EBA/GL/2017/11

21/03/2018

Richtsnoeren

inzake interne governance

1. Nalevings- en rapportageverplichtingen

Status van deze richtsnoeren

1. Dit document bevat richtsnoeren die 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 zich tot het uiterste inspannen om aan die richtsnoeren te voldoen.

2. Richtsnoeren geven weer wat in de opvatting van de 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 (bijvoorbeeld door hun wettelijk kader of hun toezichtprocessen aan te passen), ook wanneer richtsnoeren primair tot instellingen zijn gericht.

Kennisgevingsverplichtingen

3. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 stellen bevoegde autoriteiten EBA vóór 21/05/2018 ervan 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 compliance@eba.europa.eu onder vermelding van "EBA/GL/2017/11". Kennisgevingen worden ingediend door personen die bevoegd zijn om namens hun bevoegde autoriteiten 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 de EBA-verordening op haarwebsite 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. In deze richtsnoeren worden de regelingen, processen en mechanismen voor interne governance gespecificeerd die kredietinstellingen en beleggingsondernemingen overeenkomstig artikel 74, lid 1, van Richtlijn 2013/36/EU [2] dienen in te voeren om een doeltreffend en prudent bestuur van de instelling te garanderen.

Adressaten

6. Deze richtsnoeren zijn gericht tot bevoegde autoriteiten als gedefinieerd in artikel 4, lid 1, punt 40, van Verordening (EU) nr. 575/2013[3], met inbegrip van de Europese Centrale Bank voor zaken die verband houden met de taken die haar zijn toegewezen bij Verordening (EU) nr. 1024/2013, en tot instellingen als gedefinieerd in artikel 4, lid 1, punt 3, van Verordening (EU) nr. 575/2013.

Toepassingsgebied

7. 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 de risico's waaraan zij blootstaan of bloot kunnen komen te staan, en het kader voor interne risicobeheersing.

8. 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 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].

9. De termen 'leidinggevend orgaan in zijn bestuursfunctie' en 'leidinggevend orgaan in zijn toezichtfunctie' worden in deze richtsnoeren gebruikt zonder te refereren aan een specifieke

[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] Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen en tot wijziging van Verordening (EU) nr. 648/2012 (PB L 176 van 27.6.2013, blz. 1-337).

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

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.

10. 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), worden de personen die die uitvoerende functies op basis van die delegering uitvoeren, 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.

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

12. 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.

13. 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.

Definities

14. Tenzij anders aangegeven hebben de termen die in Richtlijn 2013/36/EU 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.
Instellingen	kredietinstellingen en beleggingsondernemingen als gedefinieerd in artikel 4, lid 1, respectievelijk punten 1 en 2, van Verordening (EU) nr. 575/2013.
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.
Medewerker met een sleutelfunctie	personen die een aanzienlijke invloed hebben op de richting die de instelling opgaat, 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 op 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. Prudentiële consolidatie omvat alle dochterondernemingen die instellingen of financiële instellingen zijn, zoals gedefinieerd in artikel 4, lid 1, respectievelijk de punten 3 en 26, van Verordening (EU) nr. 575/2013, en kunnen ook binnen en buiten de EU gevestigde ondernemingen omvatten die nevendiensten verrichten, zoals gedefinieerd in artikel 2, lid 18, van die verordening.
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 CRD-instelling	instellingen 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[5].
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] 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. Tenuitvoerlegging

Ingangsdatum

15. Deze richtsnoeren gelden met ingang van 30 juni 2018.

Intrekking

16. De EBA-richtsnoeren inzake interne governance (GL 44) van 27 september 2011 worden per 30 juni 2018 ingetrokken.

4. Richtsnoeren

Titel I – Evenredigheid

17. 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 doeltreffend worden bereikt.

18. Instellingen houden rekening met hun omvang en interne organisatie, en met de aard, schaal en complexiteit van hun activiteiten, wanneer zij regelingen voor interne governance ontwikkelen en ten uitvoer leggen. Significante instellingen dienen geavanceerdere governanceregelingen te hebben, terwijl kleine en minder complexe instellingen eenvoudiger governanceregelingen ten uitvoer kunnen leggen.

19. Ten behoeve van de toepassing van het evenredigheidsbeginsel en om een passende tenuitvoerlegging van de vereisten te waarborgen, dienen instellingen en bevoegde autoriteiten rekening te houden met de volgende criteria:

    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 beursgenoteerd is of niet;

    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 1 bij Richtlijn 2013/36/EU en bijlage 1 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. particulieren, bedrijven, mkb/kmo's, institutionele cliënten, overheden) en de complexiteit van de producten of contracten;

k. de uitbestede activiteiten en distributiekanalen; en

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

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

1 Rol en verantwoordelijkheden van het leidinggevend orgaan

20. 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.

21. De taken van het leidinggevend orgaan dienen duidelijk omschreven te zijn, waarbij een onderscheid wordt gemaakt tussen de taken van de bestuursfunctie (uitvoerend) en die van de toezichthoudende functie (niet-uitvoerend). De verantwoordelijkheden en taken van het leidinggevend orgaan worden omschreven in een schriftelijk document en dienen naar behoren te zijn goedgekeurd door het leidinggevend orgaan.

22. Alle leden van het leidinggevend orgaan zijn volledig op de hoogte van de structuur en verantwoordelijkheden van het leidinggevend orgaan, en van de taakverdeling tussen verschillende functies van het leidinggevend orgaan en zijn comités. Om over passende controlemechanismen te beschikken mag de besluitvorming binnen het orgaan niet worden gedomineerd door één lid of een kleine groep leden. Er dient een doeltreffende interactie te zijn tussen het leidinggevend orgaan in zijn toezichtfunctie en het leidinggevend orgaan in zijn bestuursfunctie. Beide functies verstrekken elkaar voldoende informatie om hun respectieve taken te kunnen uitvoeren.

23. Tot de verantwoordelijkheden van het leidinggevend orgaan 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, met inbegrip van de risicobereidheid van de instelling en haar kader voor risicobeheer en maatregelen die ervoor moeten zorgen dat het leidinggevend orgaan voldoende tijd besteedt aan risicoaangelegenheden;

c. een adequaat en doeltreffend kader voor interne governance en interne controle, dat een heldere organisatiestructuur omvat evenals goed functionerende onafhankelijke interne risicobeheers-, nalevings- en auditfuncties met voldoende gezag, status en middelen om hun functies te vervullen;

d. de hoeveelheid, typen en verdeling van intern kapitaal en wettelijk verplicht kapitaal 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 beheerst beloningsbeleid krachtens artikel 74, lid 3, en artikel 75, lid 2, van Richtlijn 2013/36/EU[6];

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[7];

h. een selectie- en geschiktheidsbeoordelingsproces voor medewerkers met een sleutelfunctie[8];

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;

[6] 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).

[7] 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.

[8] 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.

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.

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

25. Alle leden van het leidinggevend orgaan zijn op de hoogte 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 bewaakt eventuele geïdentificeerde zwakke punten in de tenuitvoerlegging van processen, strategieën en beleid met betrekking tot de in de paragrafen 23 en 24 genoemde verantwoordelijkheden, evalueert deze periodiek en pakt ze aan. Het kader voor interne governance en de tenuitvoerlegging daarvan worden periodiek 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 is actief betrokken bij de activiteiten van een instelling en neemt besluiten op grond van een goede kennis van zaken.

29. Het leidinggevend orgaan in zijn bestuursfunctie is verantwoordelijk voor de tenuitvoerlegging van de strategieën die het leidinggevend orgaan heeft vastgesteld en bespreekt de tenuitvoerlegging en passendheid van die strategieën regelmatig 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 stelt voorstellen, toelichtingen en ontvangen informatie op constructieve wijze ter discussie en beoordeelt deze kritisch wanneer het een oordeel velt en besluiten neemt. Het leidinggevend orgaan in zijn bestuursfunctie brengt uitvoerig verslag uit aan het leidinggevend orgaan in zijn toezichtfunctie van, en informeert dit orgaan indien nodig zonder onnodig uitstel 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.

3 Toezichthoudende functie van het leidinggevend orgaan

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

32. 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.

33. Onverminderd de verantwoordelijkheden die hem zijn toegekend overeenkomstig het toepasselijke nationale ondernemingsrecht, 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- en 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, met inbegrip van haar risicobereidheid en 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 soortgelijk 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

34. De voorzitter van het leidinggevend orgaan geeft leiding aan het leidinggevend orgaan, draagt bij aan een doeltreffende informatiestroom binnen het leidinggevend orgaan en tussen het leidinggevend orgaan en zijn comités, indien die zijn opgericht, en is verantwoordelijk voor het algehele doeltreffende functioneren.

35. 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.

36. Als algemeen principe geldt dat de voorzitter van het leidinggevend orgaan een niet-uitvoerend lid is. 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.

37. De voorzitter stelt de agenda's van vergaderingen vast en zorgt ervoor dat strategische kwesties met voorrang worden besproken. Hij of zij waarborgt dat besluiten van het leidinggevend orgaan worden genomen op grond van een goede kennis van zaken en dat documenten en informatie ruim vóór de vergadering worden ontvangen.

38. De voorzitter van het leidinggevend orgaan draagt bij 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

39. 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- [9] en beloningscomités [10] 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.

40. 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.

41. Instellingen kunnen, rekening houdend met de criteria die worden uiteengezet in titel I van deze richtsnoeren, andere comités instellen (bijv. comités op het gebied van ethiek, gedrag of naleving).

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

[9] 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.

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

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

44. Comités ondersteunen de toezichthoudende functie op specifieke gebieden en bevorderen de ontwikkeling en uitvoering van een solide kader voor interne governance. 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[11]

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

46. Onafhankelijke leden [12] van het leidinggevend orgaan in zijn toezichtfunctie zijn actief betrokken bij comités.

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

48. Instellingen zorgen ervoor, 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.

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

50. De risico- en benoemingscomités dienen te bestaan uit niet-uitvoerende leden van het leidinggevend orgaan in zijn toezichtfunctie van de betrokken instelling. Het auditcomité wordt samengesteld op de wijze beschreven in artikel 41 van Richtlijn 2006/43/EG [13]. Het beloningscomité wordt samengesteld zoals beschreven in paragraaf 2.4.1 van de EBA-richtsnoeren betreffende een beheerst beloningsbeleid[14].

[11] Deze paragraaf 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.

[12] 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.

[13] 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. 8756) laatstelijk gewijzigd bij Richtlijn 2014/56/EU van het Europees Parlement en de Raad van 16 april 2014.

[14] 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).

51. In MSI's en ASI's is de meerderheid van de leden van het benoemingscomité onafhankelijk en wordt dit comité voorgezeten door een onafhankelijk lid. In andere significante instellingen, als door bevoegde autoriteiten of het nationale recht bepaald, heeft het benoemingscomité voldoende onafhankelijke leden; dergelijke instellingen kunnen het eveneens als een goede praktijk beschouwen een voorzitter van het benoemingscomité te hebben die onafhankelijk is.

52. Leden van het benoemingscomité beschikken, zowel individueel als gezamenlijk, over voldoende kennis, vaardigheden en deskundigheid op het gebied van het selectieproces en geschiktheidsvereisten.

53. In MSI's en ASI's is de meerderheid van de leden van het risicocomité onafhankelijk. In MSI's en ASI's wordt het risicocomité voorgezeten door een onafhankelijk lid. In andere significante instellingen, als door bevoegde autoriteiten of het nationale recht bepaald, heeft het risicocomité voldoende onafhankelijke leden en wordt dit comité waar mogelijk voorgezeten door een onafhankelijk lid. In geen enkele instelling mag de voorzitter van het risicocomité tevens de voorzitter van het leidinggevend orgaan of de voorzitter van enig ander comité zijn.

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

5.3 Processen van comités

55. Comités brengen regelmatig verslag uit aan het leidinggevend orgaan in zijn toezichtfunctie.

56. Er dient een passende wisselwerking te zijn tussen comités. Met inachtneming van punt 48 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.

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

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

59. Het risico- en benoemingscomité zorgen er in ieder geval voor dat zij:

    a. toegang hebben tot alle relevante informatie en gegevens die zij nodig hebben om hun rol te vervullen, met inbegrip van informatie en gegevens van relevante bedrijfs- en controlefuncties (bijv. juridische zaken, financiën, personeelszaken, IT, risico's, naleving, audit, enz.);

    b. regelmatig rapporten, ad hoc informatie, 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 die mogelijk hebben plaatsgevonden, met gedetailleerde informatie over en aanbevelingen voor corrigerende maatregelen die zijn genomen, moeten worden genomen of worden voorgesteld;

c. periodiek de inhoud, vorm en frequentie van de risicogerelateerde informatie die aan hen wordt gerapporteerd, evalueren en besluiten daarover nemen; en

d. 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

60. 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 risicobereidheid en risicostrategie 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;

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 [15] . Het risicocomité beoordeelt de risico's die samenhangen met de aangeboden financiële producten en diensten en houdt rekening 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.

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

62. Wanneer er een risicocomité is ingesteld, onderzoekt dit, onverminderd de taken van het beloningscomité, of de stimulansen die worden gegeven door het beloningsbeleid en de beloningspraktijken rekening houden met het risico, het kapitaal, de liquiditeit en de waarschijnlijkheid en het tijdstip van winsten van de instelling.

5.5 Taken van het auditcomité

63. Overeenkomstig Richtlijn 2006/43/EG[16] 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;

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[17], en met name

[15] Zie ook de EBA-richtsnoeren inzake producttoezicht- en -governanceregelingen voor retailbanken, beschikbaar op http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products.

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

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

64. 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.

65. 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.

66. 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[18].

[18] 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.

Titel III – Kader voor governance

6 Organisatiekader en -structuur

6.1 Organisatiekader

67. Het leidinggevend orgaan van een instelling zorgt voor een passende en transparante organisatie- en operationele structuur voor die instelling en heeft daar een schriftelijke beschrijving van. 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 zorgt ervoor 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, zijn helder, welomschreven, samenhangend en afdwingbaar, en zijn adequaat gedocumenteerd. De documentatie wordt wanneer nodig bijgewerkt.

68. De structuur van de instelling mag 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 belemmeren.

69. Het leidinggevend orgaan beoordeelt 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

70. 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 de risicobereidheid.

71. Het leidinggevend orgaan is verantwoordelijk 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, mogen hun aantal en in het bijzonder de onderlinge verbindingen en transacties tussen hen geen knelpunten 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 zorgt ervoor 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 de

medewerkers, de aandeelhouders en andere belanghebbenden van de instelling en voor de bevoegde autoriteit.

72. Het leidinggevend orgaan geeft sturing aan de structuur van de instelling alsmede haar ontwikkeling en beperkingen en zorgt ervoor dat de structuur gerechtvaardigd, efficiënt en niet nodeloos complex is.

73. 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 zorgt ervoor 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.

74. Het leidinggevend orgaan van een consoliderende instelling zorgt ervoor 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 worden gedocumenteerd en beschikbaar gesteld aan de betrokken relevante functies, waaronder het leidinggevend orgaan, bedrijfsonderdelen en interne controlefuncties. De leden van het leidinggevend orgaan van een consoliderende instelling zorgen ervoor 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 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 ontvangen; en

    c. periodieke rapporten ontvangen over terreinen waarop het regelgevingskader naleving eist op individueel, gesubconsolideerd en geconsolideerd niveau.

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

75. Instellingen vermijden het opzetten van complexe en potentieel niet-transparante structuren. Instellingen houden bij hun besluitvorming rekening met de resultaten van een risicobeoordeling aan de hand waarvan wordt vastgesteld of dergelijke structuren zouden kunnen worden gebruikt voor het witwassen van geld of andere financiële misdrijven, en met de respectieve controles en het toepasselijke rechtskader[19]. Daartoe houden instellingen ten minste rekening met:

    a. de mate waarin het rechtsgebied waarin de structuur wordt opgezet daadwerkelijk voldoet aan EU- en internationale normen inzake belastingtransparantie, het witwassen van geld en de bestrijding van terrorismefinanciering;

    b. de mate waarin de structuur een duidelijk economisch en legaal 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.

76. In ieder geval dienen instellingen geen ondoorzichtige of nodeloos complexe structuren op te zetten die geen duidelijk economische reden of juridisch doel hebben, of als instellingen bang zijn dat deze structuren zouden kunnen worden gebruikt voor een doel dat verband houdt met financiële misdrijven.

77. Wanneer dergelijke structuren worden opgezet, zorgt het leidinggevend orgaan 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 is vastgesteld en begrepen, en wanneer het leidinggevend orgaan er zeker van is dat alle belangrijke risico's,

[19] Voor meer details over de beoordeling van het landenrisico en het risico in verband met afzonderlijke producten en cliënten, dienen instellingen ook de definitieve gemeenschappelijke richtsnoeren inzake risicofactoren (wanneer die zijn uitgebracht) te raadplegen: https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence/-/regulatory-activity/consultation-paper.

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.

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

79. Het leidinggevend orgaan zorgt ervoor dat passende maatregelen worden genomen om de risico's van activiteiten binnen dergelijke structuren te vermijden of beperken. Dat betekent onder andere dat:

    a. de instelling adequaat beleid en adequate procedures en gedocumenteerde processen (bijv. toepasselijke limieten, informatievereisten) 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.

80. 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.

81. Instellingen nemen dezelfde risicobeheermaatregelen 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 externe 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 analyseren met name waarom een cliënt een bepaalde structuur wil opzetten.

7 Organisatiekader in de context van een groep

82. Overeenkomstig artikel 109, lid 2, van Richtlijn 2013/36/EU, dienen moederondernemingen en dochterondernemingen die onder deze richtlijn vallen, ervoor te zorgen dat regelingen, processen en mechanismen voor interne governance samenhang vertonen en goed geïntegreerd zijn op geconsolideerde en 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, om te zorgen voor solide governanceregelingen op een geconsolideerde en gesubconsolideerde basis. Bevoegde functies binnen de consoliderende instelling en haar dochterondernemingen hebben onderling contact en wisselen waar nuttig informatie uit. De regelingen, processen en mechanismen voor interne governance 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.

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

84. Op geconsolideerd en gesubconsolideerd niveau dient de consoliderende instelling ervoor te zorgen dat het groepsbrede governancebeleid wordt 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 zorgt de consoliderende instelling ervoor dat solide governanceregelingen zijn ingevoerd voor elke dochteronderneming en overweegt zij specifieke regelingen, processen en mechanismen wanneer bedrijfsactiviteiten niet in afzonderlijke rechtspersonen zijn georganiseerd, maar binnen een matrix van bedrijfsonderdelen die meer rechtspersonen omvat.

85. 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.

86. Moederondernemingen en hun dochterondernemingen zorgen ervoor dat de instellingen en entiteiten binnen de groep voldoen aan alle specifieke vereisten in elk relevant rechtsgebied.

87. De consoliderende instelling zorgt ervoor 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.

88. De governancevereisten van Richtlijn 2013/36/EU en 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 zorgt

ervoor 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 deze richtsnoeren.

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

8 Uitbestedingsbeleid[20]

90. Het leidinggevend orgaan keurt het uitbestedingsbeleid van een instelling goed, herziet het regelmatig en werkt het bij, waarbij het ervoor zorgt dat de benodigde wijzigingen tijdig ten uitvoer worden gelegd.

91. In het uitbestedingsbeleid wordt rekening 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 wordt dus duidelijk vastgelegd dat uitbesteding de instelling niet ontslaat van haar wettelijke verplichtingen en verantwoordelijkheden jegens haar cliënten.

92. In het beleidsdocument wordt 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.

93. Het beleid dient te vereisen dat de instelling, bij de selectie van belangrijke externe dienstverleners of bij de uitbesteding van activiteiten, rekening dient te houden met de vraag of de dienstverlener al dan niet over passende ethische normen of een gedragscode beschikt.

[20] De onderhavige richtsnoeren beperken zich tot het algemene uitbestedingsbeleid; specifieke uitbestedingsaspecten worden behandeld in de uitbestedingsrichtsnoeren van het CEBT, die binnenkort zullen worden herzien. Deze richtsnoeren zijn beschikbaar op https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing.

Titel IV – Risicocultuur en gedragsregels

9 Risicocultuur

94. Een solide 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 ontwikkelen een geïntegreerde en organisatiebrede risicocultuur 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 ontwikkelen een risicocultuur aan de hand van beleid, communicatie en opleiding van medewerkers inzake de activiteiten, de strategie en het risicoprofiel van instellingen, en stemmen hun communicatie en opleiding van medewerkers af op de verantwoordelijkheden van de medewerkers als het gaat om het nemen en beheren van risico's.

97. Medewerkers dienen zich volledig bewust te zijn van hun verantwoordelijkheden op het gebied van risicobeheer. Risicobeheer is niet uitsluitend een taak van risicospecialisten of werknemers in een interne controlefunctie. 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 berust in hoofdzaak bij de bedrijfseenheden, waarbij het leidinggevend orgaan toezicht uitoefent.

98. Een sterke risicocultuur omvat, 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 de medewerkers. De medewerkers handelen in overeenstemming met alle toepasselijke wet- en regelgeving en doen direct melding van waargenomen niet-naleving binnen of buiten de instelling (bijv. aan de bevoegde autoriteit middels een klokkenluidersprocedure). Het leidinggevend orgaan bevordert, bewaakt en beoordeelt op continue basis de risicocultuur van de instelling; houdt rekening met het effect van de risicocultuur op de financiële stabiliteit, het risicoprofiel en de solide governance van de instelling; en voert waar nodig wijzigingen door.

    b. Verantwoording: relevante medewerkers op alle niveaus kennen en begrijpen de kernwaarden van de instelling en, voor zover noodzakelijk voor hun functie, haar risicobereidheid en risicodraagkracht. Zij zijn in staat hun functies uit te oefenen en zijn zich ervan bewust 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 bevordert een klimaat van open communicatie en het daadwerkelijk ter discussie stellen van zaken waarin besluitvormingsprocessen de aanzet vormen tot een brede reeks standpunten, de gelegenheid bieden bestaande praktijken te toetsen, een constructieve kritische houding onder medewerkers aanwakkeren, en een open en constructieve betrokkenheid in de hele organisatie bevorderen.

d. Stimulansen: passende stimulansen spelen een essentiële rol in het afstemmen van risicogedrag op het risicoprofiel van de instelling en haar langetermijnbelangen[21].

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 ziet ook toe op naleving van deze normen door medewerkers. 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. De ten uitvoer gelegde normen richten zich 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.

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

a. lezers eraan te herinneren dat alle activiteiten van de instelling dienen te 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 medewerkers 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

[21] 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 https://www.eba.europa.eu/regulation-and-policy/remuneration.

financiële gegevens en financieel wangedrag, economische en financiële misdrijven (waaronder fraude, witwassen van geld en anti-trustpraktijken, financiële sancties, omkoping en corruptie, marktmanipulatie, misleidende verkopen en andere schendingen van wetgeving inzake consumentenbescherming);

d. aan te geven dat van medewerkers 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 medewerkers zich bewust zijn van de potentiële interne en externe disciplinaire maatregelen, gerechtelijke procedures en sancties die kunnen volgen op wangedrag en onaanvaardbaar gedrag.

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

11 Beleid inzake belangenconflicten op het niveau van de instelling

103. Het leidinggevend orgaan is verantwoordelijk 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.

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

105. De maatregelen van instellingen om belangenconflicten te beheren of, indien van toepassing, te beperken, worden gedocumenteerd en omvatten onder meer:

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; en

c. het vaststellen van adequate procedures voor transacties met gelieerde partijen, waarbij bijvoorbeeld wordt verlangd dat transacties plaatsvinden tegen marktconforme prijzen.

12 Beleid inzake belangenconflicten voor medewerkers[22]

106. Het leidinggevend orgaan is verantwoordelijk 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 medewerkers, met inbegrip van leden van het leidinggevend orgaan, die de vervulling van hun taken en verantwoordelijkheden negatief zouden kunnen beïnvloeden. Een consoliderende instelling houdt rekening met belangen binnen een groepsbreed beleid inzake belangenconflicten op een geconsolideerde of gesubconsolideerde basis.

107. Het beleid is erop gericht belangenconflicten van medewerkers te identificeren, met inbegrip van conflicten met e belangen van hun naaste familieleden. Instellingen houden er rekening mee 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, beoordelen instellingen hun belang en nemen zij besluiten over beperkende maatregelen en voeren ze die indien nodig uit.

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

109. Het beleid heeft in ieder geval betrekking 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 medewerker, lidmaatschap van een orgaan of eigendom van een orgaan met conflicterende belangen);

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

[22] 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.

c. persoonlijke of professionele relaties met medewerkers 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);

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.

110. 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 gebruik maakt van andere diensten van een instelling, niet tot een situatie mag leiden waarin medewerkers worden geacht een belangenconflict te hebben als zij binnen een toepasselijke 'de minimis'-drempel blijven.

111. Het beleid dient de procedures vast te leggen voor rapportage en communicatie met de functie die verantwoordelijk is in het kader van het beleid. Medewerkers hebben de plicht elke aangelegenheid die kan leiden of heeft geleid tot een belangenconflict, direct intern bekend te maken.

112. 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.

113. Het beleid zet de procedures, maatregelen, documentatievereisten en verantwoordelijkheden uiteen voor de identificatie en voorkoming van belangenconflicten, voor de beoordeling van het belang ervan en voor het nemen van beperkende maatregelen. Daartoe behoren onder meer de volgende procedures, vereisten, verantwoordelijkheden en maatregelen:

a. conflicterende activiteiten of transacties toewijzen aan verschillende personen;

b. voorkomen dat medewerkers die ook buiten de instelling actief zijn, ongepaste invloed verkrijgen binnen de instelling met betrekking tot deze 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. adequate procedures vaststellen voor transacties met betrokken partijen (instellingen kunnen onder meer overwegen te verlangen dat transacties plaatsvinden tegen marktconforme prijzen, te eisen dat alle relevante interne controleprocedures in hun totaliteit gelden voor dergelijke transacties, bindend advies te verlangen van onafhankelijke leden van het leidinggevend orgaan, de goedkeuring van aandeelhouders te verlangen voor de relevantste transacties en de blootstelling aan dergelijke transacties te beperken); en

e. 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.

114. Het beleid heeft in ieder geval betrekking op belangenconflicten op het niveau van het leidinggevend orgaan en biedt voldoende leidraden 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, in de weg zou staan. Instellingen dienen er rekening mee te houden dat belangenconflicten van invloed kunnen zijn op de onafhankelijkheid van geest van leden van het leidinggevend orgaan[23].

115. 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, documenteert de instelling de genomen beslissing, 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.

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

13 Interne meldingsprocedures

117. Instellingen voeren passend intern beleid en passende interne meldingsprocedures in om medewerkers 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.

[23] 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.

Medewerkers die een inbreuk melden, hoeven daar geen bewijs van te leveren; zij dienen er echter zo zeker van te zijn dat er voldoende reden is om een onderzoek te starten.

118. Om belangenconflicten te voorkomen dienen medewerkers inbreuken te kunnen melden buiten de reguliere rapportagelijnen om (bijv. via de compliance officer, de interne auditor of een onafhankelijke interne klokkenluidersprocedure). De meldingsprocedures waarborgen de bescherming 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 Richtlijn 95/46/EG.

119. De meldingsprocedures dienen beschikbaar te worden gesteld aan alle medewerkers in een instelling.

120. Informatie die medewerkers 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 de medewerker die een inbreuk meldt, dit verlangt, wordt de informatie anoniem 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.

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

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

123. 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 Richtlijn 95/46/EG, tenzij bekendmaking volgens het nationale recht vereist wordt in het kader van nader onderzoek of een daaropvolgende gerechtelijke procedure;

c. medewerkers 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 medewerkers 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

124. Bevoegde autoriteiten stellen doeltreffende en betrouwbare mechanismen in om medewerkers 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, -unit 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, naar vermoed wordt, voor de inbreuk verantwoordelijk zou zijn in overeenstemming met Richtlijn 95/46/EG; en

d. heldere procedures zoals beschreven in punt 123.

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

Titel V – Kader en mechanismen voor interne controle

15 Kader voor interne controle

126. Instellingen ontwikkelen en handhaven een cultuur 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, beschikken instellingen over interne controlefuncties met passend en voldoende gezag, status en toegang tot het leidinggevend orgaan om hun taak te vervullen, evenals een risicobeheerkader.

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

128. Het kader voor interne controle heeft betrekking 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.

129. Het kader voor interne controle van een instelling waarborgt:

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

130. Het leidinggevend orgaan is verantwoordelijk 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-, nalevings- en interne auditfuncties). Instellingen stellen door het leidinggevend orgaan goed te keuren, adequaat schriftelijk beleid, en adequate schriftelijke mechanismen en procedures voor interne risicobeheersing op, handhaven deze en werken ze regelmatig bij.

131. Een instelling dient te beschikken over een duidelijk, transparant en gedocumenteerd besluitvormingsproces en te zorgen voor een heldere toewijzing van verantwoordelijkheden en gezag binnen haar kader voor interne controle, met inbegrip van haar bedrijfsonderdelen, interne units en interne controlefuncties.

132. Instellingen stellen alle medewerkers van dit beleid en van deze mechanismen en procedures op de hoogte, evenals van belangrijke wijzigingen daarop.

133. Bij de implementatie van het kader voor interne controle brengen instellingen een adequate scheiding van taken tot stand – 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 stellen zij informatiebarrières op, bijvoorbeeld door middel van de fysieke scheiding van bepaalde afdelingen.

134. De interne controlefuncties 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.

135. Interne controlefuncties brengen regelmatig schriftelijk verslag uit aan het leidinggevend orgaan over grote vastgestelde gebreken. Deze verslagen bevatten voor elk nieuw groot gebrek dat wordt geconstateerd, de daarmee gepaard gaande relevante risico's, aanbevelingen en corrigerende maatregelen die dienen te worden genomen. Het leidinggevend orgaan geeft tijdig en doeltreffend gevolg aan de bevindingen van de interne controlefuncties om problemen te verhelpen. Er wordt een formele follow-upprocedure voor wat betreft bevindingen en de genomen corrigerende maatregelen ingevoerd.

17 Het kader voor risicobeheer

136. Instellingen beschikken als onderdeel van het algehele kader voor interne controle over een holistisch, instellingsbreed kader voor risicobeheer 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 stelt de instelling in staat geïnformeerde besluiten te nemen inzake het

nemen van risico's. Het kader voor risicobeheer omvat risico's binnen en buiten de balans, 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, gedrags-, nalevings- en strategische risico's.

137. Het kader voor risicobeheer van een instelling omvat beleid, procedures, risicolimieten en risicocontroles 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.

138. Dit kader geeft specifieke sturing aan de uitvoering van de strategieën van de instelling. Dit betekent dat zo nodig interne limieten 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 wordt binnen deze vastgestelde limieten gehouden. Het kader voor risicobeheer waarborgt 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.

139. Het kader voor risicobeheer wordt onderworpen aan onafhankelijk intern onderzoek, dat bijvoorbeeld wordt uitgevoerd door de interne auditfunctie, en wordt regelmatig opnieuw 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.

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

141. Instellingen houden er rekening mee 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.

142. 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.

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

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

145. Er worden mechanismen voor regelmatige en transparante rapportage 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 beheer van risico's. Het kader voor rapportage is nauwkeurig omschreven en gedocumenteerd.

146. 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[24]

147. Een instelling beschikt over een duidelijk gedocumenteerd beleid voor de goedkeuring van nieuwe producten. In dit beleid, dat door het leidinggevend orgaan wordt goedgekeurd, wordt ingegaan op de ontwikkeling van nieuwe markten, producten en diensten, en ingrijpende wijzigingen van bestaande markten, evenals op buitengewone transacties. Het beleid omvat daarnaast belangrijke veranderingen in daarmee verband houdende processen (bijv. nieuwe uitbestedingsregelingen) en systemen (bijv. IT-veranderingsprocessen). Het beleid voor de goedkeuring van nieuwe producten waarborgt dat goedgekeurde producten en veranderingen in overeenstemming zijn met de risicostrategie en risicobereidheid van de instelling en de bijbehorende limieten, of dat benodigde herzieningen worden aangebracht.

148. Belangrijke veranderingen of buitengewone transacties kunnen fusies en overnames zijn, waaronder de mogelijke gevolgen van onvoldoende due diligence, waardoor risico's en verplichtingen ná 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 organisatie.

149. Een instelling beschikt over specifieke procedures voor de toetsing van de naleving van dit beleid, en houdt daarbij rekening 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.

150. Het beleid voor de goedkeuring van nieuwe producten behandelt alle afwegingen 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 wordt ook 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.

151. Dit beleid geeft de belangrijkste thema's aan die aan de orde moeten komen voordat een besluit genomen wordt. 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. In het besluit om een nieuwe activiteit te initiëren wordt duidelijk aangegeven welke bedrijfseenheden en personen er verantwoordelijk voor zijn. Een

[24] Zie ook de EBA-richtsnoeren inzake producttoezicht- en -governanceregelingen voor retailbanken, beschikbaar op https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products.

nieuwe activiteit wordt pas opgestart bij beschikbaarheid van voldoende hulpmiddelen om de risico's die eraan verbonden zijn, te begrijpen en te beheersen.

152. De risicobeheerfunctie en de nalevingsfunctie worden betrokken bij de goedkeuring van nieuwe producten of bij ingrijpende wijzingen van bestaande producten, processen en systemen. Hun bijdrage bestaat onder andere 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 heeft ook een duidelijk overzicht van de uitrol van nieuwe producten (of van ingrijpende wijzigingen in bestaande producten, processen en systemen) binnen verschillende bedrijfsonderdelen en portefeuilles. Voorts is hij of zij bevoegd om te verlangen dat wijzigingen van bestaande producten eerst behandeld worden in een formele procedure van het beleid voor de goedkeuring van nieuwe producten.

19 Interne controlefuncties

153. De interne controlefuncties omvatten een risicobeheerfunctie (zie hoofdstuk 20), een nalevingsfunctie (zie hoofdstuk 21) en een interne auditfunctie (zie hoofdstuk 22). De risicobeheer- en de nalevingsfunctie worden gecontroleerd door de interne auditfunctie.

154. 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.

19.1 Hoofden van de interne controlefuncties

155. Hoofden van interne controlefuncties worden op een zodanig hiërarchisch niveau aangesteld dat zij het gezag en de status krijgen die nodig zijn om zijn of haar verantwoordelijkheden 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.

156. Indien nodig, dienen de hoofden interne controlefuncties toegang te kunnen krijgen tot en rechtstreeks te kunnen rapporteren aan het leidinggevend orgaan in zijn toezichtfunctie om hun bezorgdheid kenbaar te maken en de toezichtfunctie in voorkomend geval te

waarschuwen indien specifieke ontwikkelingen een negatieve invloed op de instelling hebben of zouden kunnen hebben. Dit zou de hoofden van interne controlefuncties er niet van moeten weerhouden eveneens te rapporteren binnen de reguliere rapportagelijnen.

157. Instellingen 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 worden 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 verwijderd. In significante instellingen worden bevoegde autoriteiten direct geïnformeerd 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

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

a. Hun medewerkers 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[25].

19.3 Combinatie van interne controlefuncties

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

[25] Zie ook de EBA-richtsnoeren betreffende een beheerst beloningsbeleid, beschikbaar op https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

19.4 Personele middelen van interne controlefuncties

160. Interne controlefuncties dienen over voldoende personele middelen te beschikken. Zij dienen te beschikken over een toereikend aantal gekwalificeerde medewerkers (zowel bij het moederbedrijf als bij een dochteronderneming). Het personeel moet op permanente basis gekwalificeerd zijn en blijven en zo nodig worden opgeleid.

161. 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

162. Instellingen stellen een risicobeheerfunctie in die de hele instelling bestrijkt. De risicobeheerfunctie beschikt over voldoende gezag, status en middelen, 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.

163. De risicobeheerfunctie heeft, indien nodig, rechtstreeks toegang tot het leidinggevend orgaan in zijn toezichtfunctie en zijn comités, indien ingesteld, waaronder met name het risicocomité.

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

165. Personeel binnen de risicobeheerfunctie beschikt over voldoende kennis, vaardigheden en ervaring wat betreft risicobeheertechnieken en -procedures, markten en producten, en heeft toegang tot regelmatige opleiding.

166. De risicobeheerfunctie is onafhankelijk van de bedrijfsonderdelen en -eenheden waarvan zij de risico's controleert, maar mag niet belet worden daarmee onderling contact 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.

167. De risicobeheerfunctie staat organisatorisch centraal in de instelling en is zodanig ingericht dat risicobeleid kan worden uitgevoerd en het kader voor risicobeheer kan worden gecontroleerd . De risicobeheerfunctie speelt een belangrijke rol bij de verwezenlijking van doeltreffende risicobeheerprocessen in de instelling. De risicobeheerfunctie is actief betrokken bij alle belangrijke risicobeheerbesluiten.

168. 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 zijn om te zorgen voor een instellings- en groepsbreed holistisch perspectief op alle risico's en om te waarborgen dat aan de risicostrategie wordt voldaan.

169. De risicobeheerfunctie verstrekt belangrijke onafhankelijke informatie, alsmede analyses en deskundige oordelen over risicoblootstellingen. Daarnaast brengt zij advies uit over voorstellen die zijn gedaan en risicobesluiten die zijn genomen door bedrijfsonderdelen of interne units, en stelt zij het leidinggevend orgaan ervan op de hoogte of de besluiten stroken met de risicobereidheid en -strategie 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

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

171. De betrokkenheid van de risicobeheerfunctie bij besluitvormingsprocessen waarborgt dat risicobeoordelingen naar behoren in aanmerking worden genomen. De verantwoordingsplicht voor genomen beslissingen berust evenwel bij de bedrijfs- en interne eenheden en uiteindelijk bij het leidinggevend orgaan.

20.2 De rol van de risicobeheerfunctie bij belangrijke veranderingen

172. Overeenkomstig hoofdstuk 18 wordt de risicobeheerfunctie 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 rapporteert zij haar bevindingen ook rechtstreeks aan het leidinggevend orgaan voordat een besluit wordt genomen.

173. De risicobeheerfunctie beoordeelt 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

174. De risicobeheerfunctie zorgt ervoor dat alle risico's worden geïdentificeerd, beoordeeld, gemeten, gemonitord, beheerd en naar behoren worden gerapporteerd door de relevante eenheden in de instelling.

175. De risicobeheerfunctie zorgt ervoor dat identificatie en beoordeling niet uitsluitend worden gebaseerd op kwantitatieve informatie of uitkomsten van modellen, maar ook een kwalitatieve benadering omvat. De risicobeheerfunctie houdt het leidinggevend orgaan op de hoogte van de aannames die worden gebruikt in en de potentiële tekortkomingen van de risicomodellen en analyses.

176. De risicobeheerfunctie waarborgt dat transacties met betrokken partijen worden getoetst en dat de risico's ervan voor de instelling worden geïdentificeerd en naar behoren worden beoordeeld.

177. De risicobeheerfunctie waarborgt dat alle geïdentificeerde risico's doeltreffend worden gemonitord door de bedrijfseenheden.

178. De risicobeheerfunctie ziet regelmatig toe op het werkelijke risicoprofiel van de instelling en toetst dit 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.

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

180. De risicobeheerfunctie beoordeelt mogelijke manieren om risico's te beperken. De rapportages aan het leidinggevend orgaan bevatten voorstellen voor passende risicobeperkende maatregelen.

20.4 De rol van de risicobeheerfunctie bij niet-goedgekeurde blootstellingen

181. De risicobeheerfunctie beoordeelt op onafhankelijke wijze overschrijdingen van risicobereidheid of risicolimieten (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 informeert de betrokken bedrijfseenheden en het leidinggevend orgaan, en beveelt mogelijke oplossingen aan. Wanneer de inbreuk significant is, rapporteert de risicobeheerfunctie rechtstreeks aan het leidinggevend orgaan in zijn toezichtfunctie, onverminderd de verplichting van de risicobeheerfunctie om aan andere interne functies en comités te rapporteren.

182. De risicobeheerfunctie speelt een belangrijke rol 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

183. Het hoofd van de risicobeheerfunctie is verantwoordelijk 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.

184. Het hoofd van de risicobeheerfunctie beschikt over voldoende deskundigheid, onafhankelijkheid en gezag op basis van senioriteit 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, benoemen significante instellingen een onafhankelijk hoofd van de risicobeheerfunctie 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 hij 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).

185. Het hoofd van de risicobeheerfunctie is in staat besluiten aan te vechten die het bestuur en het leidinggevend orgaan van de instelling hebben genomen, en de redenen van bezwaar worden formeel 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, specificeert zij de reikwijdte, de escalatie- en beroepsprocedures van zo'n vetorecht, evenals de wijze waarop het leidinggevend orgaan daarbij zal worden betrokken.

186. Instellingen stellen stringente procedures vast 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 risicobereidheid en -strategie van de instelling.

21 De nalevingsfunctie

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

188. 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 evenredigheidsbeginsel dat wordt uiteengezet in titel I, worden gecombineerd met de functie van hoofd van de risicobeheerfunctie, of kan hij worden uitgevoerd door een ander lid van het hoger personeel, mits er geen belangenconflict tussen de gecombineerde functies bestaat.

189. De nalevingsfunctie, waaronder het hoofd naleving, is onafhankelijk van de bedrijfsonderdelen en interne eenheden die zij controleert, en heeft voldoende gezag, status en middelen. 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.

190. Personeel binnen de nalevingsfunctie beschikt over voldoende kennis, vaardigheden en ervaring wat betreft nalevings- en bijbehorende procedures, en heeft toegang tot regelmatige opleiding.

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

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

193. De nalevingsfunctie zorgt ervoor 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 rapporteert aan het leidinggevend orgaan en communiceert in voorkomend geval met de risicobeheerfunctie over het nalevingsrisico van de instelling en het beheer daarvan. De nalevingsfunctie en de risicobeheerfunctie werken samen en wisselen zo nodig informatie uit om hun respectieve taken te kunnen uitvoeren. Het leidinggevend orgaan en de risicobeheerfunctie houden bij de besluitvorming rekening met de bevindingen van de nalevingsfunctie.

194. In overeenstemming met hoofdstuk 18 van deze richtsnoeren verifieert de nalevingsfunctie, in nauwe samenwerking met de risicobeheerfunctie en de juridische afdeling, ook 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.

195. Instellingen nemen passende maatregelen tegen interne en externe fraude en disciplinaire vergrijpen (bijv. inbreuken op interne procedures of overschrijdingen van limieten).

196. Instellingen zorgen ervoor 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

197. Instellingen stellen een onafhankelijke en doeltreffende interne auditfunctie (IAF) in, rekening houdend met de evenredigheidsbeginselen die in titel I worden uiteengezet, en benoemen een persoon die binnen de gehele instelling verantwoordelijk is voor deze functie. De IAF is onafhankelijk en beschikt over voldoende gezag, status en middelen. De instelling zorgt er in het bijzonder voor 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.

198. De IAF is onafhankelijk van de gecontroleerde activiteiten. De interne-auditfunctie dient daarom niet met andere functies te worden gecombineerd.

199. 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 externe vereisten naleven. Elke entiteit binnen de groep ressorteert onder de IAF.

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

201. De IAF beoordeelt of het kader voor interne controle van de instelling zoals dat is uiteengezet in hoofdstuk 15 zowel effectief als doeltreffend is. De IAF beoordeelt in het bijzonder:

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 risicobereidheid en -strategie van de instelling;

c. de vraag 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.

202. 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 waarderingen ten behoeve van de financieel-administratieve verantwoording en verslaglegging). Voorts controleert de IAF de kwaliteit en het gebruik van de instrumenten voor kwalitatieve risico-identificatie en -beoordeling en de genomen risicobeperkende maatregelen.

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

204. De IAF neemt nationale en internationale beroepsnormen in acht. Een voorbeeld hiervan zijn de normen zoals vastgesteld door het Institute of Internal Auditors.

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

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

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

Titel VI – Beheer van de bedrijfscontinuïteit

208. Instellingen stellen een gedegen bedrijfscontinuïteitsbeheerplan op dat ervoor zorgt dat zij op permanente basis kunnen opereren en dat verliezen door ernstige verstoringen van de bedrijfsactiviteiten worden beperkt.

209. Instellingen kunnen een specifieke onafhankelijke bedrijfscontinuïteitsfunctie instellen, bijv. als onderdeel van de risicobeheerfunctie[26].

210. De bedrijfsvoering van een instelling is afhankelijk van verscheidene kritieke hulpmiddelen (bijv. IT-systemen met inbegrip van clouddiensten, communicatiesystemen 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 derde partijen (bijv. door het afsluiten van verzekeringen).

211. Om een gedegen bedrijfscontinuïteitsbeheerplan te kunnen vaststellen dient de instelling zorgvuldig het risico te analyseren van blootstelling aan ernstige bedrijfsonderbrekingen en een beoordeling te maken van de hieruit volgende potentiële effecten (in zowel kwantitatief als kwalitatief opzicht). Daarbij worden interne en/of externe onderzoeken van gegevens en scenario's benut. Deze analyse bestrijkt alle bedrijfs- en interne units, met inbegrip van de risicobeheerfunctie, en houdt rekening 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.

212. Op basis van bovengenoemde analyse stelt een instelling de volgende plannen op:

    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.

213. Noodplannen, bedrijfscontinuïteitsplannen en herstelplannen worden gedocumenteerd en nauwgezet ten uitvoer gelegd. De documentatie is beschikbaar in de bedrijfsonderdelen en interne eenheden en bij de risicobeheerfunctie. Voorts wordt de documentatie opgeslagen in

[26] Zie ook artikel 312 van Verordening (EU) nr. 575/2013 (“de CRR-verordening”),

fysiek van elkaar gescheiden systemen en in noodgevallen gemakkelijk toegankelijk te zijn. Er wordt gezorgd voor gepaste opleiding. Plannen worden regelmatig getest en bijgewerkt. Tekortkomingen of fouten in de testen worden gedocumenteerd en geanalyseerd, waarna de plannen worden herzien.

Titel VII – Transparantie

214. Strategieën, beleid en procedures worden aan al het relevante personeel in een instelling 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.

215. 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.

216. 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[27].

217. Deze publicatie bevat in ieder geval:

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;

[27] Richtlijn 2013/34/EU van het Europees Parlement en de Raad van donderdag 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).

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 instellingen en op het leidinggevend orgaan;

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

i. een overzicht van het kader voor bedrijfscontinuïteitsbeheer.

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

In overeenstemming met titel III houden instellingen rekening 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
   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. Kader voor interne controle
    a) beschrijving van elke functie, met inbegrip van haar organisatie, middelen, status en gezag
    b) beschrijving van het kader voor risicobeheer, met inbegrip van de risicostrategie
7. 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) gratis dienstverlening
    f) bijkantoren
    g) dochterondernemingen, samenwerkingsverbanden, enz.
    h) gebruik van offshore centra
8. 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
9. Status van het beleid inzake interne governance, met datum
    a) ontwikkeling
    b) laatste wijziging
    c) laatste beoordeling
    d) goedkeuring door het leidinggevend orgaan.