -bereidheid te beoordelen. Zij dient ervoor te zorgen dat de risicobereidheid naar behoren wordt vertaald naar specifieke risicolimieten. De risicobeheerfunctie dient ook de risicostrategieën en risicobereidheid van bedrijfseenheden te beoordelen, waaronder de voorgestelde streefcijfers van de bedrijfseenheden, en dient door het leidinggevend orgaan te worden betrokken bij de besluitvorming over de risicostrategieën en -bereidheid. Streefcijfers dienen geloofwaardig te zijn en te stroken met de risicostrategie van de instelling.

188. De betrokkenheid van de risicobeheerfunctie bij besluitvormingsprocessen dient te waarborgen dat risicobeoordelingen naar behoren in aanmerking worden genomen. De

verantwoordingsplicht voor genomen beslissingen dienen evenwel bij de bedrijfs- en interne eenheden en uiteindelijk bij het leidinggevend orgaan te berusten.

20.2 De rol van de risicobeheerfunctie bij belangrijke veranderingen

189. Overeenkomstig hoofdstuk 18 dient de risicobeheerfunctie te worden betrokken bij de beoordeling van het effect van belangrijke veranderingen en buitengewone transacties op het risico voor de instelling en de groep als geheel voordat er besluiten over worden genomen, en dient zij haar bevindingen ook rechtstreeks aan het leidinggevend orgaan te rapporteren voordat een besluit wordt genomen.

190. De risicobeheerfunctie dient te beoordelen in hoeverre geïdentificeerde risico's het vermogen van de instelling of groep beïnvloeden om zijn of haar risicoprofiel, liquiditeit, en solide kapitaalbasis te beheren onder normale en ongunstige omstandigheden.

20.3 De rol van de risicobeheerfunctie bij het identificeren, meten, beoordelen, beheren, beperken, monitoren en rapporteren van risico's

191. De risicobeheerfunctie dient te zorgen voor een passend kader voor risicobeheer en te waarborgen dat alle risico's worden geïdentificeerd, beoordeeld, gemeten, gemonitord, beheerd en naar behoren worden gerapporteerd door de relevante eenheden in de instelling.

192. De risicobeheerfunctie dient ervoor te zorgen dat identificatie en beoordeling niet uitsluitend worden gebaseerd op kwantitatieve informatie of uitkomsten van modellen, maar ook een kwalitatieve benadering omvatten. De risicobeheerfunctie dient het leidinggevend orgaan op de hoogte te houden van de aannames die worden gebruikt in en de potentiële tekortkomingen van de risicomodellen en analyses.

193. De risicobeheerfunctie dient te waarborgen dat transacties met betrokken partijen worden getoetst en dat de risico's ervan voor de instelling worden geïdentificeerd en naar behoren worden beoordeeld.

194. De risicobeheerfunctie dient te waarborgen dat alle geïdentificeerde risico's doeltreffend worden gemonitord door de bedrijfseenheden.

195. De risicobeheerfunctie dient regelmatig toe te zien op het werkelijke risicoprofiel van de instelling en dit te toetsen aan de strategische doelstellingen en risicobereidheid van de instelling teneinde het leidinggevend orgaan in zijn bestuursfunctie in staat te stellen om besluiten te nemen en het leidinggevend orgaan in zijn toezichtfunctie in staat te stellen zijn controlerende taak uit te oefenen.

196. De risicobeheerfunctie dient trends te analyseren en nieuwe of opkomende risico's en verhoogde risico's als gevolg van veranderende omstandigheden en randvoorwaarden te onderkennen. Deze functie dient ook de werkelijke gevolgen van risico's met de eerdere schattingen (back-testing) te vergelijken om de nauwkeurigheid en doelmatigheid van het risicobeheerproces te beoordelen en te verbeteren.

197. De risicobeheerfunctie dient mogelijke manieren om risico's te beperken te beoordelen. De rapportages aan het leidinggevend orgaan dienen voorstellen voor passende risicobeperkende maatregelen te bevatten.

20.4 De rol van de risicobeheerfunctie bij niet-goedgekeurde blootstellingen

198. De risicobeheerfunctie dient op onafhankelijke wijze overschrijdingen van risicobereidheid of risicolimieten te beoordelen (met inbegrip van het vaststellen van de oorzaak en het maken van een juridische en economische analyse van de werkelijke kosten van beëindiging, beperking of afdekking van de blootstelling, afgezet tegen de potentiële kosten van handhaving ervan). De risicobeheerfunctie dient de betrokken bedrijfseenheden en het leidinggevend orgaan te informeren, en mogelijke oplossingen aan te bevelen. Wanneer de inbreuk significant is, dient de risicobeheerfunctie rechtstreeks aan het leidinggevend orgaan in zijn toezichtfunctie te rapporteren, onverminderd de verplichting van de risicobeheerfunctie om aan andere interne functies en comités te rapporteren.

199. De risicobeheerfunctie dient een belangrijke rol te spelen bij het waarborgen dat een besluit over haar aanbeveling op het relevante niveau wordt genomen, door de relevante bedrijfseenheden wordt nageleefd, en naar behoren aan het leidinggevend orgaan en, indien ingesteld, het risicocomité wordt gerapporteerd.

20.5 Hoofd van de risicobeheerfunctie

200. Het hoofd van de risicobeheerfunctie dient verantwoordelijk te zijn voor het verstrekken van uitvoerige en begrijpelijke informatie over risico's en het adviseren van het leidinggevend orgaan, zodat dit orgaan het algehele risicoprofiel van de instelling kan begrijpen. Hetzelfde geldt voor het hoofd van de risicobeheerfunctie van een moederonderneming met betrekking tot de geconsolideerde situatie.

201. Het hoofd van de risicobeheerfunctie dient over voldoende deskundigheid, onafhankelijkheid en gezag op basis van senioriteit te beschikken om besluiten aan te vechten die van invloed zijn op de blootstelling van een instelling aan risico's. Als het hoofd van de risicobeheerfunctie geen lid is van het leidinggevend orgaan, dienen significante instellingen een onafhankelijk hoofd van de risicobeheerfunctie te benoemen die geen verantwoordelijkheden voor andere functies heeft en rechtstreeks aan het leidinggevend orgaan rapporteert. Wanneer het niet evenredig is om iemand te benoemen die uitsluitend de taak van hoofd van de risicobeheerfunctie krijgt toegewezen, kan deze functie, rekening

houdend met het evenredigheidsbeginsel dat wordt uiteengezet in titel I, worden gecombineerd met de functie van hoofd van de nalevingsfunctie, of kan zij worden vervuld door een ander lid van het hoger personeel, mits er geen belangenconflict tussen de gecombineerde functies bestaat. Deze persoon dient in ieder geval voldoende gezag, status en onafhankelijkheid te hebben (bijv. hoofd van juridische zaken).

202. Het hoofd van de risicobeheerfunctie dient in staat te zijn besluiten aan te vechten die het bestuur en het leidinggevend orgaan van de instelling hebben genomen, en de redenen van bezwaar dienen formeel te worden gedocumenteerd. Als een instelling het hoofd van de risicobeheerfunctie het recht wil verlenen een veto uit te spreken over besluiten (bijv. een krediet- of beleggingsbesluit of de vaststelling van een limiet) die worden genomen op niveaus onder het leidinggevend orgaan, dient zij de reikwijdte, de escalatie- en beroepsprocedures van zo'n vetorecht, evenals de wijze waarop het leidinggevend orgaan daarbij zal worden betrokken, te specificeren.

203. Instellingen dienen stringente procedures vast te stellen voor de goedkeuring van besluiten waarmee het hoofd van de risicobeheerfunctie het niet eens is. Het leidinggevend orgaan in zijn toezichtfunctie dient rechtstreeks te kunnen communiceren met het hoofd van de risicobeheerfunctie over belangrijke risicoproblemen, waaronder ontwikkelingen die mogelijk niet stroken met de risicostrategie en -bereidheid van de instelling.

21 Nalevingsfunctie

204. Instellingen dienen een permanente en doeltreffende nalevingsfunctie in te stellen die nalevingsrisico's beheert, en een persoon te benoemen die binnen de gehele instelling deze functie uitoefent (de nalevingsfunctionaris of hoofd naleving).

205. Wanneer het niet evenredig is om iemand te benoemen die uitsluitend de taak van hoofd van de nalevingsfunctie krijgt toegewezen, kan deze functie, rekening houdend met het in titel 1 uiteengezette evenredigheidsbeginsel, worden gecombineerd met de functie van hoofd van de risicobeheerfunctie, of kan zij worden uitgevoerd door een ander lid van het hoger personeel, mits er geen belangenconflict tussen de gecombineerde functies bestaat.

206. De nalevingsfunctie, waaronder het hoofd naleving, dient onafhankelijk te zijn van de bedrijfsonderdelen en interne eenheden die zij controleert, en dient voldoende gezag, status en middelen te hebben. Rekening houdend met de evenredigheidscriteria die zijn uiteengezet in titel I, kan deze functie worden ondersteund door of gecombineerd met de risicobeheerfunctie of andere passende functies, bijv. de juridische afdeling of personeelszaken.

207. Personeel binnen de nalevingsfunctie dient te beschikken over voldoende kennis, vaardigheden en ervaring wat betreft nalevings- en bijbehorende procedures, en toegang te hebben tot regelmatige opleiding.

208. Het leidinggevend orgaan in zijn toezichtfunctie dient toe te zien op de tenuitvoerlegging van een duidelijk gedocumenteerd nalevingsbeleid, dat aan het voltallige personeel dient te worden bekendgemaakt. Instellingen dienen een procedure op te zetten om wijzigingen in de wet- en regelgeving die van toepassing is op hun activiteiten, regelmatig te beoordelen.

209. De nalevingsfunctie dient het leidinggevend orgaan te adviseren over de maatregelen die genomen dienen te worden om de naleving van alle toepasselijke wet- en regelgeving en normen te waarborgen, en het mogelijke effect van eventuele wijzigingen in het wet- en regelgevend kader op de activiteiten en het nalevingskader van de instelling te beoordelen.

210. De nalevingsfunctie dient ervoor te zorgen dat naleving wordt bewaakt door middel van een gestructureerd en duidelijk gedefinieerd programma voor toezicht op de naleving en dat het nalevingsbeleid wordt nageleefd. De nalevingsfunctie dient te rapporteren aan het leidinggevend orgaan en in voorkomend geval met de risicobeheerfunctie te communiceren over het nalevingsrisico van de instelling en het beheer daarvan. De nalevingsfunctie en de risicobeheerfunctie dienen samen en te werken zo nodig informatie uit te wisselen om hun respectieve taken te kunnen uitvoeren. Het leidinggevend orgaan en de risicobeheerfunctie dienen bij de besluitvorming rekening te houden met de bevindingen van de nalevingsfunctie.

211. In overeenstemming met hoofdstuk 18 van deze richtsnoeren dient de nalevingsfunctie, in nauwe samenwerking met de risicobeheerfunctie en de juridische afdeling, ook te verifiëren of nieuwe producten en nieuwe procedures voldoen aan het geldende juridische kader en, zo nodig, aan bekende op handen zijnde wijzigingen in de wet- en regelgeving en toezichtvereisten.

212. Instellingen dienen op passende wijze op te treden tegen intern of extern gedrag dat fraude, witwassen of terrorismefinanciering of andere financiële misdrijven en inbreuken op de voorschriften (zoals inbreuken op interne procedures en inbreuken op limieten) in de hand kan werken of mogelijk kan maken.

213. Instellingen dienen ervoor te zorgen dat hun dochterondernemingen en bijkantoren maatregelen nemen om te waarborgen dat hun activiteiten voldoen aan lokale wet- en regelgeving. Als lokale wet- en regelgeving de toepassing van door de groep ingestelde striktere procedures en nalevingssystemen in de weg staat, vooral wanneer die de openbaarmaking en uitwisseling van noodzakelijke informatie tussen entiteiten binnen de groep verhindert, stellen dochterondernemingen en bijkantoren de nalevingsfunctionaris of het hoofd naleving van de consoliderende instelling hiervan op de hoogte.

22 Interne auditfunctie

214. Instellingen dienen een onafhankelijke en doeltreffende interne auditfunctie (IAF) in te stellen, rekening houdend met de in titel I uiteengezette evenredigheidsbeginselen, en dienen een persoon te benoemen die binnen de gehele instelling verantwoordelijk is voor deze functie. De IAF dient onafhankelijk te zijn en over voldoende gezag, status en middelen te

beschikken. De instelling dient er in het bijzonder voor te zorgen dat de kwalificatie van de personeelsleden en de middelen van de IAF, met name haar controle-instrumenten en risico-analysemethoden, toereikend zijn voor de omvang en locaties van de instelling, en voor de aard, schaal en complexiteit van de risico's die inherent zijn aan het bedrijfsmodel, de werkzaamheden, de risicocultuur en de risicobereidheid van de instelling.

215. De IAF dient onafhankelijk te zijn van de gecontroleerde activiteiten. De interne auditfunctie dient daarom niet met andere functies te worden gecombineerd.

216. De IAF dient, op grond van een op risico's gebaseerde benadering, op onafhankelijke wijze een oordeel te geven en op objectieve wijze zekerheid te verschaffen dat alle activiteiten en eenheden van een instelling, met inbegrip van uitbestede activiteiten, het beleid en de procedures van de instelling en de wettelijke vereisten naleven. Elke entiteit binnen de groep dient onder de IAF te ressorteren.

217. De IAF dient niet betrokken te zijn bij het ontwerpen, selecteren, tot stand brengen en uitvoeren van specifiek beleid en specifieke mechanismen en procedures voor interne controle, en risicolimieten. Dit dient het leidinggevend orgaan in zijn bestuursfunctie er echter niet van te weerhouden om input te vragen van interne audit over kwesties die verband houden met risico's, interne controles en naleving van toepasselijke regels.

218. De IAF dient te beoordelen of het kader voor interne controle van de instelling zoals dat is uiteengezet in hoofdstuk 15 zowel effectief als doeltreffend is. De IAF dient in het bijzonder het volgende te beoordelen:

a. de geschiktheid van het governancekader van de instelling;

b. of bestaand beleid en bestaande procedures toereikend blijven en voldoen aan juridische en regelgevingsvereisten en aan de risicostrategie en risicobereidheid van de instelling;

c. of de procedures in overeenstemming zijn met de toepasselijke wet- en regelgeving en met besluiten van het leidinggevend orgaan;

d. of de procedures op correcte en doeltreffende wijze worden uitgevoerd (bijv. nakoming van transacties, het risiconiveau dat daadwerkelijk wordt bereikt enz.); en

e. de toereikendheid, kwaliteit en doeltreffendheid van de controles die worden uitgevoerd door en de verslaglegging die wordt gedaan door de diverse bedrijfsonderdelen en de risicobeheer- en nalevingsfuncties.

219. De IAF dient met name de integriteit van de processen te controleren en daarbij de betrouwbaarheid te waarborgen van de methoden en technieken, en de aannames en informatiebronnen die in de interne modellen van de instelling worden gebruikt (bijv.

risicomodellering en boekhoudkundige metingen). Voorts dient de IAF de kwaliteit en het gebruik van de instrumenten voor kwalitatieve risico-identificatie en -beoordeling en de genomen risicobeperkende maatregelen te beoordelen.

220. De IAF dient onbelemmerde instellingsbrede toegang te hebben tot alle gegevens, documenten, informatie en gebouwen van de instelling. Daartoe behoort ook toegang tot managementinformatiesystemen en notulen van alle comités en besluitvormingsorganen.

221. De IAF dient nationale en internationale beroepsnormen in acht te nemen. Een voorbeeld hiervan zijn de normen zoals vastgesteld door het Institute of Internal Auditors.

222. Werkzaamheden in het kader van de interne-auditfunctie dienen te worden verricht op basis van een auditplan en een gedetailleerd op risico's gebaseerd auditprogramma.

223. Ten minste eenmaal per jaar dient een intern auditplan te worden opgesteld op basis van de jaarlijkse interne audit-controledoelstellingen. Het interne auditplan dient te worden goedgekeurd door het leidinggevend orgaan.

224. Alle auditaanbevelingen dienen op de passende managementniveaus te worden onderworpen aan een formele follow-upprocedure om de doeltreffende en tijdige omzetting ervan te waarborgen en rapporteren.

Titel VI – Beheer van de bedrijfscontinuïteit[40]

225. Instellingen dienen een gedegen bedrijfscontinuïteitsbeheer- en herstelplan op te stellen dat ervoor zorgt dat zij op permanente basis kunnen opereren en dat verliezen door ernstige verstoringen van de bedrijfsactiviteiten worden beperkt.

226. Instellingen kunnen een specifieke onafhankelijke bedrijfscontinuïteitsfunctie instellen, bijv. als onderdeel van de risicobeheerfunctie[41].

227. De bedrijfsvoering van een instelling is afhankelijk van verscheidene kritieke hulpmiddelen (bijv. IT-systemen met inbegrip van clouddiensten, communicatiesystemen, cruciale personeelsleden en gebouwen). Het doel van bedrijfscontinuïteitsbeheer is het beperken van operationele, financiële, juridische en reputatiegevolgen en andere ingrijpende gevolgen van een ramp of langdurige onderbreking in het functioneren van deze hulpmiddelen en, als gevolg daarvan, de verstoring van de normale bedrijfsprocessen van de instelling. Andere vormen van risicobeheermaatregelen kunnen bedoeld zijn om de kans op dergelijke incidenten te verkleinen of de financiële gevolgen ervan over te dragen op derden (bijv. door het afsluiten van verzekeringen).

[40] Instellingen worden ook verwezen naar de EBA-richtsnoeren betreffende ICT-risico's, beschikbaar op:

[41] Zie ook artikel 312 van Verordening (EU) nr. 575/2013.

228. Om een gedegen bedrijfscontinuïteitsbeheerplan te kunnen vaststellen, dient de instelling zorgvuldig de risicofactoren ten aanzien van, en haar blootstelling aan, ernstige bedrijfsonderbrekingen te analyseren en een beoordeling te maken van de hieruit volgende potentiële effecten (in zowel kwantitatief als kwalitatief opzicht). Daarbij dienen interne en/of externe onderzoeken van gegevens en scenario's te worden benut. In deze analyse dienen alle bedrijfs- en interne eenheden aan bod te komen, met inbegrip van de risicobeheerfunctie, en moet rekening worden gehouden met hun onderlinge afhankelijkheid en verwevenheid. De resultaten van de analyse dienen bij te dragen aan de bepaling van de herstelprioriteiten en -doelstellingen van de instelling.

229. Op basis van bovengenoemde analyse dient een instelling de volgende plannen op te stellen:

a. noodplannen en bedrijfscontinuïteitsplannen die ervoor zorgen dat de instelling passend op noodsituaties reageert en in staat is haar belangrijkste bedrijfsactiviteiten doorgang te laten vinden indien zich een onderbreking van de normale bedrijfsprocedures voordoet; en

b. herstelplannen voor kritieke hulpbronnen die de instelling in staat stellen de normale bedrijfsprocedures binnen een gepaste termijn te hervatten. Eventuele restrisico's voortkomend uit potentiële verstoringen in de bedrijfsvoering dienen te stroken met de risicobereidheid van de instelling.

230. Noodplannen, bedrijfscontinuïteitsplannen en herstelplannen dienen te worden gedocumenteerd en nauwgezet ten uitvoer te worden gelegd. De documentatie dient beschikbaar te zijn in de bedrijfsonderdelen en interne eenheden en bij de risicobeheerfunctie. Voorts dient de documentatie te worden opgeslagen in fysiek van elkaar gescheiden systemen en in noodgevallen gemakkelijk toegankelijk te zijn. Er dient te worden gezorgd voor gepaste opleiding. Plannen dienen regelmatig te worden getest en bijgewerkt. Tekortkomingen of fouten in de testen dienen te worden gedocumenteerd en geanalyseerd, waarna de plannen dienen te worden herzien.

Titel VII – Transparantie

231. Strategieën, beleid en procedures dienen aan al het relevante personeel in een instelling te worden meegedeeld. Het personeel van een instelling dient het beleid en de procedures die relevant zijn voor hun taken en verantwoordelijkheden, te begrijpen en na te leven.

232. Bijgevolg dient het leidinggevend orgaan de relevante werknemers op duidelijke en samenhangende wijze in te lichten en van recente informatie te voorzien over de strategieën en beleidsmaatregelen, in ieder geval voor zover dit nodig is om het personeel in staat te stellen zijn taken uit te voeren. De informatie kan worden aangereikt door middel van schriftelijke richtsnoeren, handboeken of andere middelen.

233. Waar moederondernemingen er door bevoegde autoriteiten uit hoofde van artikel 106, lid 2, van Richtlijn 2013/36/EU toe worden verplicht jaarlijks een beschrijving te publiceren van hun juridische structuur en van de governance- en organisatiestructuur van de groep instellingen, dient deze informatie per land alle entiteiten binnen de groepsstructuur te omvatten, zoals vastgelegd in Richtlijn 2013/34/EU[42].

234. Deze publicatie dient in ieder geval het volgende te bevatten:

a. een overzicht van de interne organisatie van de instellingen en de groepsstructuur zoals gedefinieerd in Richtlijn 2013/34/EU en wijzigingen daarop, met inbegrip van de belangrijkste rapportagelijnen en verantwoordelijkheden;

b. eventuele belangrijke veranderingen sinds de vorige publicatie en de datum van de belangrijke verandering;

c. nieuwe juridische, governance- of organisatiestructuren;

d. informatie over de structuur, organisatie en leden van het leidinggevend orgaan, waaronder het aantal leden en het aantal leden dat is gekwalificeerd als onafhankelijk, met vermelding van het geslacht en de duur van het mandaat van elk lid van het leidinggevend orgaan;

e. de belangrijkste verantwoordelijkheden van het leidinggevend orgaan;

f. een lijst van de comités van het leidinggevend orgaan in zijn toezichtfunctie en hun samenstelling;

g. een overzicht van het beleid inzake belangenconflicten dat van toepassing is op de instelling en op het leidinggevend orgaan;

h. een overzicht van het kader voor interne controle; en

i. een overzicht van het kader voor bedrijfscontinuïteitsbeheer.

[42] Richtlijn 2013/34/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende de jaarlijkse financiële overzichten, geconsolideerde financiële overzichten en aanverwante verslagen van bepaalde ondernemingsvormen, tot wijziging van Richtlijn 2006/43/EG van het Europees Parlement en de Raad en tot intrekking van de Richtlijnen 78/660/EEG en 83/349/EEG van de Raad (PB L 182 van 29.6.2013, blz. 19).

Bijlage I – Aspecten waarmee rekening dient te worden gehouden bij de ontwikkeling van een beleid inzake interne governance

In overeenstemming met titel III dienen instellingen rekening te houden met de volgende aspecten wanneer zij beleid en regelingen voor interne governance documenteren:

1. Aandeelhoudersstructuur
2. Groepsstructuur, indien van toepassing (juridische en functionele structuur)
3. De samenstelling en het functioneren van het leidinggevend orgaan
   a) selectiecriteria, met vermelding van de wijze waarop rekening wordt gehouden met diversiteit
   b) aantal, duur van het mandaat, roulering, leeftijd
   c) onafhankelijke leden van het leidinggevend orgaan
   d) uitvoerende leden van het leidinggevend orgaan
   e) niet-uitvoerende leden van het leidinggevend orgaan
   f) interne taakverdeling, indien van toepassing
4. Governancestructuur en organisatieschema (en de gevolgen voor de groep, indien van toepassing)
   a) gespecialiseerde comités
      i. samenstelling
      ii. functioneren
   b) bestuur, indien dat er is
      i. samenstelling
      ii. functioneren
5. Medewerkers met een sleutelfunctie
   a) hoofd van de risicobeheerfunctie
   b) hoofd van de nalevingsfunctie
   c) hoofd van de interne auditfunctie
   d) chief financial officer
   e) andere medewerkers met een sleutelfunctie
6. Het kader voor interne controle

a) beschrijving van elke functie, met inbegrip van haar organisatie, middelen, status en gezag

7. Beschrijving van de risicostrategie en het kader voor risicobeheer
8. Organisatiestructuur (en de gevolgen voor de groep, indien van toepassing)
   a) operationele structuur, bedrijfsonderdelen en toewijzing van bevoegdheden en verantwoordelijkheden
   b) uitbesteding
   c) aanbod aan producten en diensten
   d) geografisch werkterrein
   e) dienstverlening onder het stelsel van de vrijheid van dienstverrichting
   f) bijkantoren
   g) dochterondernemingen, samenwerkingsverbanden enz.
   h) gebruik van offshore centra
9. Gedragscode en gedrag (en de gevolgen voor de groep, indien van toepassing)
   a) strategische doelstellingen en bedrijfswaarden
   b) interne codes en regelgeving, preventiebeleid
   c) beleid inzake belangenconflicten
   d) klokkenluiden
10. Status van het beleid inzake interne governance, met datum
    a) ontwikkeling
    b) laatste wijziging
    c) laatste beoordeling
    d) goedkeuring door het leidinggevend orgaan.