EBA/GL/2021/14

22 november 2021

Richtsnoeren

inzake interne governance overeenkomstig Richtlijn (EU) 2019/2034

1. Nalevings- en rapportageverplichtingen

Status van deze richtsnoeren

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

2. De richtsnoeren geven weer wat in de opvatting van EBA passende toezichtpraktijken binnen het Europees Systeem voor financieel toezicht zijn en hoe het recht van de Unie op een specifiek gebied dient te worden toegepast. Bevoegde autoriteiten als bedoeld in artikel 4, lid 2, van Verordening (EU) nr. 1093/2010 voor wie de 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 beleggingsondernemingen zijn gericht.

Rapportageverplichtingen

3. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 moeten bevoegde autoriteiten EBA er vóór 16.05.2022 van in kennis stellen of zij aan deze richtsnoeren voldoen of voornemens zijn deze op te volgen, met opgave van redenen indien zij niet aan de richtsnoeren voldoen of niet voornemens zijn deze op te volgen. Bevoegde autoriteiten die bij het verstrijken van de termijn niet hebben gereageerd, worden geacht niet te hebben voldaan aan de richtsnoeren. Deze kennisgevingen worden ingediend door het formulier op de EBA-website te versturen naar compliance@eba.europa.eu onder vermelding van “EBA/GL/2021/14”. Kennisgevingen worden ingediend door personen die bevoegd zijn om namens hun bevoegde autoriteit te melden of deze aan de richtsnoeren voldoet. Elke verandering in de status van de naleving moet eveneens aan EBA worden gemeld.

4. Kennisgevingen worden overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 op de website van EBA bekendgemaakt.

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

2. Onderwerp, toepassingsgebied en definities

Onderwerp

5. Deze richtsnoeren beschrijven, overeenkomstig artikel 26, lid 4, van Richtlijn (EU) 2019/2034[2], de interne governanceregelingen, -processen en -mechanismen die beleggingsondernemingen dienen in te voeren overeenkomstig titel IV, hoofdstuk 2, afdeling 2, van die richtlijn om een doeltreffend en prudent bestuur van hun ondernemingen te waarborgen.

6. De richtsnoeren gelden onverminderd het bepaalde in de artikelen 9, 16, 23 en 24 van Richtlijn (EU) 2014/65, in Gedelegeerde Verordening (EU) 2017/565 van de Commissie en in Gedelegeerde Richtlijn (EU) 2017/593 van de Commissie.

Adressaten

7. Deze richtsnoeren zijn gericht tot bevoegde autoriteiten als bedoeld in artikel 4, lid 2, onder viii), van Verordening (EU) 1093/2010 en gedefinieerd in artikel 3, lid 1, punt 5, van Richtlijn (EU) 2019/2034, en tot financiële instellingen als bedoeld in artikel 4, lid 1, van Verordening (EU) 1093/2010 die beleggingsondernemingen zijn als gedefinieerd in artikel 4, lid 1, punt 1, van Richtlijn (EU) 2014/65, die niet vallen onder artikel 2, lid 2, van Richtlijn (EU) 2019/2034 en die niet voldoen aan alle voorwaarden om te worden gekwalificeerd als kleine en niet-verweven beleggingsondernemingen volgens artikel 12, lid 1, van Verordening (EU) 2019/2033.

Toepassingsgebied

8. Deze richtsnoeren gelden voor governanceregelingen van beleggingsondernemingen als vereist volgens Richtlijn (EU) 2019/2034, met inbegrip van hun organisatiestructuur en de bijbehorende verantwoordelijkheidslijnen, alsmede voor procedures voor de identificatie, het beheer, de monitoring en de rapportage van alle risico's[3] waaraan zij blootstaan of bloot kunnen komen te staan, en voor het kader voor interne controle.

[2] Richtlijn (EU) 2019/2034 van het Europees Parlement en de Raad van 27 november 2019 betreffende het prudentiële toezicht op beleggingsondernemingen en tot wijziging van Richtlijnen 2002/87/EG, 2009/65/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU en 2014/65/EU.

[3] Iedere verwijzing naar risico's in deze richtsnoeren omvat alle risico's waaraan beleggingsondernemingen zijn of kunnen zijn blootgesteld, waaronder risico's voor cliënten, voor de markt en voor de beleggingsonderneming zelf, liquiditeitsrisico's, operationele risico's, waaronder juridische en IT-risico's, reputatierisico's, ESG-risico's en risico's op het gebied van witwassen en terrorismefinanciering.

9. Deze richtsnoeren gelden op individuele en geconsolideerde basis binnen het omschreven toepassingsgebied in overeenstemming met artikel 25 van Richtlijn (EU) 2019/2034.

10. De richtsnoeren beogen betrekking te hebben op alle bestaande bestuursmodellen zonder een bepaald model te bepleiten. 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 23 en 24, van Richtlijn (EU) 2019/2034, dient te worden opgevat als een orgaan met leidinggevende (uitvoerende) en toezichthoudende (niet-uitvoerende) functies[4].

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

12. In lidstaten waarin het leidinggevend orgaan de uitvoerende functie 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 op basis van die delegering deze uitvoerende functies vervullen en het beleid van de instelling bepalen, 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 bestuursorgaan of de bestuursorganen van de beleggingsonderneming op grond van het nationale recht.

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

14. 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.

[4] Zie ook overweging 27 van Richtlijn 2019/2034/EU.

Definities

15. Tenzij anders aangegeven, hebben de termen die in Richtlijn (EU) 2019/2034 en Verordening (EU) nr. 2033/2019 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 beleggingsonderneming binnen haar risicodraagkracht en overeenkomstig haar bedrijfsmodel bereid is te nemen om haar strategische doelen te bereiken.
Risicodraagkracht	het maximale risiconiveau dat een beleggingsonderneming 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 houding en het gedrag van een beleggingsonderneming ten aanzien van het 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 hun dagelijkse activiteiten en is van invloed op de risico's die zij aangaan.
Personeel	alle medewerkers van een beleggingsonderneming en haar dochterondernemingen op geconsolideerde basis en alle leden van hun respectieve leidinggevende organen in hun bestuursfunctie en hun toezichtfunctie.
Chief executive officer (CEO)	de persoon die algemeen verantwoordelijk is voor het beheren en aansturen van het geheel aan bedrijfsactiviteiten van een beleggingsonderneming.
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 van interne controlefuncties	de personen op het hoogste hiërarchische niveau die belast zijn met het daadwerkelijke beheer van de dagelijkse activiteiten van de onafhankelijke risicobeheerfunctie, de compliance- en de interne auditfunctie.
Medewerkers met een sleutelfunctie	personen die een aanzienlijke invloed hebben op de leiding over de beleggingsonderneming, 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

	beleggingsondernemingen volgens een risicogebaseerde 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.
EU-moederonderneming	een EU-moederbeleggingsonderneming, EU-moederbeleggingsholding of gemengde financiële EU-moederholding die moet voldoen aan de prudentiële vereisten op basis van de geconsolideerde situatie overeenkomstig artikel 7 van Verordening (EU) 2019/2033.
Prudentiële consolidatie	de toepassing van de prudentiële regels die zijn vastgelegd in artikel 25 van Richtlijn (EU) 2019/2034 en artikel 7 van Verordening (EU) 2019/2033[5].
Beursgenoteerde beleggingsondernemingen	beleggingsondernemingen waarvan de financiële instrumenten in een of meer lidstaten zijn toegelaten tot handel op een gereguleerde markt of op een multilaterale handelsfaciliteit zoals gedefinieerd in artikel 4, punten 21 en 22, van Richtlijn 2014/65/EU[6].
Aandeelhouder	een persoon die aandelen in een beleggingsonderneming bezit, of, afhankelijk van de rechtsvorm van een beleggingsonderneming, andere eigenaren of leden van de beleggingsonderneming.
Bestuursfunctie	een functie als lid van het leidinggevend orgaan van een beleggingsonderneming of een andere rechtspersoon.

3. Uitvoering

Ingangsdatum

16. Deze richtsnoeren gelden vanaf 30 april 2022.

[5] Zie ook de technische reguleringsnormen inzake de consolidatie van beleggingsondernemingen overeenkomstig Richtlijn (EU) 2019/2034.

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

4. Richtsnoeren

Titel I – Evenredigheid

17. Bevoegde autoriteiten en beleggingsondernemingen houden bij de toepassing van deze richtsnoeren rekening met het evenredigheidsbeginsel als omschreven in artikel 26, lid 3, van Richtlijn (EU) 2019/2034 en nader gespecificeerd in titel I van deze richtsnoeren teneinde te waarborgen dat de interne governanceregelingen die zijn ingesteld door beleggingsondernemingen, ook binnen de context van groepen beleggingsondernemingen, passen bij het specifieke risicoprofiel van de onderneming en de groep, evenredig zijn met hun omvang en interne organisatie, relevant voor hun bedrijfsmodel, geschikt voor de aard, omvang en complexiteit van hun activiteiten en voldoende om doeltreffend de doelen van de relevante regelgevingsvereisten en -bepalingen te bereiken.

18. Met betrekking tot het voorgaande punt wordt rekening gehouden met de verscheidenheid aan bedrijfsmodellen volgens welke beleggingsondernemingen en groepen beleggingsondernemingen werken, bijvoorbeeld als beleggingsadviseurs, portefeuillebeheerders, handelsplatforms, bewaarders, uitvoerende of wholesale makelaars en handelsondernemingen. Dienovereenkomstig worden de interne governanceregelingen beschouwd als in overeenstemming met het specifieke risicoprofiel van de onderneming en de groep, evenredig met hun omvang en interne organisatie, relevant voor hun bedrijfsmodel, geschikt voor de aard, omvang en complexiteit van hun activiteiten en voldoende om doeltreffend de doelen van de relevante regelgevingsvereisten en -bepalingen te bereiken, als wordt gewaarborgd dat beleggingsondernemingen met een complexere organisatie of een grotere omvang geavanceerdere governanceregelingen hebben, terwijl beleggingsondernemingen met een eenvoudiger organisatie of met een geringere omvang eenvoudiger governanceregelingen kunnen invoeren. Beleggingsondernemingen dienen er evenwel rekening mee te houden dat de omvang of het systeembelang van een beleggingsonderneming op zichzelf niet per se indicatief is voor de mate waarin die beleggingsonderneming aan risico's blootstaat.

19. Bij de toepassing van het evenredigheidsbeginsel als omschreven in artikel 26, lid 3, van Richtlijn (EU) 2019/2034 en nader gespecificeerd in punt 20 van deze richtsnoeren, waarborgen bevoegde autoriteiten en beleggingsondernemingen dat die toepassing er niet toe leidt dat wordt afgezien van de regelgevingsvereisten voor beleggingsondernemingen of dat ze zodanig worden toegepast dat er geen waarborg is voor solide governanceregelingen, een heldere organisatiestructuur, adequate interne controlemechanismen, een degelijk en doeltreffend risicobeheer en een passend beloningsbeleid.

20. Ten behoeve van de toepassing van het evenredigheidsbeginsel en om een passende uitvoering van de regelgevingsvereisten en deze richtsnoeren te waarborgen, houden beleggingsondernemingen en bevoegde autoriteiten rekening met de onderstaande aspecten:

a. de omvang in termen van de balans van de beleggingsonderneming en haar dochterondernemingen die onder de prudentiële consolidatie vallen;

b. of de waarde van activa van de beleggingsonderneming binnen en buiten de balanstelling gemiddeld 100 miljoen EUR of minder bedraagt over de periode van vier jaar die onmiddellijk voorafgaat aan het betrokken boekjaar, overeenkomstig de criteria in artikel 32, lid 4, onder a), van Richtlijn (EU) 2019/2034;

c. de activa in beheer;

d. of de beleggingsonderneming over een vergunning beschikt om geld of activa van cliënten te houden;

e. de bewaarde en beheerde activa;

f. het volume aan verwerkte orders;

g. de omvang van de dagelijkse handelsstromen;

h. de geografische aanwezigheid van de beleggingsonderneming en de omvang van haar activiteiten in elk rechtsgebied, met inbegrip van activiteiten in derde landen;

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

j. of het een beursgenoteerde beleggingsonderneming is;

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

l. het soort activiteiten waarvoor de beleggingsonderneming een vergunning heeft, de diensten die zij verricht (bijv. bijlage I, delen A en B bij Richtlijn 2014/65/EU) en andere diensten (bijv. clearingdiensten) die de beleggingsonderneming verricht;

m. het onderliggende bedrijfsmodel en de onderliggende bedrijfsstrategie; de aard en complexiteit van de bedrijfsactiviteiten, en de organisatiestructuur van de beleggingsonderneming;

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

o. de eigendoms- en financieringsstructuur van de beleggingsonderneming;

p. het type cliënt;

q. de complexiteit van de financiële instrumenten of contracten;

r. de uitbestede functies en distributiekanalen; en

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

21. Beleggingsondernemingen die rechtspersonen zijn die worden bestuurd door één enkele natuurlijke persoon, beschikken over alternatieve regelingen die een degelijk en prudent bestuur van die beleggingsondernemingen waarborgen en ervoor zorgen dat naar behoren rekening wordt gehouden met interne governanceregelingen.

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

1 Rol en verantwoordelijkheden van het leidinggevend orgaan

22. Het leidinggevend orgaan draagt de uiteindelijke en algemene verantwoordelijkheid voor de beleggingsonderneming; het bepaalt, houdt toezicht op en legt verantwoording af voor de uitvoering binnen de beleggingsonderneming van de governanceregelingen, zoals met name genoemd in de artikelen 26, 28 en 29 van Richtlijn (EU) 2019/2034, die een doeltreffend en prudent beheer van de beleggingsonderneming waarborgen.

23. De taken van het leidinggevend orgaan zijn duidelijk omschreven, waarbij 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 naar behoren goedgekeurd door het leidinggevend orgaan. 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, wanneer van toepassing.

24. Er is een doeltreffende interactie 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. Om over passende controlemechanismen te beschikken, wordt de besluitvorming binnen het leidinggevend orgaan niet gedomineerd door één lid of een kleine groep leden.

25. Onverminderd de taken en verantwoordelijkheden die Richtlijn (EU) 2014/65 toewijst aan het leidinggevend orgaan, behoren de vaststelling en goedkeuring van en het toezicht op de uitvoering van de volgende aspecten tot de verantwoordelijkheden van het leidinggevend orgaan:

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

b. de algemene risicostrategie, met inbegrip van de risicobereidheid van de beleggingsonderneming en haar risicobeheerkader, met adequaat beleid en adequate procedures, rekening houdend met de macro-economische omgeving en de bedrijfscyclus van de beleggingsonderneming en maatregelen om te waarborgen dat het leidinggevend orgaan voldoende tijd besteedt aan risicobeheerkwesties; een toereikend en doeltreffend kader voor interne governance en interne controle dat een duidelijke organisatiestructuur en goed functionerende interne controlemechanismen omvat. Dergelijke mechanismen dienen een permanente en doeltreffende compliancefunctie te omvatten en, waar passend en evenredig overeenkomstig titel I, interne risicobeheer- en auditfuncties die voldoende gezag, status en middelen hebben om hun functies onafhankelijk te verrichten en naleving van toepasselijke regelgevingsvereisten te waarborgen in de context van het voorkomen van het witwassen van geld en terrorismefinanciering; ook dienen ze doelen te omvatten voor het liquiditeitsbeheer van de beleggingsonderneming;

c. een beloningsbeleid dat in overeenstemming is met de beginselen die worden uiteengezet in de artikelen 26 en 30 tot en met 33 van Richtlijn (EU) 2019/2034 en de EBA-richtsnoeren betreffende een goed beloningsbeleid krachtens Richtlijn (EU) 2019/2034[7];

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

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

f. 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;

[7] EBA Richtsnoeren betreffende een goed beloningsbeleid overeenkomstig Richtlijn (EU) 2019/2034.

[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.

[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.

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

g. een risicocultuur overeenkomstig hoofdstuk 8 van deze richtsnoeren, waarin aandacht wordt geschonken aan het risicobewustzijn en het risicogedrag van de beleggingsonderneming;

h. een bedrijfscultuur en waarden overeenkomstig hoofdstuk 9 die verantwoordelijk en ethisch gedrag bevorderen, met inbegrip van een gedragscode of soortgelijk instrument;

i. een beleid inzake belangenconflicten op het niveau van de beleggingsonderneming overeenkomstig hoofdstuk 10, en voor personeel overeenkomstig hoofdstuk 11; en

j. 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.

26. Het leidinggevend orgaan streeft er bij het opzetten en goedkeuren van en het houden van toezicht op de uitvoering van de in punt 25 genoemde aspecten, naar een bedrijfsmodel en governanceregelingen – met inbegrip van een kader voor risicobeheer – te waarborgen die rekening houden met de risico's waaraan beleggingsondernemingen blootstaan of kunnen worden blootgesteld of de risico's die zij voor anderen inhouden of kunnen inhouden[10]. Bij het inventariseren van alle risico's waaraan zij zijn blootgesteld, nemen beleggingsondernemingen alle relevante risicofactoren in aanmerking, met inbegrip van milieutechnische, maatschappelijke en governancegerelateerde risicofactoren (ESG). Beleggingsondernemingen nemen in aanmerking dat laatstgenoemde hun prudentiële risico's kunnen doen toenemen[11]. Voorbeelden van dergelijke risico's zijn juridische (verbintenisrechtelijke of arbeidsrechtelijke) risico's, risico's in verband met mogelijke mensenrechtenschendingen of andere ESG-risicofactoren die van invloed kunnen zijn op het land waar een dienstverlener is gevestigd en op het vermogen van die dienstverlener om het overeengekomen niveau van de dienstverlening te waarborgen.

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

28. Alle leden van het leidinggevend orgaan behoren op de hoogte te zijn van de algemene bedrijfsactiviteiten, de financiële situatie en de risicosituatie van de beleggingsonderneming, waarbij rekening wordt gehouden met het economische klimaat, en van besluiten die zijn

[10] Zie artikel 26 van Richtlijn (EU) 2019/2034.

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

genomen die een belangrijke impact hebben op de activiteiten van de beleggingsonderneming.

29. Een lid van het leidinggevend orgaan kan verantwoordelijk zijn voor een interne controlefunctie zoals vermeld in titel V, paragraaf 18.1, mits het lid geen andere mandaten heeft die de interne controleactiviteiten van het lid en de onafhankelijkheid van de interne controlefunctie in het geding zouden brengen.

30. Het leidinggevend orgaan dient eventuele geïdentificeerde zwakke punten in de uitvoering van processen, strategieën en beleid met betrekking tot de in de punten 25 en 26 genoemde verantwoordelijkheden te monitoren, periodiek te evalueren en aan te pakken. Het kader voor interne governance en de uitvoering daarvan dienen periodiek te worden getoetst en geactualiseerd, rekening houdend met het evenredigheidsbeginsel, zoals verder toegelicht in titel I. Wanneer een beleggingsonderneming te maken krijgt met belangrijke veranderingen, dient een grondigere toetsing te worden uitgevoerd.

31. Wanneer beleggingsondernemingen rechtspersonen zijn die worden bestuurd door één enkele natuurlijke persoon, overeenkomstig hun statuten en nationale wetgeving, dienen de verwijzingen in deze richtsnoeren naar een leidinggevend orgaan te worden opgevat als van toepassing op de ene persoon die verantwoordelijk is voor de invoering van alternatieve regelingen om een degelijk en prudent bestuur van die beleggingsonderneming te waarborgen en ervoor te zorgen dat naar behoren rekening wordt gehouden met interne governanceregelingen.

2 De bestuursfunctie van het leidinggevend orgaan

32. Het leidinggevend orgaan in zijn bestuursfunctie is actief betrokken bij de activiteiten van een beleggingsonderneming en neemt besluiten op grond van een goede kennis van zaken.

33. Het leidinggevend orgaan in zijn bestuursfunctie is verantwoordelijk voor de uitvoering van de strategieën die het leidinggevend orgaan heeft vastgesteld en dient de uitvoering en passendheid van die strategieën regelmatig te bespreken met het leidinggevend orgaan in zijn toezichtfunctie. De operationele uitvoering kan door de directie van de beleggingsonderneming worden verricht.

34. 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 regelmatig en 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 beleggingsonderneming, bijv. belangrijke besluiten inzake bedrijfsactiviteiten en genomen risico's, de beoordeling van het economische en

bedrijfsklimaat van de beleggingsonderneming, haar liquiditeit en solide kapitaalbasis, en de beoordeling van haar belangrijke risicoblootstellingen.

35. Onverminderd de omzetting van Richtlijn 2015/849/EU (de antiwitwasrichtlijn) in nationaal recht, wijst het leidinggevend orgaan overeenkomstig de vereisten van artikel 46, lid 4, van Richtlijn 2015/849/EU een van zijn leden aan als verantwoordelijke persoon voor de uitvoering van de wettelijke en bestuursrechtelijke bepalingen die nodig zijn voor de naleving van deze richtlijn, met inbegrip van de overeenkomstige AML/CTF-beleidsvoorschriften en -procedures binnen de instelling en op het niveau van het leidinggevend orgaan.

3 Toezichthoudende functie van het leidinggevend orgaan

36. 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 beleggingsonderneming.

37. Onverminderd het nationale recht bevat het leidinggevend orgaan in zijn toezichtfunctie onafhankelijke leden 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.

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

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

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. naar behoren de taken en rol te vervullen van het risicocomité en de beloningscommissie wanneer deze niet zijn ingesteld;

d. de doeltreffendheid van het kader voor interne governance van de beleggingsonderneming 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 beleggingsonderneming, 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 beleggingsonderneming consistent ten uitvoer wordt gelegd;

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

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

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 beleggingsonderneming hebben of kunnen hebben; en

j. toe te zien op de uitvoering van het interne-auditplan, nadat eerst het risicocomité, indien ingesteld, daarbij is betrokken.

4 De rol van de voorzitter van het leidinggevend orgaan

39. 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 ingesteld, en is verantwoordelijk voor het algehele doeltreffende functioneren.

40. 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 besproken.

41. Wanneer het de voorzitter is toegestaan uitvoerende taken op zich te nemen, treft de beleggingsonderneming maatregelen om een eventueel nadelig effect op de controlemechanismen van de beleggingsonderneming te beperken (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). De voorzitter van het leidinggevend orgaan in zijn toezichtfunctie bij een beleggingsonderneming bekleedt niet tegelijkertijd de functie van CEO binnen dezelfde beleggingsonderneming, tenzij dat door de instelling is beargumenteerd en door de bevoegde autoriteiten is toegestaan.

42. 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 goede kennis van zaken en dat documenten en informatie ruim vóór de vergadering worden ontvangen.

43. 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

44. Overeenkomstig artikel 28 van Richtlijn (EU) 2019/2034 en tenzij anders gespecificeerd door nationale wetgeving[12], moeten beleggingsondernemingen met een waarde van hun activa binnen en buiten de balanstelling van gemiddeld meer dan 100 miljoen EUR over de vier jaar onmiddellijk voorafgaand aan het betrokken boekjaar, een risicocomité en een beloningscommissie instellen om het leidinggevend orgaan in zijn toezichtfunctie te adviseren en de door dit orgaan te nemen besluiten voor te bereiden.

45. Wanneer geen risicocomité wordt ingesteld, dienen de verwijzingen naar dit comité in deze richtsnoeren te worden begrepen als verwijzingen naar het leidinggevend orgaan in zijn toezichtfunctie.

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

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

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

[12] Artikel 28 van Richtlijn (EU) 2019/2034 eist dat beleggingsondernemingen die niet voldoen aan de criteria van artikel 32, lid 4, onder a), een risicocomité instellen, bestaande uit leden van het leidinggevende orgaan die in de betrokken beleggingsonderneming geen enkele uitvoerende functie uitoefenen.

5.2 Samenstelling van comités[13]

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

50. Onafhankelijke leden [14] van het leidinggevend orgaan in zijn toezichtfunctie zijn actief betrokken bij comités.

51. Wanneer overeenkomstig Richtlijn (EU) 2019/2034 of nationale wetgeving comités moeten worden ingesteld, geldt als algemeen beginsel dat deze ten minste drie leden hebben en ten minste één onafhankelijk lid, rekening houdend met de criteria van titel I van deze richtsnoeren en de gemeenschappelijke richtsnoeren van ESMA en EBA voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie. Wanneer er binnen het leidinggevend orgaan in zijn toezichtfunctie niet voldoende leden zijn om een goede samenstelling van comités als uiteengezet in dit hoofdstuk, te waarborgen, kunnen de taken van het comité worden gedelegeerd aan één lid van het leidinggevend orgaan in zijn toezichtfunctie, die naar behoren wordt ondersteund door medewerkers. Comités kunnen bestaan uit dezelfde groep leden, rekening houdend met de criteria van titel I en het aantal onafhankelijke leden van het leidinggevend orgaan in zijn toezichtfunctie, evenals de specifieke ervaring, kennis en vaardigheden waarover de comités collectief en de afzonderlijke leden daarvan dienen te beschikken. De beargumentering van de samenstelling van comités wordt gedocumenteerd.

52. Het risicocomité bestaat uit niet-uitvoerende leden van het leidinggevend orgaan in zijn toezichtfunctie van de betrokken beleggingsonderneming. De beloningscommissie wordt samengesteld zoals beschreven in paragraaf 2.3 van de EBA-richtsnoeren inzake degelijk beloningsbeleid[15].

53. Het risicocomité wordt waar mogelijk voorgezeten door een onafhankelijk lid. Leden van het risicocomité beschikken, zowel individueel als gezamenlijk, over voldoende kennis, vaardigheden en deskundigheid op het gebied van respectievelijk het selectieproces en geschiktheidsvereisten, en risicobeheer- en -controlepraktijken. De voorzitter van het risicocomité in een beleggingsonderneming is, waar mogelijk, niet tevens de voorzitter van het leidinggevend orgaan of de voorzitter van enig ander comité.

5.3 Processen van comités

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

[13] 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.

[14] 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.

[15] EBA-richtsnoeren inzake degelijk beloningsbeleid overeenkomstig artikel 34, lid 3, van Richtlijn (EU) 2019/2034.

55. Er is een passende wisselwerking tussen comités. Met inachtneming van punt 51 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.

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

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

58. Het risicocomité dient ten minste:

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

    b. regelmatig rapporten, ad-hocinformatie, mededelingen en adviezen van hoofden van interne controlefuncties te ontvangen met betrekking tot het actuele risicoprofiel van de beleggingsonderneming, haar risicocultuur en haar risicolimieten, evenals aangaande eventuele belangrijke inbreuken[16] die mogelijk hebben plaatsgevonden, met gedetailleerde informatie over en aanbevelingen voor corrigerende maatregelen die zijn genomen, moeten worden genomen of worden voorgesteld; de inhoud, het format en de frequentie van de risico-informatie die aan hen wordt gerapporteerd, te onderwerpen aan periodieke evaluatie en besluitvorming; en

    c. waar nodig te 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

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

    a. het leidinggevend orgaan in zijn toezichtfunctie te adviseren en ondersteunen voor wat betreft de algemene feitelijke en toekomstige risicostrategie en risicobereidheid van de beleggingsonderneming, en het leidinggevend orgaan bij te staan bij het toezicht op de uitvoering van die strategie, teneinde ervoor te zorgen dat deze in lijn

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

zijn met de zakelijke doelstellingen en de bedrijfscultuur en -waarden van de beleggingsonderneming;

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

c. toe te zien op de uitvoering van de strategieën voor kapitaal- en liquiditeitsbeheer evenals voor alle andere relevante risico's van een beleggingsonderneming, zoals risico's voor cliënten, de markt en ondernemingen, operationele (waaronder juridische en IT-risico's) en reputatierisico's, om de toereikendheid hiervan 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 beleggingsonderneming, marktontwikkelingen of aanbevelingen die worden gedaan door de risicobeheerfunctie;

e. te adviseren over 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 beleggingsonderneming zou reageren op externe en interne gebeurtenissen;

g. toe te zien op de afstemming tussen alle belangrijke aan cliënten aangeboden financiële instrumenten en diensten, en het bedrijfsmodel en de risicostrategie van de beleggingsonderneming. Indien een risicocomité is ingesteld, dient dit de risico's die samenhangen met de aangeboden financiële instrumenten en diensten te beoordelen en rekening te houden met de afstemming van de prijzen die aan de producten en diensten worden toegekend en de winst die hiermee wordt behaald; en

h. de aanbevelingen van interne of externe auditors te beoordelen en de passende uitvoering van genomen maatregelen op te volgen.

60. Het risicocomité werkt samen met andere comités waarvan de activiteiten gevolgen kunnen hebben voor de risicostrategie (bijv. de beloningscommissie indien ingesteld) en communiceert op regelmatige basis met de interne controlefuncties van de beleggingsonderneming, met name de risicobeheerfunctie.

Titel III – Kader voor governance

6 Organisatiekader en -structuur

6.1 Organisatiekader

61. Het leidinggevend orgaan van een beleggingsonderneming zorgt voor een passende en transparante organisatie- en operationele structuur voor die beleggingsonderneming en heeft daarvan een schriftelijke beschrijving. Deze structuur getuigt van en is bevorderend voor een doeltreffend en prudent beheer van de beleggingsonderneming op individueel en geconsolideerd niveau.

62. Het leidinggevend orgaan zorgt ervoor dat de interne controlefuncties over passende financiële en personele middelen beschikken en de bevoegdheden hebben die nodig zijn om hun rol doeltreffend te vervullen. Voor de compliancefunctie geldt als minimale eis dat deze onafhankelijk optreedt en dat er een passende scheiding van taken is. De rapportagelijnen en de toewijzing van verantwoordelijkheden binnen een beleggingsonderneming, met name die tussen medewerkers met een sleutelfunctie, zijn helder, welomschreven, samenhangend, afdwingbaar en adequaat gedocumenteerd. De documentatie wordt wanneer nodig bijgewerkt.

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

64. 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 beleggingsonderneming beïnvloeden. Wanneer zwakke punten worden vastgesteld, voert het leidinggevend orgaan eventueel noodzakelijke aanpassingen snel door.

6.2 Ken uw structuur

65. Het leidinggevend orgaan kent en begrijpt de juridische, organisatie- en operationele structuur van de beleggingsonderneming ten volle ("ken uw structuur") en zorgt ervoor dat die structuur aansluit op de goedgekeurde bedrijfs- en risicostrategie en risicobereidheid, en door haar kader voor risicobeheer wordt gedekt.

66. Het leidinggevend orgaan is verantwoordelijk voor de goedkeuring van deugdelijke strategieën en beleid voor de vaststelling van nieuwe structuren. Wanneer een beleggingsonderneming 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 beleggingsonderneming en, in voorkomend geval, de structuren binnen een groep, rekening houdend met de criteria die zijn vastgelegd in hoofdstuk 7, duidelijk, doeltreffend en transparant zijn voor het personeel, de aandeelhouders en andere belanghebbenden van de beleggingsonderneming en voor de bevoegde autoriteit.

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

68. Het leidinggevend orgaan van een EU-moederonderneming kent niet alleen de juridische, organisatie- en operationele structuur van de groep, 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 moederbeleggingsonderneming 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 beleggingsondernemingen binnen de groep voldoen aan alle rapportagevereisten van de toezichthouder op een individuele en geconsolideerde basis.

69. Het leidinggevend orgaan van een EU-moederonderneming zorgt ervoor dat de verschillende entiteiten van de groep (met inbegrip van de EU-moederonderneming zelf) voldoende informatie ontvangen, zodat zij een duidelijk beeld hebben van de algemene doelstellingen, de strategieën en het risicoprofiel van de groep, en van de manier waarop de betrokken groepsentiteit is ingebed in de structuur en operationele werking van de groep. Dergelijke informatie en herzieningen daarvan dienen te worden gedocumenteerd en beschikbaar te worden gesteld aan de betrokken relevante functies, waaronder het leidinggevend orgaan, bedrijfsonderdelen en interne controlefuncties. De leden van het leidinggevend orgaan van een EU-moederonderneming 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 ontvangen met een beoordeling van de algemene structuur van de beleggingsonderneming en van de verenigbaarheid van activiteiten van de afzonderlijke entiteiten met de goedgekeurde groepsbrede strategie; en

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

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

70. Beleggingsondernemingen vermijden het opzetten van complexe en potentieel niet-transparante structuren. Beleggingsondernemingen 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, het financieren van terrorisme of andere financiële misdrijven, en met de respectieve controles en het toepasselijke rechtskader[17]. Daartoe houden beleggingsondernemingen ten minste rekening met:

a. de mate waarin het rechtsgebied waarin de structuur wordt opgezet daadwerkelijk voldoet aan EU- en internationale normen inzake belastingtransparantie en de bestrijding van het witwassen van geld en de financiering van terrorisme[18];

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

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

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

e. of de structuur passend toezicht door het leidinggevend orgaan van de beleggingsonderneming of het vermogen van de beleggingsonderneming 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.

71. In ieder geval zetten beleggingsondernemingen geen ondoorzichtige of nodeloos complexe structuren op die geen duidelijke economische reden of juridisch doel hebben, en evenmin

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

[18] Zie ook Gedelegeerde Verordening (EU) 2019/758 van de Commissie van 31 januari 2019 tot aanvulling van Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen inzake de minimumactie en de soort bijkomende maatregelen waartoe krediet- en financiële instellingen verplicht zijn met het oog op het beperken van het witwasrisico en het risico van terrorismefinanciering in bepaalde derde landen: https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/rts-on-the-implementation-of-group-wide-aml/cft-policies-in-third-countries

structuren die aanleiding zouden kunnen vormen tot zorg dat ze mogelijk worden opgezet voor een doel dat verband houdt met financiële misdrijven.

72. Wanneer dergelijke structuren worden opgezet, zorgt het leidinggevend orgaan ervoor 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 worden alleen goedgekeurd en gehandhaafd als hun doel duidelijk vastgesteld en begrepen is, en als het leidinggevend orgaan er zeker van is dat alle belangrijke risico's, met inbegrip van reputatierisico's, zijn vastgesteld, dat alle risico's doeltreffend kunnen worden beheerd en op passende wijze gerapporteerd, en dat doeltreffend toezicht is gewaarborgd. Hoe complexer en ondoorzichtiger de organisatie- en operationele structuur en hoe groter de risico's, des te intensiever het toezicht erop dient te zijn.

73. Beleggingsondernemingen documenteren hun besluiten en zijn in staat om hun besluiten te rechtvaardigen tegenover bevoegde autoriteiten.

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

    a. de beleggingsonderneming adequaat beleid, adequate procedures en gedocumenteerde processen (bijv. toepasselijke limieten en informatiestromen) heeft ingevoerd voor het overwegen, naleven en goedkeuren, en voor het 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 EU-moederonderneming 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 beleggingsonderneming op gezette tijden beoordeelt of het nog steeds noodzakelijk is om dergelijke structuren te handhaven.

75. Deze structuren en activiteiten, met inbegrip van de vraag of deze in overeenstemming zijn met wetgeving en professionele normen, wordt regelmatig getoetst. Wanneer een interne auditfunctie is ingesteld, voert deze de toetsing uit volgens een risicogebaseerde aanpak.

76. Beleggingsondernemingen nemen doeltreffende risicobeheermaatregelen wanneer zij activiteiten uitvoeren voor cliënten die niet standaard of niet transparant zijn (bijv. cliënten helpen met het opzetten van vehikels in offshore rechtsgebieden, het optuigen van complexe structuren, het financieren van transacties voor hen, of de verlening van trusteediensten) en die soortgelijke uitdagingen voor de interne governance inhouden en aanzienlijke operationele en reputatierisico's met zich meebrengen. Beleggingsondernemingen analyseren met name waarom een cliënt een bepaalde structuur wil opzetten.

7 Organisatiekader in de context van een groep

77. Overeenkomstig artikel 25 van Richtlijn (EU) 2019/2034 en artikel 7 van Verordening (EU) 2019/2033, en tenzij artikel 8 van Verordening (EU) 2019/2033 door bevoegde autoriteiten wordt toegepast, zorgen EU-moederondernemingen en hun dochterondernemingen die onder Richtlijn (EU) 2019/2034 vallen, ervoor dat governanceregelingen, -processen en -mechanismen consistent zijn en goed zijn geïntegreerd op geconsolideerde basis. Met het oog hierop passen moederondernemingen en dochterondernemingen die onder de prudentiële consolidatie vallen, dergelijke regelingen, processen en mechanismen in hun niet onder Richtlijn (EU) 2019/2034 vallende dochterondernemingen toe, met inbegrip van dochterondernemingen die in derde landen, waaronder in offshore financiële centra, zijn opgericht, om te zorgen voor solide governanceregelingen op een geconsolideerde basis. Bevoegde functies binnen de EU-moederonderneming en haar dochterondernemingen onderhouden onderling contact en wisselen waar nuttig informatie uit. De regelingen, processen en mechanismen voor governance waarborgen dat de EU-moederonderneming voldoende gegevens en informatie tot haar beschikking heeft en in staat is het groepsbrede risicoprofiel te beoordelen, zoals omschreven in paragraaf 6.2.

78. Het leidinggevend orgaan van een dochteronderneming die onder Richtlijn (EU) 2019/2034 valt, keurt het groepsbrede governancebeleid dat op geconsolideerd niveau is vastgesteld, goed en voert dit uit op individueel niveau, op een wijze die voldoet aan alle specifieke vereisten van EU- en nationale wetgeving.

79. Op geconsolideerd niveau zorgt de EU-moederonderneming ervoor dat het in titel V genoemde groepsbrede governancebeleid en interne controlekader worden nageleefd door alle beleggingsondernemingen en andere entiteiten die onder de prudentiële consolidatie vallen, met inbegrip van dochterondernemingen die zelf niet onder Richtlijn (EU) 2019/2034 vallen. Bij de uitvoering van governancebeleid zorgt de EU-moederonderneming 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.

80. Een EU-moederonderneming houdt rekening met de belangen van al haar dochterondernemingen. Ook denkt zij na over hoe strategieën en beleid op de lange termijn bijdragen aan het belang van elke dochteronderneming en van de groep als geheel.

81. EU-moederondernemingen en hun dochterondernemingen zorgen ervoor dat de beleggingsondernemingen en entiteiten binnen de groep voldoen aan alle specifieke regelgevingsvereisten in elk relevant rechtsgebied.

82. De EU-moederonderneming 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 25 tot en met 32 van Richtlijn (EU) 2019/2034 en aan deze richtsnoeren, zolang dit niet in strijd is met de wetten van het derde land.

83. De governancevereisten van Richtlijn (EU) 2019/2034 en de bepalingen van deze richtsnoeren gelden voor in de EU gevestigde beleggingsondernemingen, 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 EU-moederonderneming is, omvat de prudentiële consolidatie binnen de EU niet het niveau van de in een derde land gevestigde moederonderneming en andere rechtstreekse dochterondernemingen van die moederonderneming. De EU-moederonderneming 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 (EU) 2019/2034 en de nadere specificaties in deze richtsnoeren.

84. Bij het vaststellen van beleid en het documenteren van governanceregelingen houden beleggingsondernemingen rekening met de in bijlage I genoemde aspecten. Hoewel beleid en documentatie in aparte documenten kunnen worden vastgelegd, dienen beleggingsondernemingen te overwegen deze te combineren of ernaar te verwijzen in één enkel kaderdocument voor governance.

Titel IV – Risicocultuur en gedragsregels

8 Risicocultuur

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

86. Beleggingsondernemingen ontwikkelen een geïntegreerde en organisatiebrede risicocultuur die berust op een volledig inzicht in en een holistisch perspectief op de risico's die zij lopen, waaronder risico's voor cliënten, voor de markt en voor de beleggingsonderneming zelf, alsmede liquiditeitsrisico's, met name de risico's die een wezenlijke impact kunnen hebben op het beschikbare eigen vermogen of dat vermogen aanzienlijk kunnen uitputten, alsmede de wijze waarop deze worden beheerd, rekening houdend met de risicodraagkracht en de risicobereidheid van de beleggingsonderneming.

87. Beleggingsondernemingen ontwikkelen een risicocultuur door middel van beleid, communicatie en opleiding van personeel inzake de activiteiten, de strategie en het risicoprofiel van de beleggingsonderneming, en stemmen hun communicatie en personeelsopleiding af op de verantwoordelijkheden van het personeel als het gaat om het nemen en beheren van risico's.

88. Personeelsleden 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 beleggingsonderneming, rekening houdend met de risicobereidheid en -draagkracht van de beleggingsonderneming berust in hoofdzaak bij de bedrijfseenheden, waarbij het leidinggevend orgaan toezicht uitoefent.

89. 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 beleggingsonderneming. De leden dienen deze waarden in hun gedrag tot uiting te brengen. Het bestuur van beleggingsondernemingen, waaronder de medewerkers met een sleutelfunctie, dient bij te dragen aan de interne communicatie van kernwaarden en verwachtingen naar het personeel. Personeelsleden dienen in overeenstemming met alle toepasselijke wet- en regelgeving te handelen en direct melding te doen van waargenomen niet-naleving binnen of buiten de beleggingsonderneming (bijv. aan de bevoegde autoriteit middels een klokkenluidersprocedure). Het leidinggevend orgaan dient voortdurend de risicocultuur van de beleggingsonderneming te bevorderen, monitoren en beoordelen; rekening te houden met het effect van de risicocultuur op de financiële stabiliteit, het risicoprofiel en de solide governance van de beleggingsonderneming; en waar nodig wijzigingen door te voeren.

b. Verantwoording: relevante personeelsleden op alle niveaus kennen en begrijpen de kernwaarden van de beleggingsonderneming en, voor zover noodzakelijk voor hun functie, haar risicobereidheid en risicodraagkracht. Zij zijn in staat om 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 beleggingsonderneming.

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, biedt de gelegenheid bestaande praktijken te toetsen, wakkert een constructieve kritische houding onder het personeel aan en bevordert een open en constructieve betrokkenheid in de hele organisatie.

d. Stimulansen: passende stimulansen spelen een essentiële rol in het afstemmen van risicogedrag op het risicoprofiel van de beleggingsonderneming en haar langetermijnbelangen[19].

[19] Zie ook de EBA-richtsnoeren betreffende een degelijk beloningsbeleid overeenkomstig Richtlijn (EU) 2034/2019.

9 Ondernemingswaarden en gedragscode

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

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

92. Het beleid van beleggingsondernemingen is genderneutraal. Dit betreft, maar is niet beperkt tot, het beleid ten aanzien van beloning, werving, loopbaanontwikkeling en opvolging, toegang tot opleiding en mogelijkheden om te solliciteren naar interne vacatures. Instellingen waarborgen gelijke kansen [20] voor alle personeelsleden ongeacht hun geslacht, ook ten aanzien van loopbaanperspectieven, en streven naar verbetering van de vertegenwoordiging van het geslacht dat ondervertegenwoordigd is in het leidinggevend orgaan en in de groep personeelsleden met leidinggevende verantwoordelijkheden zoals gedefinieerd in de Gedelegeerde Verordening van de Commissie (technische reguleringsnormen inzake geïdentificeerde personeelsleden). Beleggingsondernemingen monitoren de ontwikkelingen in de loonkloof tussen mannen en vrouwen. Wanneer beleggingsondernemingen vijftig personeelsleden of meer hebben [21] , monitoren zij deze ontwikkelingen apart voor geïdentificeerde personeelsleden (met uitzondering van leden van het leidinggevend orgaan), leden van het leidinggevend orgaan in zijn bestuursfunctie, leden van het leidinggevend orgaan in zijn toezichtfunctie en andere personeelsleden. Beleggingsondernemingen hebben een beleid gericht op herintegratie van hun personeelsleden na moederschaps-, vaderschaps- of ouderschapsverlof[22].

93. De ten uitvoer gelegde normen richten zich op het versterken van de solide governanceregelingen van de beleggingsonderneming en op het terugdringen van de risico's waaraan de beleggingsonderneming is blootgesteld, met name operationele en reputatierisico's, die een aanzienlijke ongunstige impact op de winstgevendheid en duurzaamheid van een beleggingsonderneming kunnen hebben als gevolg van boetes,

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

[21] Zie ook de EBA-richtsnoeren betreffende een degelijk beloningsbeleid overeenkomstig Richtlijn (EU) 2019/2034.

[22] Zie ook de EBA-richtsnoeren betreffende een degelijk beloningsbeleid overeenkomstig Richtlijn (EU) 2019/2034.

proceskosten, door bevoegde autoriteiten opgelegde beperkingen, andere financiële en strafrechtelijke sancties, en het verlies aan merkwaarde en consumentenvertrouwen.

94. Het leidinggevend orgaan voert een helder en gedocumenteerd beleid ten aanzien van de wijze waarop aan deze normen dient te worden voldaan. Dit beleid dient:

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

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

    c. beginselen uiteen te zetten aangaande en voorbeelden te verstrekken van toelaatbaar en ontoelaatbaar gedrag, met name in verband met de opgave van onjuiste financiële gegevens en financieel wangedrag, economische en financiële misdrijven waaronder, maar niet beperkt tot, fraude, witwassen van geld en terrorismefinanciering, anti-trustpraktijken, financiële sancties, omkoping en corruptie, marktmanipulatie, misleidende verkopen en andere schendingen van wetgeving inzake consumentenbescherming, en fiscale misdrijven, hetzij rechtstreeks hetzij onrechtstreeks gepleegd, zoals door middel van onrechtmatige of verboden dividendarbitrageregelingen;

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

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

95. Beleggingsondernemingen controleren de naleving van dergelijke normen en zorgen voor bewustzijn bij personeelsleden, bijv. door het verstrekken van opleiding. Beleggingsondernemingen stellen vast welke functie verantwoordelijk is voor het toezicht op naleving van de gedragscode of een 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.

10 Beleid inzake belangenconflicten op het niveau van de beleggingsonderneming

96. Het leidinggevend orgaan is verantwoordelijk voor de vaststelling en goedkeuring van en het toezicht op de uitvoering 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 beleggingsonderneming, bijv. als gevolg van de verschillende activiteiten en rollen van de beleggingsonderneming, van verschillende beleggingsondernemingen die onder de prudentiële consolidatie vallen of van verschillende bedrijfsonderdelen of -eenheden binnen een beleggingsonderneming, of met betrekking tot externe belanghebbenden. Wanneer beleggingsondernemingen dit beleid vaststellen, zijn zij zich ervan bewust dat dit beleid ook in overeenstemming moet zijn met artikel 16, lid 3, en artikel 23 van Richtlijn 2014/65/EU en de artikelen 33 tot en met 35 van Gedelegeerde Verordening 2017/565 van de Commissie.

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

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

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

11 Beleid inzake belangenconflicten voor personeelsleden[23]

98. Onverminderd artikel 23 van Richtlijn 2014/65/EU en hoofdstuk 2, afdeling 3, van Gedelegeerde Verordening (EU) 2017/565 van de Commissie, is het leidinggevend orgaan verantwoordelijk voor de vaststelling en goedkeuring van en het toezicht op de uitvoering 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 beleggingsonderneming 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 EU-moederonderneming houdt rekening met belangen binnen een groepsbreed beleid inzake belangenconflicten op een geconsolideerde basis.

99. Het beleid is erop gericht belangenconflicten van medewerkers te identificeren, met inbegrip van conflicten met de belangen van hun naaste familieleden. Beleggingsondernemingen

[23] 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 overeenkomstig Richtlijn 2013/36/EU en Richtlijn 2014/65/EU.

dienen er rekening mee te houden dat belangenconflicten niet alleen kunnen ontstaan als gevolg van bestaande persoonlijke of professionele relaties, maar ook van dergelijke relaties uit het verleden. Wanneer belangenconflicten ontstaan, beoordelen beleggingsondernemingen hoe zwaarwegend deze zijn, nemen zij besluiten over beperkende maatregelen, en voeren zij die indien nodig uit.

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

101. 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, lidmaatschap van een orgaan of eigendom van een orgaan of entiteit met conflicterende belangen);

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

    c. persoonlijke of professionele relaties met personeelsleden van de beleggingsondernemingen 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 met belangrijke leveranciers, adviesbedrijven of andere dienstverleners); en

    f. politieke invloed of politieke relaties.

102. Niettemin dienen beleggingsondernemingen er rekening mee te houden dat het feit dat iemand aandeelhouder van een beleggingsonderneming is of gebruikmaakt van andere diensten van een beleggingsonderneming, niet mag leiden tot een situatie waarin personeelsleden worden geacht een belangenconflict te hebben als zij binnen een toepasselijke ‘de minimis’-drempel blijven.

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

104. 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 beleggingsonderneming centraal te staan in de genomen besluiten.

105. 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 personeelsleden die ook buiten de beleggingsonderneming actief zijn, ongepaste invloed verkrijgen binnen de beleggingsonderneming met betrekking tot deze andere activiteiten;

    c. vastleggen dat de leden van het leidinggevend orgaan zich dienen 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; en

    d. voorkomen dat leden van het leidinggevend orgaan bestuursfuncties vervullen bij concurrerende beleggingsondernemingen.

106. Het beleid dient in ieder geval betrekking te hebben op belangenconflicten op het niveau van het leidinggevend orgaan en voldoende leidraden te bieden voor de identificatie en het beheer van belangenconflicten die het vermogen van leden van het leidinggevend orgaan tot het nemen van objectieve en onpartijdige beslissingen die erop gericht zijn de belangen van de beleggingsonderneming optimaal te behartigen, zouden kunnen belemmeren. Beleggingsondernemingen houden er rekening mee dat belangenconflicten van invloed kunnen zijn op de onafhankelijkheid van geest van leden van het leidinggevend orgaan[24].

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

108. Feitelijke of potentiële belangenconflicten die zijn aangemeld bij de verantwoordelijke functie binnen de beleggingsonderneming dienen naar behoren te worden beoordeeld en beheerd. Als een belangenconflict van een personeelslid is vastgesteld, documenteert de beleggingsonderneming de genomen beslissing, met name wanneer het belangenconflict en

[24] 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 overeenkomstig Richtlijn 2013/36/EU en Richtlijn 2014/65/EU.

de bijbehorende risico's zijn aanvaard en, als het belangenconflict is aanvaard, de manier waarop dit afdoende is beperkt of weggenomen.

109. 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.

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

110. Als onderdeel van hun beleid inzake belangenconflicten voor personeelsleden (hoofdstuk 11) en het beheer van belangenconflicten van leden van het leidinggevend orgaan zoals uiteengezet in punt 107, zet het leidinggevend orgaan een kader op voor het in kaart brengen en beheren van belangenconflicten in de context van het verstrekken van leningen en het aangaan van andere transacties, bijv. beursintroducties, dienstovereenkomsten of uitbestedingsovereenkomsten met leden van het leidinggevend orgaan en hun verbonden partijen.

111. Beleggingsondernemingen overwegen aanvullende categorieën van verbonden partijen aan te wijzen waarop zij hun kader voor belangenconflicten inzake leningen en transacties geheel of gedeeltelijk van toepassing verklaren.

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

113. Het leidinggevend orgaan zet de toepasselijke besluitvormingsprocessen op inzake het verstrekken van leningen aan en het aangaan van andere transacties met leden van het leidinggevend orgaan en hun verbonden partijen. Binnen dat kader kan onderscheid worden gemaakt tussen enerzijds standaard zakelijke transacties[25] die worden aangegaan in het kader van de normale bedrijfsuitoefening en conform de reguliere marktvoorwaarden, en anderzijds transacties met personeelsleden onder voorwaarden die voor alle personeelsleden gelden. Verder kan in het kader voor belangenconflicten en het besluitvormingsproces ook onderscheid worden gemaakt tussen belangrijke en niet-belangrijke leningen en andere belangrijke transacties, verschillende soorten leningen en andere transacties en het niveau van de feitelijke of potentiële belangenconflicten die zij kunnen doen ontstaan.

114. Als onderdeel van het kader voor belangenconflicten hanteert het leidinggevend orgaan passende drempelwaarden (bijv. per producttype, volume of afhankelijk van de voorwaarden)

[25] Onder zakelijke transacties wordt onder meer verstaan leasing, factoring, diensten in verband met beursintroducties, fusies en overnames, en de koop en verkoop van eigendommen.

die het bedrag aangeven waarboven de transactie met een lid van het leidinggevend orgaan of een verbonden partij altijd goedkeuring van het leidinggevend orgaan behoeft. Beslissingen inzake belangrijke leningen en andere belangrijke transacties met leden van het leidinggevend orgaan die niet conform reguliere marktvoorwaarden worden verstrekt of verricht, maar onder voorwaarden die voor alle personeelsleden gelden, worden altijd door het leidinggevend orgaan genomen.

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

116. Alvorens een beslissing te nemen over een lening of andere transactie met een lid van het leidinggevend orgaan of hun verbonden partijen, beoordeelt de beleggingsonderneming het risico waaraan zij als gevolg van die transactie mogelijk wordt blootgesteld.

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

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

118. Voor de toepassing van artikel 26 van Richtlijn (EU) 2019/2034 documenteren beleggingsondernemingen gegevens over leningen aan leden van het leidinggevend orgaan en hun verbonden partijen naar behoren, met vermelding van in ieder geval:

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

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

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

d. de datum waarop de lening is goedgekeurd;

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

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

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

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

12 Interne meldingsprocedures

120. Beleggingsondernemingen voeren passend intern meldingsbeleid en passende interne meldingsprocedures in opdat medewerkers potentiële of feitelijke inbreuken op Verordening (EU) nr. 2033/2019 en nationale bepalingen tot omzetting van Richtlijn (EU) 2019/2034 via een specifiek, onafhankelijk en zelfstandig kanaal kunnen melden, en onderhouden deze. Er wordt van personeelsleden die een inbreuk melden, niet geëist dat zij daarvan bewijs leveren; zij dienen er echter zo zeker van te zijn dat er voldoende reden is om een onderzoek te starten. Daarnaast richten beleggingsondernemingen passende processen en procedures in die waarborgen dat zij voldoen aan hun verplichtingen uit hoofde van de nationale uitvoering van Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden.

121. Om belangenconflicten te voorkomen dienen personeelsleden inbreuken te kunnen melden buiten de reguliere rapportagelijnen om (bijv. via de nalevingsfunctionaris, 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 Verordening (EU) 2016/679[26] (AVG).

122. De meldingsprocedures worden beschikbaar gesteld aan alle personeelsleden in een beleggingsonderneming.

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

124. Beleggingsondernemingen zorgen ervoor dat de persoon die de inbreuk meldt, afdoende wordt beschermd tegen eventuele negatieve gevolgen, zoals vergelding, discriminatie of

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

andere soorten onbillijke behandeling. De beleggingsonderneming zorgt ervoor dat geen enkele persoon die onder controle van de beleggingsonderneming 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.

125. Beleggingsondernemingen 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 beleggingsonderneming deze op zodanige wijze dat de betrokken persoon wordt beschermd tegen onbedoelde negatieve effecten die het doel van de maatregel overstijgen.

126. Interne meldingsprocedures dienen met name:

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

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

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

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

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

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

g. te waarborgen dat de gegevens goed worden bewaard.

13 Melding van inbreuken aan bevoegde autoriteiten

127. Overeenkomstig artikel 22 van Richtlijn (EU) 2019/2034 zetten bevoegde autoriteiten doeltreffende en betrouwbare mechanismen op opdat mogelijke of daadwerkelijke inbreuken op Verordening (EU) 2019/2033 en nationale bepalingen tot omzetting van Richtlijn (EU) 2019/2034 aan de bevoegde autoriteiten kunnen worden gemeld. Deze mechanismen bevatten ten minste:

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

b. passende bescherming als bedoeld in hoofdstuk 13;

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

d. heldere procedures zoals beschreven in hoofdstuk 12.

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

Titel V – Kader en mechanismen voor interne controle

14 Kader voor interne controle

129. Beleggingsondernemingen ontwikkelen en handhaven een cultuur die een positieve houding jegens risicobeheersing en naleving binnen de beleggingsonderneming aanmoedigt, evenals een solide en alomvattend kader voor interne controle. Krachtens dit kader zijn de bedrijfsonderdelen van beleggingsondernemingen verantwoordelijk voor het beheren van de risico's die zij lopen bij het uitvoeren van hun activiteiten en beschikken zij over controles die de naleving van interne en externe vereisten waarborgen. Als onderdeel van dit kader beschikken beleggingsondernemingen over een permanente en doeltreffende interne compliancefunctie [27] met passend en voldoende gezag, status en toegang tot het leidinggevend orgaan om haar taak te vervullen, evenals over een risicobeheerkader. Beleggingsondernemingen hebben ook een interne risicobeheer- en auditfunctie, waar dat evenredig is met inachtneming van de criteria in titel I.

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

[27] Onverminderd artikel 22 van de Gedelegeerde Verordening (EU) 565/2017 van de Commissie.

controlefuncties op groepsniveau en het leidinggevend orgaan van de beleggingsonderneming.

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

132. 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.

133. Het kader voor interne controle van een beleggingsonderneming waarborgt het volgende:

a. doeltreffende en efficiënte activiteiten;

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

c. de betrouwbaarheid van financiële en niet-financiële informatie die intern of extern wordt gerapporteerd;

d. solide administratieve en boekhoudkundige procedures; en

e. naleving van wetten, regelgeving, toezichtvereisten en het interne beleid en de interne procedures, regels en besluiten van de beleggingsonderneming.

15 Invoering van een kader voor interne controle

134. 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 naleving, met inbegrip van AML/CTF-naleving als dat een afzonderlijke controlefunctie is, en risicobeheer en interne auditfuncties, indien deze zijn ingesteld). Beleggingsondernemingen stellen, door het leidinggevend orgaan goed te keuren, adequate schriftelijke beleidslijnen, mechanismen en procedures voor interne controle op, handhaven deze en werken ze regelmatig bij. Wanneer er geen risicobeheerfunctie is ingesteld, is het leidinggevend orgaan verantwoordelijk voor het vaststellen en monitoren van toereikende procedures en toereikend beleid voor risicobeheer.

135. Een beleggingsonderneming beschikt over een duidelijk, transparant en gedocumenteerd besluitvormingsproces en zorgt voor een heldere toewijzing van verantwoordelijkheden en bevoegdheden binnen haar kader voor interne controle, met inbegrip van haar bedrijfsonderdelen, interne eenheden en interne controlefuncties.

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

137. 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.

138. Interne controlefuncties brengen bij het leidinggevend orgaan regelmatig schriftelijk verslag uit over grote vastgestelde gebreken. Deze rapporten bevatten voor elk nieuw vastgesteld belangrijk gebrek de relevante betrokken risico's, een effectbeoordeling, aanbevelingen en te nemen corrigerende maatregelen. Het leidinggevend orgaan volgt de bevindingen van de interne controlefuncties tijdig en doeltreffend op en eist toereikende herstelacties. Er wordt een formele follow-upprocedure voor bevindingen en corrigerende maatregelen opgesteld.

16 Het kader voor risicobeheer

139. Beleggingsondernemingen beschikken, als onderdeel van het algehele kader voor interne controle, over een holistisch, organisatiebreed kader voor risicobeheer dat zich uitstrekt over al hun bedrijfsonderdelen en interne eenheden, waaronder interne controlefuncties, waarin de economische realiteit van al hun risicoblootstellingen ten volle wordt erkend met inbegrip van de risico's die de ondernemingen opleveren voor henzelf, hun cliënten en hun markten, en liquiditeitsrisico's, met name die welke een wezenlijke impact kunnen hebben op het beschikbare eigen vermogen of dit vermogen aanzienlijk kunnen uitputten. Het kader voor risicobeheer stelt de beleggingsonderneming in staat om geïnformeerde besluiten te nemen inzake het nemen van risico's. Het kader voor risicobeheer omvat alle risico's, evenals feitelijke risico's en toekomstige risico's waaraan de beleggingsonderneming mogelijk is of kan worden blootgesteld. Risico's worden bottom-up en top-down beoordeeld, binnen elk bedrijfsonderdeel en over alle bedrijfsonderdelen heen, waarbij gebruik wordt gemaakt van consistente terminologie en onderling verenigbare methodieken binnen de gehele beleggingsonderneming en op geconsolideerd 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 markt-, liquiditeits-, concentratie-, operationele, IT-, reputatie-, juridische en gedragsrisico's, nalevingsrisico's in verband met AML/CTF en andere financiële misdrijven, ESG-risico's en strategische risico's.

140. Het kader voor risicobeheer van een beleggingsonderneming bevat 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 beleggingsonderneming en op geconsolideerd niveau.

141. Dit kader geeft specifieke sturing aan de uitvoering van de strategieën van de beleggingsonderneming. Dit betekent dat zo nodig interne limieten worden vastgesteld en gehandhaafd die stroken met de risicobereidheid van de beleggingsonderneming, en overeenstemmen met het deugdelijk functioneren, de financiële kracht, kapitaalbasis en de strategische doelstellingen van de beleggingsonderneming. Het risicoprofiel van een beleggingsonderneming 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.

142. Het kader voor risicobeheer wordt onderworpen aan een onafhankelijk interne toetsing, die bijvoorbeeld wordt uitgevoerd door de interne auditfunctie, en regelmatig opnieuw wordt getoetst aan de risicobereidheid van de beleggingsonderneming, 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, waaronder veranderingen in de inkomsten; eventuele toename van de complexiteit van de bedrijfsactiviteiten van de beleggingsonderneming, het risicoprofiel of de werkstructuur; geografische expansie; fusies en overnames; en de introductie van nieuwe producten of bedrijfsonderdelen.

143. Beleggingsondernemingen ontwikkelen passende methoden voor het identificeren, meten of beoordelen van risico's, waaronder zowel toekomstgerichte als retrospectieve instrumenten. De instrumenten maken het mogelijk om het feitelijke risicoprofiel af te zetten tegen de risicobereidheid van de beleggingsonderneming, en om potentiële risicoblootstellingen en risicoblootstellingen in stresssituaties onder een reeks voorziene ongunstige omstandigheden te identificeren en te beoordelen met inachtneming van de risicodraagkracht van de beleggingsonderneming. De instrumenten geven informatie over iedere eventueel benodigde aanpassing van het risicoprofiel. Beleggingsondernemingen doen voldoende voorzichtige aannames wanneer zij stressscenario's opstellen.

144. Beleggingsondernemingen 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 beleggingsonderneming. 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 wordt expliciet aandacht besteed aan belangrijke trends en gegevens

betreffende het macro-economische klimaat om hun potentiële effect op blootstellingen en portefeuilles in kaart te brengen.

145. De uiteindelijke verantwoordelijkheid voor risicobeoordeling berust uitsluitend bij de beleggingsonderneming, die haar risico's dus kritisch dient te evalueren en zich niet uitsluitend dient te verlaten op externe beoordelingen.

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

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

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

149. 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 beleggingsonderneming heen, als naar boven en naar beneden in de managementketen.

17 Interne controlefuncties

150. De interne controlefuncties omvatten een doeltreffende en permanente interne compliancefunctie en, waar passend en evenredig, rekening houdend met de criteria in titel I, een risicobeheerfunctie en een interne auditfunctie. De controlefuncties zijn er onder meer verantwoordelijk voor te waarborgen dat de AML/CTF-vereisten worden nageleefd. Wanneer beleggingsondernemingen geen risicobeheerfunctie en interne auditfunctie opzetten en in stand houden, kunnen zij op verzoek aantonen dat het beleid en de procedures voor een intern controlekader die zij hebben aangenomen en ingevoerd, daadwerkelijk hetzelfde resultaat opleveren als de in deze titel V verstrekte richtsnoeren.

151. Wanneer de beleggingsonderneming geen interne risicobeheer- of auditfunctie instelt, berusten de verantwoordelijkheden van deze functies als omschreven in deze richtsnoeren,

bij de medewerkers die zijn belast met de vastgestelde procedures en uiteindelijk bij het leidinggevend orgaan, dat de operationele taken intern of extern mag delegeren.

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

17.1 Hoofden van de interne controlefuncties

153. Hoofden van interne controlefuncties worden op een zodanig hiërarchisch niveau aangesteld dat zij het gezag en de status krijgen die nodig zijn om hun verantwoordelijkheden te vervullen. Daartoe dienen de hoofden van de risicobeheer- en, indien ingesteld, compliance- 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.

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

155. Beleggingsondernemingen beschikken over gedocumenteerde processen voor de toewijzing van de functie van hoofd van een interne controlefunctie en voor de intrekking van zijn of haar verantwoordelijkheden. De hoofden van interne controlefuncties mogen in geen geval uit hun functie worden verwijderd zonder voorafgaande goedkeuring van het leidinggevend orgaan in zijn toezichtfunctie.

17.2 Onafhankelijkheid van interne controlefuncties

156. Om als onafhankelijk functionerend te worden aangemerkt, dienen de interne 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, tenzij is aangetoond dat, rekening houdend met de criteria in titel I voor de toepassing van het evenredigheidsbeginsel, de interne controlefuncties nog altijd doeltreffend zijn. In dat geval beoordelen beleggingsondernemingen of de doeltreffendheid van hun interne controlefuncties in gevaar is gekomen.

b. Ze zijn, waar passend, organisatorisch gescheiden van de activiteiten die zij dienen te monitoren en controleren.

c. 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[28].

17.3 Personele middelen van interne controlefuncties

157. Interne controlefuncties beschikken over voldoende middelen. Zij hebben een voldoende aantal gekwalificeerde medewerkers (zowel op het niveau van het moederbedrijf als van de dochteronderneming), rekening houdend met het evenredigheidsbeginsel zoals vastgelegd in titel I. Het personeel blijft continu gekwalificeerd en wordt zo nodig opgeleid.

158. Interne controlefuncties beschikken over passende IT-systemen en ondersteuning, en hebben toegang tot de interne en externe informatie die nodig is om aan hun verantwoordelijkheden te voldoen. Zij hebben toegang tot alle benodigde informatie over alle bedrijfsonderdelen en relevante risicodragende dochterondernemingen, met name die welke potentieel belangrijke risico's voor de beleggingsondernemingen kunnen voortbrengen.

18 Risicobeheerfunctie

159. De risicobeheerfunctie strekt zich uit over de gehele beleggingsonderneming. 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.

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

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

162. 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.

163. De risicobeheerfunctie staat organisatorisch centraal in de beleggingsonderneming 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

[28] 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

verwezenlijking van doeltreffende risicobeheerprocessen in de beleggingsonderneming. De risicobeheerfunctie is actief betrokken bij alle belangrijke risicobeheerbesluiten.

164. In een groep is de risicobeheerfunctie in de EU-moederonderneming in staat een groepsbreed holistisch perspectief te bieden op alle risico's en ervoor te zorgen dat de risicostrategie wordt nageleefd.

165. 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 eenheden, en stelt zij het leidinggevend orgaan ervan op de hoogte of die informatie en adviezen stroken met de risicostrategie en risicobereidheid van de beleggingsonderneming. De risicobeheerfunctie kan aanbevelingen doen voor de verbetering van het kader voor risicobeheer en voor corrigerende maatregelen in het geval van overtredingen van risicobeleid, -procedures en -limieten.

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

166. De risicobeheerfunctie wordt in een vroeg stadium actief betrokken bij de uitwerking van de risicostrategie van de beleggingsonderneming en bij de verwezenlijking van doeltreffende risicobeheerprocessen in de beleggingsonderneming. De risicobeheerfunctie verschaft het leidinggevend orgaan alle relevante risicogerelateerde informatie op basis waarvan dit orgaan de risicobereidheid van de beleggingsonderneming 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 en risicobereidheid. Streefcijfers dienen geloofwaardig te zijn en te stroken met de risicostrategie en -bereidheid van de beleggingsonderneming.

167. 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.

18.2 De rol van de risicobeheerfunctie bij belangrijke veranderingen

168. Voordat besluiten worden genomen over belangrijke veranderingen in processen of systemen of buitengewone transacties, wordt de risicobeheerfunctie betrokken bij de beoordeling van het effect van dergelijke veranderingen en buitengewone transacties op het risico voor de

beleggingsonderneming en de groep als geheel, en rapporteert zij haar bevindingen ook rechtstreeks aan het leidinggevend orgaan voordat een besluit wordt genomen.

169. De risicobeheerfunctie beoordeelt in hoeverre geïdentificeerde risico's van invloed zijn op het vermogen van de beleggingsonderneming of groep om zijn of haar risicoprofiel, liquiditeit en solide kapitaalbasis te beheren onder normale en ongunstige omstandigheden.

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

170. De risicobeheerfunctie zorgt voor een passend kader voor risicobeheer en waarborgt dat alle risico's worden geïdentificeerd, beoordeeld, gemeten, gemonitord, beheerd en naar behoren worden gerapporteerd door de relevante eenheden in de beleggingsonderneming.

171. De risicobeheerfunctie zorgt ervoor dat identificatie en beoordeling niet uitsluitend worden gebaseerd op kwantitatieve informatie of uitkomsten van modellen, maar ook een kwalitatieve benadering omvatten. 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.

172. De risicobeheerfunctie waarborgt dat transacties met verbonden partijen worden getoetst en dat de risico's ervan voor de beleggingsonderneming worden geïdentificeerd en naar behoren worden beoordeeld.

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

174. De risicobeheerfunctie ziet regelmatig toe op het werkelijke risicoprofiel van de beleggingsonderneming en toetst dit aan de strategische doelstellingen en risicobereidheid van de beleggingsonderneming teneinde het leidinggevend orgaan in zijn bestuursfunctie in staat te stellen besluiten te nemen en het leidinggevend orgaan in zijn toezichtfunctie in staat te stellen zijn controlerende taak uit te oefenen.

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

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

18.4 De rol van de risicobeheerfunctie bij limieten

177. De risicobeheerfunctie beoordeelt op onafhankelijke wijze overschrijdingen van risicobereidheid of risicolimieten (dit omvat ook 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.

178. 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.

18.5 Hoofd van de risicobeheerfunctie

179. Het hoofd van de risicobeheerfunctie, indien deze is ingesteld, 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 beleggingsonderneming kan begrijpen. Hetzelfde geldt voor het hoofd van de risicobeheerfunctie van een moederbeleggingsonderneming met betrekking tot de geconsolideerde situatie. Wanneer er geen onafhankelijke functie is ingesteld, berusten de verantwoordelijkheden van het hoofd van de risicobeheerfunctie bij de medewerkers die belast zijn met de risicobeheerprocedures of rechtstreeks bij de leden van het leidinggevend orgaan.

180. 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 beleggingsonderneming aan risico's. Als het hoofd van de risicobeheerfunctie geen lid is van het leidinggevend orgaan, benoemen beleggingsondernemingen, met inachtneming van het evenredigheidsbeginsel dat wordt uiteengezet in titel I, 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 compliancefunctie, of kan zij worden vervuld door een ander lid van het hoger personeel, mits er geen belangenconflict tussen de verrichte taken bestaat. Deze persoon beschikt in ieder geval over voldoende gezag, status en onafhankelijkheid (bijv. hoofd van juridische zaken).

181. Het hoofd van de risicobeheerfunctie is in staat besluiten van het bestuur en het leidinggevend orgaan van de beleggingsonderneming aan te vechten, en de redenen van bezwaren worden formeel gedocumenteerd. Als een beleggingsonderneming 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 dat vetorecht, evenals de wijze waarop het leidinggevend orgaan daarbij zal worden betrokken.

182. Beleggingsondernemingen stellen stringente procedures vast voor de goedkeuring van besluiten waarover het hoofd van de risicobeheerfunctie een negatief oordeel heeft gegeven. Het leidinggevend orgaan in zijn toezichtfunctie kan rechtstreeks communiceren met het hoofd van de risicobeheerfunctie over belangrijke risicoproblemen, waaronder ontwikkelingen die mogelijk niet stroken met de risicostrategie en -bereidheid van de beleggingsonderneming.

19 Compliancefunctie[29]

183. Beleggingsondernemingen stellen een permanente en doeltreffende compliancefunctie in die nalevingsrisico's beheert, en benoemen een persoon die binnen de gehele beleggingsonderneming deze functie uitoefent (de nalevingsfunctionaris). De compliancefunctie, het nalevingsbeleid en de nalevingsprocedures dienen ook in overeenstemming te zijn met artikel 22 van Gedelegeerde Verordening (EU) 2017/565 van de Commissie en de ESMA-richtsnoeren over de compliancefunctie.

184. De rol van de nalevingsfunctionaris kan, met inachtneming van het evenredigheidsbeginsel als omschreven in titel I, worden gecombineerd met de functie van hoofd van de risicobeheerfunctie of kan, wanneer het niet evenredig is iemand te benoemen die uitsluitend deze taak krijgt toegewezen, worden vervuld door een ander lid van het hoger personeel (bijv. hoofd van juridische zaken), mits er geen belangenconflict tussen de verrichte taken bestaat.

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

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

187. De compliancefunctie adviseert het leidinggevend orgaan over de maatregelen die moeten worden genomen om de naleving van alle toepasselijke wet- en regelgeving en normen te

[29] Dit hoofdstuk dient te worden gelezen onverminderd en in samenhang met de richtsnoeren van ESMA over de compliancefunctie.

waarborgen, en beoordeelt het mogelijke effect van eventuele wijzigingen in het wet- en regelgevend kader op de activiteiten en het nalevingskader van de beleggingsonderneming.

188. De compliancefunctie 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 compliancefunctie rapporteert aan het leidinggevend orgaan en communiceert in voorkomend geval met de risicobeheerfunctie over het nalevingsrisico van de beleggingsonderneming en het beheer daarvan. De compliancefunctie 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 compliancefunctie.

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

190. Beleggingsondernemingen 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 EU-moederonderneming hiervan op de hoogte.

20 Interne auditfunctie

191. De interne auditfunctie, indien deze is ingesteld, is onafhankelijk en beschikt over voldoende gezag, status en middelen. De beleggingsonderneming zorgt er in het bijzonder voor dat de kwalificatie van de personeelsleden en de middelen van de interne auditfunctie, met name haar controle-instrumenten en risico-analysemethoden, toereikend zijn voor de omvang en locaties van de beleggingsonderneming, en voor de aard, schaal en complexiteit van de risico's die inherent zijn aan het bedrijfsmodel, de activiteiten, de risicocultuur en de risicobereidheid van de beleggingsonderneming.

192. De interne auditfunctie is onafhankelijk van de gecontroleerde activiteiten. Daarom wordt de interne auditfunctie niet met andere functies gecombineerd.

193. De interne auditfunctie verschaft, op grond van een risicogebaseerd onderzoek, op onafhankelijke en objectieve wijze zekerheid dat alle activiteiten en eenheden van een beleggingsonderneming, met inbegrip van uitbestede activiteiten, in overeenstemming zijn met het beleid en de procedures van de beleggingsonderneming en de wettelijke vereisten. Elke entiteit binnen de groep ressorteert onder de interne auditfunctie.

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

195. De interne auditfunctie beoordeelt of het kader voor interne controle van de beleggingsonderneming zoals dat is uiteengezet in hoofdstuk 15, zowel effectief als doeltreffend is. De interne auditfunctie beoordeelt in het bijzonder:

    a. de geschiktheid van het governancekader van de beleggingsonderneming;

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

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

    d. of de procedures op correcte en doeltreffende wijze ten uitvoer worden gelegd (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 compliancefuncties.

196. De interne auditfunctie controleert met name de integriteit van de processen en waarborgt daarbij de betrouwbaarheid van de methoden en technieken, en de aannames en informatiebronnen die in de interne modellen van de beleggingsonderneming worden gebruikt (bijv. risicomodellering en boekhoudkundige metingen). Voorts beoordeelt de interne auditfunctie de kwaliteit en het gebruik van de instrumenten voor kwalitatieve risico-identificatie en -beoordeling en de genomen risicobeperkende maatregelen.

197. De interne auditfunctie heeft binnen de gehele beleggingsonderneming onbelemmerde toegang tot alle gegevens, documenten, informatie en gebouwen van de beleggingsonderneming. Daartoe behoort ook toegang tot managementinformatiesystemen en notulen van alle comités en besluitvormingsorganen.

198. De interne auditfunctie neemt nationale en internationale professionele normen in acht. Een voorbeeld hiervan zijn de normen zoals vastgesteld door het Institute of Internal Auditors.

199. Interne auditwerkzaamheden worden verricht op basis van een auditplan en een gedetailleerd, risicogebaseerd auditprogramma.

200. 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.

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

Titel VI – Beheer van de bedrijfscontinuïteit

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

203. Beleggingsondernemingen kunnen een specifieke onafhankelijke bedrijfscontinuïteitsfunctie instellen.

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

205. Om een gedegen bedrijfscontinuïteitsbeheerplan te kunnen vaststellen, analyseert de beleggingsonderneming zorgvuldig de risicofactoren ten aanzien van, en haar blootstelling aan, ernstige bedrijfsonderbrekingen, en maakt zij een beoordeling van de potentiële (kwantitatieve en kwalitatieve) effecten hiervan. Daarbij worden interne en/of externe onderzoeken van gegevens en scenario's benut. In deze analyse komen alle bedrijfsonderdelen en interne eenheden aan bod, met inbegrip van de risicobeheerfunctie en risicobeheerprocedures, en wordt rekening gehouden met hun onderlinge afhankelijkheid en verwevenheid. De resultaten van de analyse dragen bij aan de bepaling van de herstelprioriteiten en -doelstellingen van de beleggingsonderneming.

206. Op basis van bovengenoemde analyse stelt een beleggingsonderneming de volgende plannen op:

    a. noodplannen en bedrijfscontinuïteitsplannen die ervoor zorgen dat de beleggingsonderneming 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 beleggingsonderneming 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 beleggingsonderneming.

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

Titel VII – Transparantie

208. Al het relevante personeel in een beleggingsonderneming wordt op de hoogte gesteld van strategieën, beleid en procedures. De medewerkers van een beleggingsonderneming dienen het beleid en de procedures die relevant zijn voor hun taken en verantwoordelijkheden, te begrijpen en na te leven.

209. 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 specifieke taken uit te voeren. De informatie kan worden aangereikt door middel van schriftelijke richtsnoeren, handboeken of andere middelen.

210. Waar moederondernemingen er door bevoegde autoriteiten uit hoofde van artikel 44 van Richtlijn (EU) 2019/2034 toe worden verplicht jaarlijks een beschrijving te publiceren van hun juridische structuur en van de governance- en organisatiestructuur van de groep beleggingsondernemingen, dient deze informatie per land alle entiteiten binnen de groepsstructuur te omvatten, zoals vastgelegd in Richtlijn 2013/34/EU[30].

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

a. een overzicht van de interne organisatie van de beleggingsondernemingen 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;

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

c. nieuwe juridische, governance- of organisatiestructuren;

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

e. de belangrijkste verantwoordelijkheden van het leidinggevend orgaan;

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

g. een overzicht van het beleid inzake belangenconflicten dat van toepassing is op de beleggingsonderneming 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 beleggingsondernemingen 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. Samenstelling en functioneren van het leidinggevend orgaan
   a) selectiecriteria, met vermelding van de wijze waarop rekening wordt gehouden met diversiteit
   b) aantal, duur van het mandaat, roulering, leeftijd
   c) onafhankelijke leden van het leidinggevend orgaan
   d) uitvoerende leden van het leidinggevend orgaan
   e) niet-uitvoerende leden van het leidinggevend orgaan
   f) interne taakverdeling, indien van toepassing
4. Governancestructuur en organisatieschema (en de gevolgen voor de groep, indien van toepassing)
   a) gespecialiseerde comités
      i. samenstelling
      ii. functioneren
   b) bestuur, indien dat er is
      i. samenstelling
      ii. functioneren
5. Medewerkers met een sleutelfunctie
   a) hoofd van de risicobeheerfunctie
   b) hoofd van de compliancefunctie
   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
7. Beschrijving van de risicostrategie en het kader voor risicobeheer
8. Organisatiestructuur (en de gevolgen voor de groep, indien van toepassing)
    a) operationele structuur, bedrijfsonderdelen en toewijzing van bevoegdheden en verantwoordelijkheden
    b) uitbesteding
    c) aanbod aan producten en diensten
    d) geografisch werkterrein
    e) dienstverlening onder het stelsel van de vrijheid van dienstverrichting
    f) bijkantoren
    g) dochterondernemingen, samenwerkingsverbanden enz.
    h) gebruik van offshore centra
9. Gedragscode en gedrag (en de gevolgen voor de groep, indien van toepassing)
    a) strategische doelstellingen en bedrijfswaarden
    b) Interne codes en voorschriften, waaronder beleid voor het bestrijden van het witwassen van geld en terrorismefinanciering
    c) beleid inzake belangenconflicten
    d) klokkenluiden
10. Status van het beleid inzake interne governance, met datum
    a) ontwikkeling
    b) laatste wijziging
    c) laatste beoordeling
    d) goedkeuring door het leidinggevend orgaan