Europese Bankautoriteit

EBA BS 2011 116 definitief

27 september 2011

EBA-richtsnoeren inzake interne governance

(GL 44)

Londen, 27 september 2011

EBA-richtsnoeren inzake interne governance

Status van de richtsnoeren

1. Dit document bevat richtsnoeren die zijn uitgebracht op grond van artikel 16 van 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 (hierna "de EBA-verordening") Overeenkomstig artikel 16, lid 3, van de EBA-verordening moeten bevoegde autoriteiten en financiële instellingen zich tot het uiterste inspannen om aan de richtsnoeren te voldoen.

2. Richtsnoeren geven weer wat in de opvatting van de EBA passende toezichtpraktijken binnen het Europees Systeem voor financieel toezicht zijn en hoe het recht van de Unie op een specifiek gebied dient te worden toegepast. De EBA verwacht derhalve van alle bevoegde autoriteiten en deelnemers aan de financiële markten voor wie de richtsnoeren gelden, dat ze deze zullen naleven, tenzij anders aangegeven. Bevoegde autoriteiten voor wie deze richtsnoeren gelden, moeten deze op passende wijze in hun toezichtpraktijken integreren (bijv. door hun rechtskader of hun toezichtvoorschriften, -leidraden of -processen aan te passen), ook wanneer specifieke richtsnoeren in dit document primair tot instellingen zijn gericht.

Kennisgevingsverplichtingen

3. Bevoegde autoriteiten stellen de EBA vóór 28 november 2012 ervan in kennis of zij aan deze richtsnoeren voldoen of voornemens zijn deze op te volgen, of, indien dit niet het geval is, wat de redenen van de niet-naleving zijn. Kennisgevingen worden bij de EBA (compliance@eba.europa.eu) ingediend door daartoe bevoegde personen namens hun bevoegde autoriteit.

4. De in de vorige paragraaf bedoelde kennisgeving van bevoegde autoriteiten wordt gepubliceerd op de website van de EBA, overeenkomstig artikel 16 van de EBA-verordening.

In deze richtsnoeren zijn tekstkaders opgenomen waarin bepaalde aspecten nader worden toegelicht, waarbij voorbeelden dan wel de beweegredenen achter een bepaling worden gegeven.

Inhoudsopgave

Titel I – Onderwerp, toepassingsgebied en definities

1. Onderwerp

Deze richtsnoeren hebben tot doel de verwachtingen inzake toezicht met elkaar in overeenstemming te brengen en de juiste uitvoering van interne-governanceregelingen te bevorderen overeenkomstig artikel 22 van en bijlage V bij Richtlijn 2006/48/EG en de nationale voorschriften op het gebied van het vennootschapsrecht.

2. Toepassingsgebied en -niveau

1. Bevoegde autoriteiten dienen instellingen te verplichten om de in deze richtsnoeren inzake interne governance neergelegde bepalingen na te leven.
2. De toepassing van deze richtsnoeren dient door de bevoegde autoriteiten te worden beoordeeld in het kader van het toetsings- en evaluatieproces.

Toelichting
Het Comité van Europese bankentoezichthouders (CEBT) en de EBA hebben richtsnoeren inzake het proces van bedrijfseconomisch toezicht opgesteld, die te vinden zijn op de website van de EBA.

3. De richtsnoeren zijn van toepassing op instellingen (op individuele basis) en op moederondernemingen (op geconsolideerde en sub-geconsolideerde basis), tenzij in deze richtsnoeren anders wordt bepaald.
4. De bepalingen van deze richtsnoeren eerbiedigen het evenredigheidsbeginsel zoals neergelegd in de Richtlijnen 2006/48 en 2006/49 (als gewijzigd). Een instelling kan aantonen hoe haar aanpak – waarin de aard, omvang en complexiteit van haar activiteiten terug te vinden zijn – beantwoordt aan het door de richtsnoeren geëiste resultaat.

3. Definities

1. In deze richtsnoeren dient onder "leidinggevend orgaan" te worden verstaan: het bestuurslichaam (of de bestuurslichamen) van een instelling, met daarin verenigd de toezicht- en bestuursfuncties, dat de uiteindelijke beslissingsbevoegdheid heeft en bevoegd is om de strategie, doelstellingen en algemene richting van de instelling te bepalen. Tot het leidinggevend orgaan dienen de personen te behoren die effectief leiding geven aan de bedrijfsactiviteiten van de instelling.
2. In deze richtsnoeren dient onder "instellingen" te worden verstaan: kredietinstellingen en beleggingsondernemingen als omschreven in Richtlijn 2006/48/EG en Richtlijn 2006/49/EG.

Titel II – Eisen ten aanzien van de interne governance van instellingen

A. Bedrijfsstructuur en -organisatie

4. Organisatiekader

1. Het leidinggevend orgaan van een instelling dient te zorgen voor een geschikte en transparante bedrijfsstructuur voor die instelling. Deze structuur dient te getuigen van en bevorderend te zijn voor een doeltreffend en prudent beheer van de instelling, zowel op individuele basis als op het niveau van de groep. De rapportagelijnen en de toewijzing van verantwoordelijkheden dienen helder, welomschreven, samenhangend en verplichtend te zijn.
2. Het leidinggevend orgaan moet ervoor zorgen dat de structuur van een instelling en, in voorkomend geval, de structuren binnen een groep duidelijk en transparant zijn, niet alleen voor het eigen personeel van de instelling maar ook voor haar toezichthouders.
3. Het leidinggevend orgaan moet bepalen hoe de verschillende elementen van de bedrijfsstructuur elkaar aanvullen en met elkaar communiceren. De structuur mag het vermogen van het leidinggevend orgaan om de risico's van de instelling of groep te overzien en doeltreffend te beheren niet belemmeren.
4. Het leidinggevend orgaan moet beoordelen hoe wijzigingen in de groepsstructuur inwerken op de gezondheid ervan. Het leidinggevend orgaan moet eventueel noodzakelijke aanpassingen snel doorvoeren.

Toelichting
Wijzigingen kunnen bijvoorbeeld voortkomen uit de oprichting van nieuwe dochterondernemingen, fusies en overnames, uit het afstoten of opheffen van delen van de groep, of uit externe ontwikkelingen.

5. Controlemechanismen in een groepsstructuur

1. Binnen een groepsstructuur dient het leidinggevend orgaan van de moederonderneming van een instelling de algemene verantwoordelijkheid voor adequate interne governance in de hele groep te hebben en voor een governanceraamwerk te zorgen dat past bij de structuur, bedrijfsactiviteiten en risico's van de groep en haar deelentiteiten.
2. Het leidinggevend orgaan van een gereglementeerde dochteronderneming van een groep dient zich op het niveau van de rechtspersoon te houden aan dezelfde waarden en beleidsvormen op het gebied van interne governance als die van haar moederonderneming, tenzij juridische en toezichtvereisten of overwegingen ten aanzien van de evenredigheid anders bepalen. Bijgevolg moet het leidinggevend orgaan van een gereglementeerde dochteronderneming binnen haar eigen verantwoordelijkheden inzake interne governance zijn beleid vaststellen en besluiten of praktijken op het niveau van de groep evalueren om

te voorkomen dat de gereglementeerde dochteronderneming hierdoor in een situatie terechtkomt waarin wordt gehandeld in strijd met geldende voorschriften van wettelijke of bestuursrechtelijke dan wel prudentiële aard. Het leidinggevend orgaan van de gereglementeerde dochteronderneming moet er tevens voor zorgen dat deze besluiten of praktijken niet ten koste gaan van:

a. de deugdelijke en prudente bedrijfsvoering van de dochteronderneming;

b. de financiële gezondheid van de dochteronderneming; of

c. de juridische belangen van de stakeholders van de dochteronderneming.

3. De leidinggevende organen van de moederonderneming en haar dochterondernemingen moeten onderstaande paragrafen toepassen en in acht nemen, rekening houdend met het effect van de groepsdimensie op hun interne governance.
4. Bij de uitoefening van zijn verantwoordelijkheden inzake interne governance moet het leidinggevend orgaan van een instelling zich bewust zijn van alle materiële risico's en problemen die afbreuk kunnen doen aan de groep, de moederinstelling en haar dochterorganisaties. Zij moet derhalve adequaat toezicht uitoefenen op haar dochterondernemingen onder gelijktijdige eerbiediging van de onafhankelijke wettelijke en bestuursverantwoordelijkheden die van toepassing zijn op de bestuursorganen van gereglementeerde dochterondernemingen.
5. Om zich van zijn verantwoordelijkheden op het gebied van interne governance te kwijten, moet het leidinggevend orgaan van een moederonderneming:

a. een governancestructuur opzetten die bijdraagt aan een doeltreffend toezicht op de dochterondernemingen en rekening houdt met de aard, omvang en complexiteit van de verschillende risico's waaraan de groep en haar dochterondernemingen zijn blootgesteld;

b. goedkeuring verlenen aan beleid inzake interne governance op groepsniveau voor haar dochterondernemingen, waarin de verbintenis is opgenomen om aan alle governancevereisten te voldoen;

c. er zorg voor dragen dat er voor elke dochteronderneming toereikende middelen zijn om te voldoen aan de normen op het niveau van zowel de groep als de lokale governance;

d. over passende middelen beschikken om erop toe te zien dat alle dochterondernemingen alle toepasselijke interne-governancevereisten vervullen; en

e. ervoor zorgen dat rapportagelijnen in een groep duidelijk en transparant zijn, met name ingeval business lines afwijken van de juridische structuur van de groep.

6. Met het oog op een sterke governance moet een gereglementeerde dochteronderneming overwegen een voldoende aantal onafhankelijke leden zitting te laten nemen in het leidinggevend orgaan. Onafhankelijke leden van het leidinggevend orgaan zijn niet-uitvoerende directeuren die een onafhankelijke positie innemen ten opzichte van de dochteronderneming en haar groep en de controlerende aandeelhouder.

6. Ken uw structuur

1. Het leidinggevend orgaan dient de operationele structuur van een instelling ten volle te kennen en te begrijpen ("ken uw structuur") en ervoor te zorgen dat die structuur aansluit op de goedgekeurde bedrijfsstrategie en het risicoprofiel.

Toelichting
Het is essentieel dat het leidinggevend orgaan de operationele structuur van een instelling volledig kent en begrijpt. Wanneer een instelling binnen haar groep een groot aantal rechtspersonen opricht, kunnen het aantal en in het bijzonder de onderlinge verbindingen en transacties tussen deze rechtspersonen knelpunten vormen bij het ontwerp van haar interne governance en voor het beheer van en toezicht op de risico's van de groep als geheel, wat op zichzelf een risico met zich brengt.

2. Het leidinggevend orgaan moet in staat zijn de structuur van de instelling alsmede haar ontwikkeling en beperkingen te sturen en begrijpen. Voorts moet het kunnen aantonen dat de structuur in orde en niet nodeloos complex is. Het is eveneens verantwoordelijk voor de goedkeuring van deugdelijke strategieën en beleidsvormen voor de vaststelling van nieuwe structuren. Het leidinggevend orgaan moet daarnaast de risico's herkennen van een complexe rechtspersoonstructuur en ervoor zorgen dat de instelling tijdig informatie kan verstrekken over het type, de statuten, de eigendomsstructuur en de bedrijfsactiviteiten van iedere rechtspersoon.
3. Het leidinggevend orgaan van een moederonderneming van een instelling moet niet alleen de bedrijfsorganisatie van de groep kennen, maar ook het doel van haar verschillende entiteiten alsmede hun onderlinge verbanden en betrekkingen. Daarom is het zaak ook inzicht te hebben in operationele risico's die specifiek zijn voor de groep, in blootstellingen binnen de groep en in de wijze waarop financierings-, kapitaal- en risicoprofielen van de groep onder normale en ongunstige omstandigheden kunnen worden beïnvloed.
4. Het leidinggevend orgaan van een moederonderneming moet ervoor zorgen dat de verschillende entiteiten van de groep (met inbegrip van de instelling zelf) voldoende informatie ontvangen zodat zij alle een duidelijk beeld hebben van de algemene doelstellingen en risico's van de groep. Elke significante informatiestroom tussen entiteiten die relevant is voor de operationele werking

van de groep moet worden gedocumenteerd en op verzoek terstond beschikbaar worden gesteld aan het leidinggevend orgaan, de werknemers in een controlefunctie en de toezichthouders, naargelang wat van toepassing is.

5. Het leidinggevend orgaan van een moederonderneming van een instelling moet ervoor zorgen dat het op de hoogte blijft van de risico's die de structuur van de groep met zich brengt. Het betreft in dit verband:
   a. informatie over belangrijke risicobronnen, en
   b. periodieke rapporten waarin een beoordeling is vervat van de algemene structuur van de instelling en van de verenigbaarheid van activiteiten van de afzonderlijke entiteiten met de goedgekeurde strategie.

7. Activiteiten die niet standaard of niet transparant zijn

1. Indien een instelling haar activiteiten verricht via special-purpose- of aanverwante structuren dan wel actief is in rechtsgebieden die transparantie in de weg staan of niet aan internationale banknormen voldoen, dient het leidinggevend orgaan het doel en de structuur van die activiteiten alsmede de specifieke daarmee verband houdende risico's goed te begrijpen. Het leidinggevend orgaan mag alleen met deze activiteiten instemmen als het ervan overtuigd is dat de risico's passend worden beheerd.

Toelichting

Behalve van dit beginsel kunnen bevoegde autoriteiten zich ook bedienen van de kernbeginselen voor een effectief bankentoezicht, uitgewerkt door het Bazels Comité voor bankentoezicht, bij de evaluatie van bedrijfsactiviteiten in rechtsgebieden die niet volledig transparant zijn of niet aan internationale banknormen voldoen.

De instelling kan gerechtvaardigde redenen hebben om activiteiten te ontplooien in bepaalde rechtsgebieden (of met entiteiten of wederpartijen die in deze rechtsgebieden actief zijn), dan wel bepaalde structuren op te tuigen (bijvoorbeeld special purpose vehicles of corporate trusts). Activiteiten in rechtsgebieden die niet volledig transparant zijn of niet aan de internationale banknormen voldoen (bijvoorbeeld op het gebied van bedrijfseconomisch toezicht, belastingen, bestrijding van witwassen of bestrijding van terrorismefinanciering) of zich laten kenmerken door complexe of ondoorzichtige structuren kunnen bepaalde wettelijke, financiële en reputatierisico's met zich brengen. Ook kunnen ze afbreuk doen aan het vermogen van het leidinggevend orgaan om toezicht op de bedrijfsactiviteiten uit te oefenen, en een doeltreffend bankentoezicht belemmeren. Dergelijke structuren moeten daarom alleen worden goedgekeurd en gehandhaafd wanneer hun doel is vastgesteld en begrepen, doeltreffend toezicht

gewaarborgd is en alle bijbehorende materiële risico's die zij doen ontstaan naar behoren kunnen worden beheerd.

Het leidinggevend orgaan moet dus bijzondere aandacht aan al deze situaties schenken omdat ze het zeer moeilijk maken wegwijs te worden in de structuur van de groep.

2. Het leidinggevend orgaan moet op permanente basis passende strategieën, beleidsmaatregelen en procedures vaststellen, handhaven en evalueren die bedoeld zijn om dergelijke structuren en activiteiten goed te keuren en te handhaven met als oogmerk te waarborgen dat ze in overeenstemming blijven met het beoogde doel ervan.
3. Het leidinggevend orgaan moet zorgen voor passende maatregelen om de risico's van dergelijke activiteiten te vermijden of beperken. Dat betekent onder andere dat:

    a. de instelling adequate beleidsvormen, procedures en gedocumenteerde processen heeft ingevoerd (bijv. toepasselijke limieten, informatievereisten) voor het overwegen, goedkeuren en risicobeheer van deze activiteiten, rekening houdend met de gevolgen voor de operationele structuur van de groep;

    b. informatie over deze activiteiten en de bijbehorende risico's toegankelijk is voor het hoofdkantoor van de instelling en de accountants en wordt gerapporteerd aan het leidinggevend orgaan en de toezichthouders;

    c. de instelling op gezette tijden de continue noodzaak om activiteiten te verrichten die transparantie in de weg staan, langs de meetlat legt.

4. Dezelfde maatregelen moeten genomen worden wanneer een instelling voor klanten activiteiten verricht die niet standaard en niet transparant zijn.

Toelichting

Klantgerichte activiteiten die niet standaard en niet transparant zijn (bijv. klanten helpen met het oprichten van vehikels in externe rechtsgebieden, het optuigen van complexe structuren en het financieren van de betrokken transacties, of de verlening van trusteediensten) kunnen uitdagingen voor de interne governance inhouden en grote operationele en reputatierisico's met zich brengen. Het nemen van dezelfde risicobeheermaatregelen als voor de eigen bedrijfsactiviteiten van de instelling is derhalve noodzakelijk.

5. Al deze structuren en activiteiten moeten aan periodieke interne en externe accountantscontroles worden onderworpen.

B. Het leidinggevend orgaan

B.1 Taken en verantwoordelijkheden van het leidinggevend orgaan

8. Verantwoordelijkheden van het leidinggevend orgaan

1. De algehele verantwoordelijkheid voor de instelling dient bij het leidinggevend orgaan te liggen, dat tevens de strategie van de instelling dient vast te stellen. De verantwoordelijkheden van het leidinggevend orgaan dienen duidelijk in een schriftelijk document te worden vastgelegd en te worden goedgekeurd.

Toelichting
Deugdelijke uitoefening van de verantwoordelijkheden van het leidinggevend orgaan vormt de basis voor de gedegen en prudente bedrijfsvoering van de instelling. De op schrift gestelde verantwoordelijkheden moeten ook voldoen aan de nationale voorschriften op het gebied van het vennootschapsrecht.

2. De belangrijkste verantwoordelijkheden van het leidinggevend orgaan betreffen onder andere de vaststelling van en het toezicht op:

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

    b. de algehele risicostrategie en -beleidslijnen van de instelling, met inbegrip van haar risicotolerantie/-bereidheid en haar kader voor risicobeheer;

    c. de hoeveelheid, typen en verdeling van intern kapitaal en eigen middelen toereikend om de risico's van de instelling te dekken;

    d. een solide en transparante organisatiestructuur met effectieve communicatie- en rapportagekanalen;

    e. een beleid voor benoeming en opvolging van personen die belangrijke posities bekleden in de instelling;

    f. een beloningsstelsel dat aansluit op de risicostrategieën van de instelling;

    g. de governancebeginselen en ondernemingswaarden van de instelling, onder andere door middel van een gedragscode of soortgelijk document; en

    h. een adequaat en doeltreffend kader voor interne controle dat voorziet in doelmatige functies van risicobeheersing, compliance en interne audit, alsmede een deugdelijk raamwerk voor financiële verslaglegging en boekhouding.

3. Het behoort ook tot de taak van het leidinggevend orgaan om deze beleidslijnen en strategieën geregeld te herzien. Het leidinggevend orgaan is verantwoordelijk voor een goede communicatie met toezichthoudende instanties en andere belanghebbende partijen.

9. Beoordeling van het kader voor interne governance

1. Het leidinggevend orgaan dient op de doeltreffendheid van het kader voor interne governance van de instelling toe te zien en deze regelmatig te beoordelen.
2. Het kader voor interne governance en de tenuitvoerlegging daarvan moet ten minste een maal per jaar worden herzien. Het accent moet daarbij liggen op veranderingen in interne en externe factoren die op de instelling van invloed zijn.

10. De bestuurs- en toezichtfuncties van het leidinggevend orgaan

1. Er dient te worden gezorgd voor een effectieve wisselwerking tussen bestuurs- en toezichtfuncties in het leidinggevend orgaan.

Toelichting

De lidstaten maken gewoonlijk gebruik van twee **governancestructuren** – een monistisch of dualistisch bestuursmodel. In beide structuren vervullen het leidinggevend orgaan in zijn bestuursfunctie en het leidinggevend orgaan in zijn toezichtfunctie elk hun eigen rol in de leiding van de instelling, rechtstreeks of via comités.

Vanuit de bestuursfunctie worden de lijnen uitgezet voor de instelling, wordt ervoor gezorgd dat de strategie daadwerkelijk wordt uitgevoerd, en is men verantwoordelijk voor de dagelijkse activiteiten van de instelling.

Vanuit de toezichtfunctie wordt toegezien op bestuurders en aan hen advies verstrekt. Vanuit de rol van toezichthouder levert men een constructieve bijdrage aan de strategie van een instelling; er wordt toegezien op de werkzaamheden van het bestuur en op de verwezenlijking van overeengekomen doelstellingen. Voorts worden de integriteit van de financiële informatie, doeltreffend risicobeheer en interne controles gewaarborgd.

Er moet een goede wisselwerking zijn tussen de toezichthouders en bestuurders van een instelling om goed bestuur te bewerkstelligen, de overeengekomen strategie uit te voeren en in het bijzonder de risico's te beheersen waar de instelling mee te maken heeft. Er kunnen grote verschillen bestaan tussen de wet- en regelgevingskaders van landen, maar dat mag geen beletsel vormen voor een doeltreffende wisselingwerking tussen de bestuurs- en toezichtfuncties, ongeacht of het leidinggevend orgaan uit één of meerdere organen bestaat.

2. Het leidinggevend orgaan in zijn toezichtfunctie moet:

a. gereed en in staat zijn om voorstellen, toelichtingen en informatie van leden van het leidinggevend orgaan in zijn bestuursfunctie op de proef te stellen en kritisch te evalueren;

b. erop toezien dat de strategie, de risicotolerantie/-bereidheid en het beleid van de instelling consistent worden toegepast en dat de prestatienormen worden gehandhaafd in overeenstemming met de financiële belangen en solvabiliteit op de lange termijn; en

c. op basis van deze normen toezicht houden op de leden van het leidinggevend orgaan in zijn bestuursfunctie bij de uitoefening van hun taken.

3. Het leidinggevend orgaan in zijn bestuursfunctie moet de bedrijfsvoering en risicostrategieën coördineren en op gezette tijden de uitvoering van deze strategieën bespreken met het leidinggevend orgaan in zijn toezichtfunctie.
4. Vanuit beide functies moeten voldoende gegevens aan elkaar worden verstrekt. Het leidinggevend orgaan in zijn bestuursfunctie moet regelmatig, en zo nodig onverwijld, het leidinggevend orgaan in zijn toezichtfunctie uitgebreide informatie verstrekken die van belang is voor de beoordeling van de situatie, het bestuur van de instelling en het behoud van haar financiële zekerheid.

B.2 De samenstelling en het functioneren van het leidinggevend orgaan

11. De samenstelling, benoeming en opvolging binnen het leidinggevend orgaan

1. Het leidinggevend orgaan dient een adequaat aantal leden en een passende samenstelling te hebben. Het leidinggevend orgaan dient een beleid te hebben voor het kiezen van, toezien op en het plannen van de opvolging van zijn leden.
2. Een instelling moet de omvang en samenstelling van haar leidinggevend orgaan afstemmen op haar eigen omvang en samenstelling en op de aard en reikwijdte van haar activiteiten. Bij de leden van een gekozen leidinggevend orgaan moet voldoende gezamenlijke expertise aanwezig zijn.
3. Het leidinggevend orgaan moet geschikte en ervaren kandidaten identificeren en selecteren en zorgen voor een opvolgingsplan waarin naar behoren rekening wordt gehouden met eventuele andere wettelijke vereisten inzake samenstelling, benoeming en opvolging.
4. Het leidinggevend orgaan moet zorgen dat een instelling beleid heeft voor het selecteren van nieuwe leden en de herbenoeming van bestaande leden. Dit beleid moet voorzien in een omschrijving van de nodige competenties en vaardigheden om voldoende expertise te waarborgen.
5. Leden van het leidinggevend orgaan moeten voor een passende termijn worden benoemd. Herbenoemingen moeten gebaseerd zijn op het hiervoor omschreven

profiel en mogen alleen geschieden na een weloverwegen beoordeling van de prestaties van het lid gedurende zijn/haar zittingstermijn.

6. Bij het maken van een opvolgingsplan voor zijn leden moet het leidinggevend orgaan rekening houden met het aflopen van de contracten van zijn leden om, voor zover mogelijk, te voorkomen dat te veel leden tegelijkertijd moeten worden vervangen.

12. Toewijding, onafhankelijkheid en beheer van belangenconflicten in het leidinggevend orgaan

1. De leden van het leidinggevend orgaan dienen zich actief voor de bedrijfsactiviteiten van de instelling in te zetten en in staat te zijn hun eigen oordeelkundige, objectieve en onafhankelijke besluiten te nemen en afwegingen te maken.
2. Leden van een leidinggevend orgaan moeten worden geselecteerd op voldoende expertise en onafhankelijkheid. Een instelling moet ervoor zorgen dat de leden in staat zijn om met voldoende tijd en inzet zich doeltreffend van hun verantwoordelijkheden te kwijten.
3. De leden van het leidinggevend orgaan dienen slechts een beperkt aantal mandaten te vervullen of andere tijdrovende beroepsmatige activiteiten te verrichten. Bovendien moeten de leden hun beroepsmatige nevenactiviteiten (bijv. mandaten in andere ondernemingen) bij de instelling aanmelden. Omdat de voorzitter meer taken en verantwoordelijkheden heeft, wordt van hem/haar extra inzet verwacht.
4. Voor alle leden moet schriftelijk worden aangegeven hoeveel tijd er naar verwachting ten minste aan de werkzaamheden zal worden besteed. Indien wordt overwogen een nieuw lid te benoemen of men wordt ingelicht over een nieuw mandaat van een bestaand lid, moeten de leden van het leidinggevend orgaan de kandidaat vragen hoe hij/zij denkt voldoende tijd vrij te maken voor de uitoefening van haar verantwoordelijkheden jegens de instelling. Een bijeenkomst van de leden van het leidinggevend orgaan in zijn toezichtfunctie moet worden bekendgemaakt. Een instelling moet ook de openbaarmaking overwegen van lange perioden waarin leden van het leidinggevend orgaan in zijn toezichtfunctie afwezig zijn.
5. Van leden van het leidinggevend orgaan wordt verlangd dat zij objectief, kritisch en onafhankelijk kunnen optreden. Om de mogelijkheid tot het vellen van objectieve en onafhankelijke oordelen te vergroten is het zaak om leden te werven uit een voldoende brede groep van kandidaten en om over een voldoende aantal niet-uitvoerende leden te beschikken.

Toelichting

Dat de bestuurs- en toezichtfunctie binnen het leidinggevend orgaan formeel van elkaar gescheiden zijn, doet niets af aan de noodzaak dat de objectiviteit en onafhankelijkheid van het leidinggevend orgaan in zijn toezichtfunctie wordt gegarandeerd door een passende keuze van onafhankelijke leden.

6. Het leidinggevend orgaan moet op schrift gesteld beleid hebben inzake het beheer van belangenconflicten voor zijn leden. Dit beleid moet het volgende bepalen:

   a. Het is de taak van een lid om belangenconflicten door nevenfuncties die niet zijn aangemeld bij en goedgekeurd door het leidinggevend orgaan te voorkomen en om, ingeval ze toch bestaan, daar op een passende manier mee om te gaan.

   b. De leden moeten een herzienings- of goedkeuringsprocedure doorlopen alvorens bepaalde activiteiten te ontplooien (zoals zitting nemen in een ander leidinggevend orgaan) om te voorkomen dat dergelijke nevenactiviteiten zorgen voor een belangenconflict.

   c. Het is de taak van een lid om de instelling in te lichten over eender welke aangelegenheid die kan leiden of heeft geleid tot een belangenconflict.

   d. Het is de verantwoordelijkheid van een lid zich te onthouden van deelname aan de besluitvorming over of stemming inzake aangelegenheden die belangenconflicten met zich kunnen brengen, of wanneer de objectiviteit of het vermogen zijn/haar taken naar behoren uit te oefenen anderszins in het geding kan komen.

   e. Er moet worden voorzien in adequate procedures voor transacties met betrokken partijen die op "arms-length" basis plaatsvinden.

   f. De wijze waarop het leidinggevend orgaan zou optreden bij niet-naleving van het beleid, moet worden aangegeven.

13. Kwalificaties binnen het leidinggevend orgaan

1. Leden van het leidinggevend orgaan dienen voor hun posities gekwalificeerd te zijn en te blijven door middel van opleiding en duidelijk inzicht te hebben in de governanceregelingen van de instelling en de rol die zij daarin vervullen.
2. De leden van het leidinggevend orgaan, zowel individueel als collectief, moeten beschikken over de benodigde expertise, ervaring, competenties, inzichten en persoonlijke kwaliteiten, met inbegrip van professionele deskundigheid en persoonlijke integriteit, om hun taken naar behoren uit te voeren.
3. De leden van het leidinggevend orgaan moeten actuele kennis hebben van de bedrijfsactiviteiten die de instelling ontplooit op een niveau dat evenredig is aan

hun verantwoordelijkheden. Zij moeten in dit verband voldoende inzicht hebben in gebieden waarvoor zij weliswaar geen rechtstreekse verantwoordelijk dragen, maar collectief verantwoording verschuldigd zijn.

4. In collectief verband moeten zij volledig inzicht hebben in de aard van de bedrijfsvoering en de bijbehorende risico's. Daarnaast moeten zij beschikken over de juiste expertise en ervaring voor elk van de materiële activiteiten die de instelling wenst te ontplooien om mogelijk te maken dat governance en toezicht op doeltreffende wijze geschiedt.
5. Een instelling moet voorzien in een deugdelijke procedure die moet waarborgen dat de leden van het leidinggevend orgaan, zowel individueel als collectief, over toereikende kwalificaties beschikken.
6. De leden van het leidinggevend orgaan moeten nieuwe kennis en vaardigheden opdoen en hun bestaande kennis en vaardigheden behouden en verdiepen om zich te kwijten van hun verantwoordelijkheden. Instellingen moeten ervoor zorgen dat de leden toegang hebben tot op maat gesneden opleidingsprogramma's die rekening moeten houden met eventuele hiaten in het kennisprofiel waar de instelling om vraagt en met de actuele kennis van de leden. Aandachtspunten in dit verband kunnen risicobeheerinstrumenten en -modellen van de instelling zijn, nieuwe ontwikkelingen, veranderingen in de organisatie, complexe producten, nieuwe producten of markten en fusies. Er moet ook voorzien worden in opleiding op zakelijke gebieden die niet onder de rechtstreekse verantwoordelijkheid van afzonderlijke leden vallen. Het leidinggevend orgaan moet voldoende tijd, financiële middelen en andere hulpbronnen aan opleiding toewijzen.

14. De organisatie en het functioneren van het leidinggevend orgaan

1. Het leidinggevend orgaan dient voor haar eigen organisatie en functioneren gepaste interne-governancepraktijken vast te stellen en te voorzien in de middelen die waarborgen dat deze praktijken worden nagevolgd en periodiek ter verbetering worden herzien.

Toelichting
Deugdelijke interne-governancepraktijken en -procedures voor het leidinggevend orgaan geven zowel intern als extern belangrijke signalen af over het beleid en de doelstellingen van de instelling op het vlak van governance. De praktijken en procedures betreffen onder andere de vergaderfrequentie en de bijbehorende werkprocedures en notulen alsmede de rol van de voorzitter en de inzet van comités.

2. Het leidinggevend orgaan dient regelmatig bijeen te komen om zijn verantwoordelijkheden adequaat en doeltreffend uit te oefenen. De leden van het leidinggevend orgaan moeten voldoende tijd vrijmaken ter voorbereiding op

de vergadering. Deze voorbereiding omvat de opstelling van een agenda. De notulen moeten de agendapunten bevatten en duidelijk vermelden welke besluiten genomen zijn en welke maatregelen zijn afgesproken. Deze praktijken en procedures moeten samen met de rechten, verantwoordelijkheden en kernactiviteiten van het leidinggevend orgaan op schrift worden gesteld en periodiek door dit orgaan aan een herziening worden onderworpen.

Het leidinggevend orgaan beoordelen op zijn functioneren

3. Het leidinggevend orgaan moet op gezette tijden een beoordeling maken van de individuele en collectieve efficiëntie en effectiviteit van zijn activiteiten, zijn praktijken en procedures op het gebied van governance, en van het functioneren van de comités. Voor de beoordeling kunnen externe facilitators worden ingezet.

De rol van de voorzitter van het leidinggevend orgaan

4. De voorzitter moet ervoor zorgen dat besluiten van het leidinggevend orgaan op een deugdelijke basis en met goede kennis van zaken worden genomen. Hij of zij moet een open en kritische discussie aanmoedigen en bevorderen en ervoor zorgen dat afwijkende meningen in het besluitvormingsproces kunnen worden geuit en bespreekbaar zijn.

Toelichting

De voorzitter speelt een cruciale rol in het goede functioneren van het leidinggevend orgaan. Hij of zij treedt op als leider van het leidinggevend orgaan en is er verantwoordelijk voor dat het over de hele linie doeltreffend functioneert.

5. In een monistisch systeem dient het voorzitterschap van het leidinggevend orgaan en de functie van chief executive officer van een instelling niet door één persoon te worden bekleed. Is het voorzitterschap van het leidinggevend orgaan en de CEO-functie in de instelling toch verenigd in één persoon, dan moet de instelling maatregelen hebben ingevoerd waarmee mogelijke schade aan het systeem van "checks and balances" zo veel mogelijk wordt beperkt.

Toelichting

In het kader van wederzijdse controle en evenwicht zou het leidinggevend orgaan in zijn toezichtfunctie bijvoorbeeld plaats kunnen bieden voor een gezaghebbend en onafhankelijk senior lid of iemand in een vergelijkbare positie.

Gespecialiseerde comités van het leidinggevend orgaan

6. Het leidinggevend orgaan in zijn toezichtfunctie moet overwegen gespecialiseerde comités op te richten, rekening houdend met de omvang en complexiteit van de instelling, waar leden van het leidinggevend orgaan zitting in nemen (bij bepaalde onderwerpen kunnen andere personen worden uitgenodigd die deskundigheid en advies ter zake kunnen inbrengen). Voorbeelden van gespecialiseerde comités zijn een accountantscomité, een risicocomité, een beloningscomité, een benoemingscomité of comité personele middelen en/of een comité op het gebied van governance, ethiek of naleving.

Toelichting
Het delegeren van taken aan dergelijke comités ontslaat het leidinggevend orgaan in zijn toezichtfunctie geenszins van zijn verplichting om zich collectief te kwijten van zijn taken en verantwoordelijkheden, maar het kan bijdragen aan de ondersteuning van de werkzaamheden op specifieke gebieden indien het de ontwikkeling en uitvoering van praktijken en besluiten op het gebied van good governance bevordert.

7. Een gespecialiseerd comité moet gekenmerkt zijn door een optimale mix van deskundigheid, competenties en ervaring en de combinatie daarvan moet haar in staat stellen de relevante thema's volledig te doorgronden, objectief te evalueren en er met een frisse blik naar te kijken. Een voldoende aantal onafhankelijke leden moet zitting hebben in een comité. Elk comité moet een schriftelijk mandaat hebben (waarin ook haar werkingssfeer is vastgelegd) van het leidinggevend orgaan in zijn toezichtfunctie alsmede vastgestelde werkwijzen. In een comité kan een systeem van roterend voorzitterschap en lidmaatschap worden toegepast.

Toelichting
Een roterend lidmaatschap en voorzitterschap helpt ongepaste machtsconcentraties te voorkomen en nieuwe perspectieven aan te boren.

8. De respectieve comitévoorzitters dienen regelmatig verslag uit te brengen bij het leidinggevend orgaan. Met het oog op samenhang en het vermijden van hiaten moet er een passende wisselwerking zijn tussen de gespecialiseerde comités. Dit kan worden bereikt door deel te nemen aan elkaars activiteiten. Zo zou de voorzitter van een gespecialiseerd comité ook zitting kunnen nemen in een ander gespecialiseerd comité.

Het accountantscomité

9. Een accountantscomité (of vergelijkbaar comité) moet onder andere de interne controle, interne audit en risicobeheersystemen controleren op doeltreffendheid; toezien op de externe accountants van de instelling;

aanbevelingen doen betreffende goedkeuring door het leidinggevend orgaan van de benoeming, de beloning en het ontslag van externe accountants; de frequentie en reikwijdte van de audit nazien en goedkeuren; accountantsrapporten beoordelen; en controleren of het leidinggevend orgaan in zijn bestuursfunctie tijdig de nodige correctieve maatregelen neemt om gebrekkige controles, niet-naleving van wetgeving, voorschriften en beleid, en andere door de accountants vastgestelde problemen aan te pakken. Daarnaast moet het accountantscomité toezien op de vaststelling door de instelling van de grondslagen voor de financiële verslaggeving.

Toelichting
Zie ook artikel 41 van Richtlijn 2006/43/EG betreffende de wettelijke controles van jaarrekeningen en geconsolideerde jaarrekeningen.

10. De voorzitter van het comité moet onafhankelijk zijn. Indien de voorzitter voorheen een bestuursfunctie in de instelling heeft bekleed, moet een redelijke termijn zijn verstreken voordat het voorzitterschap van het comité wordt aanvaard.
11. De leden van het accountantscomité als geheel moeten recente en relevante praktijkervaring hebben opgedaan op het gebied van de financiële markten, of vanwege in het verleden verrichte zakelijke activiteiten voldoende beroepservaring hebben verkregen die rechtstreeks verband houdt met de activiteiten op die markten. De voorzitter van het accountantscomité moet in ieder geval beschikken over specialistische kennis over en ervaring met de toepassing van boekhoudbeginselen en internecontroleprocessen.

Het risicocomité

12. Een risicocomité (of vergelijkbaar comité) moet het leidinggevend orgaan van advies dienen over de risicostrategie van de instelling en de algemene risicotolerantie/-bereidheid nu en in de toekomst. Ook moet zij toezien op de uitvoering van voornoemde strategie. Om het risicocomité doeltreffender te laten functioneren, moet zij regelmatig communiceren met de risicobeheerder en risicodirecteur van de instelling en moet zij, in voorkomend geval, toegang hebben tot extern deskundigenadvies, vooral in verband met voorgestelde strategische transacties, zoals fusies en overnames.

B.3 Kader voor gedragsregels

15. Ondernemingswaarden en gedragscode

1. Het leidinggevend orgaan dient hoge ethische en beroepsnormen te ontwikkelen en te bevorderen.

Toelichting

Reputatieschade kan leiden tot moeilijk terug te winnen verlies aan vertrouwen en kan gevolgen hebben voor de gehele markt.

De instelling van passende normen (bijv. een gedragscode) voor professioneel en verantwoordelijk gedrag voor de hele instelling moet helpen de risico's waaraan zij is blootgesteld, te beperken. Vooral de operationele en reputatierisico's zullen kleiner worden als deze normen hoge prioriteit krijgen en naar behoren worden nageleefd.

2. Het leidinggevend orgaan moet helder beleid voeren over hoe aan deze normen moet worden voldaan.
3. Deze normen moeten voortdurend worden gecontroleerd op toepassing en naleving en aan het leidinggevend orgaan moet regelmatig verslag worden uitgebracht over de resultaten.

16. Belangenconflicten op instellingsniveau

1. Het leidinggevend orgaan dient een doeltreffend beleid voor het identificeren van bestaande en mogelijke belangenconflicten vast te stellen, uit te voeren en te handhaven. Belangenconflicten door nevenfuncties die zijn aangemeld bij en goedgekeurd door het leidinggevend orgaan, dienen naar behoren te worden beheerd.
2. Een beleidsdocument moet voorzien in de identificatie van betrekkingen, diensten, activiteiten of transacties waarbij belangenconflicten kunnen ontstaan en moet aangeven hoe deze conflicten moeten worden beheerd. Dit beleid moet van toepassing zijn op betrekkingen en transacties tussen verschillende klanten van een instelling en die tussen een instelling en:
   a. haar klanten (als gevolg van het zakelijk model en/of de verschillende door de instellingen verleende diensten en verrichte activiteiten);
   b. haar aandeelhouders;
   c. de leden van het leidinggevend orgaan;
   d. haar personeel;
   e. belangrijke leveranciers of zakenpartners; en
   f. overige betrokken partijen (haar moederonderneming of dochterondernemingen).
3. Een moederonderneming moet rekening houden met de belangen van al haar dochterondernemingen en deze met elkaar in evenwicht brengen. Ook moet zij nadenken over hoe die belangen bijdragen aan de algemene langetermijndoelstelling en -belangen van de groep als geheel.

4. Het beleid inzake belangenconflicten moet maatregelen bevatten die worden vastgesteld om belangenconflicten te voorkomen of te beheren. Het kan daarbij gaan om procedures en maatregelen:

   a. om taken adequaat te scheiden, waarbij conflictueuze activiteiten binnen de keten van transacties of diensten alsmede toezichts- en rapportageverantwoordelijkheden in verband met conflictueuze activiteiten aan verschillende personen worden toegewezen;

   b. om informatiebarrières in te stellen zoals een fysieke afscheiding van bepaalde afdelingen; en

   c. om te voorkomen dat personen die ook buiten de instelling actief zijn, ongepaste invloed verkrijgen binnen de instelling met betrekking tot deze activiteiten.

17. Interne meldingsprocedures

1. Het leidinggevend orgaan dient passende interne meldingsprocedures in te voeren op basis waarvan het personeel vermeende misstanden op het gebied van interne governance kan melden.
2. Een instelling moet passende interne meldingsprocedures vaststellen die het personeel kan gebruiken om de aandacht te vestigen op wezenlijke en gerechtvaardigde punten van zorg in verband met interne governance. Deze procedures moeten voorzien in een vertrouwelijke behandeling van dergelijke meldingen. Om belangenconflicten te voorkomen moet het mogelijk zijn deze punten van zorg buiten de reguliere rapportagelijnen aan te melden (bijv. via de compliance officer, de interne auditor of een interne klokkenluidersprocedure). De alarmprocedure moet voor alle medewerkers in een instelling toegankelijk zijn. Informatie die door een medewerker via de alarmprocedure wordt verstrekt, moet, indien relevant, beschikbaar worden gemaakt voor het leidinggevend orgaan.

Toelichting
In sommige lidstaten beschikt het personeel naast de interne meldingsprocedure in een instelling ook over de mogelijkheid om vermeende misstanden van dit type bij de toezichthoudende autoriteit aan te kaarten.

B.4 Het uitbestedings- en beloningsbeleid

18. Uitbesteding

1. Het uitbestedingsbeleid van een instelling dient door het leidinggevend orgaan te worden goedgekeurd en regelmatig te worden herzien.

Toelichting

Het onderhavige richtsnoer beperkt zich tot het uitbestedingsbeleid. Voor specifieke uitbestedingsaspecten wordt verwezen naar de uitbestedingsrichtsnoeren van de CEBT (*CEBS Guidelines on Outsourcing*), die te vinden zijn op de website van de EBA.

Van instellingen wordt verwacht dat zij aan beide groepen richtsnoeren voldoen. Wanneer bepalingen met elkaar in tegenspraak zijn, dienen de meer specifieke richtsnoeren van de CEBT voorrang te krijgen. Ingeval een aangelegenheid niet in de CEBT-richtsnoeren wordt behandeld, dient het algemene beginsel van de onderhavige richtsnoeren te worden toegepast.

2. Het uitbestedingsbeleid moet rekening houden met het uitbestedingseffect op bedrijfsactiviteiten van een instelling en de daarmee gepaard gaande risico's (operationele, reputatie- en concentratierisico's). Het beleid moet voorschrijven dat de rapportage- en controleregelingen van het begin tot het einde van een uitbestedingscontract worden uitgevoerd (waaronder de uitwerking van het zakelijk motief voor een uitbesteding, het aangaan van een uitbestedingscontract, de uitvoering van het contract tot aan de vervaldatum, noodplannen en exitstrategieën). Het beleid moet regelmatig worden herzien en bijgewerkt, en aanpassingen moeten tijdig worden verricht.
3. Een instelling blijft volledig verantwoordelijk voor alle uitbestede diensten en activiteiten en hieruit voortvloeiende managementbesluiten. In het beleidsdocument inzake uitbesteding moet dus duidelijk worden gemaakt dat een uitbesteding de instelling niet ontslaat van haar wettelijke verplichtingen en verantwoordelijkheden jegens haar klanten.
4. Vermeld moet worden dat uitbestedingsregelingen een doelmatig toezicht ter plekke en op afstand niet mogen belemmeren en niet mogen indruisen tegen beperkingen inzake toezicht op het gebied van diensten en activiteiten. Het beleid moet ook van toepassing zijn op interne uitbesteding (bijv. door een van de groep te onderscheiden juridische eenheid) en rekening houden met relevante specifieke omstandigheden binnen de groep.

19. Beheer van het beloningsbeleid

1. Het leidinggevend orgaan van een instelling dient het uiteindelijke toezicht op het beloningsbeleid uit te oefenen.

Toelichting

De onderhavige richtsnoeren voorzien in het *algemene* kader dat van toepassing is op het beheer van het beloningsbeleid. *Specifieke* aspecten op dit gebied worden behandeld in de CEBT-richtsnoeren inzake beloningsbeleid van

december 2010. Van instellingen wordt verwacht dat zij aan beide groepen richtsnoeren voldoen.

2. Het leidinggevend orgaan in zijn toezichtfunctie moet de beginselen van het algehele beloningsbeleid voor zijn instelling handhaven, goedkeuren en monitoren. De procedures van de instelling voor de vaststelling van de beloning moeten helder, goed gedocumenteerd en intern transparant zijn.
3. Het leidinggevend orgaan is algemeen verantwoordelijk voor het algehele beloningsbeleid en de beoordeling ervan, maar ook de controlefuncties moeten er op adequate wijze bij betrokken worden. De leden van het leidinggevend orgaan en andere personeelsleden die bij het ontwerp en de uitvoering van het beloningsbeleid betrokken zijn, dienen te beschikken over relevante expertise en moeten tot een onafhankelijk oordeel kunnen komen over de geschiktheid van het beloningsbeleid en de gevolgen ervan voor het risicobeheer.
4. Daarnaast moet het beloningsbeleid gericht zijn op het voorkomen van belangenconflicten. Het leidinggevend orgaan in zijn bestuursfunctie moet niet zijn eigen beloning kunnen vaststellen; hiervoor kan bijvoorbeeld een onafhankelijk beloningscomité worden ingeschakeld. Een bedrijfseenheid moet niet de beloning voor haar eigen controlefuncties kunnen vaststellen.
5. Het leidinggevend orgaan moet toezien op de uitvoering van het beloningsbeleid om te waarborgen dat het beleid werkt zoals bedoeld. Voorts moet de uitvoering van het beloningsbeleid aan een centrale en onafhankelijke toetsing worden onderworpen.

C. Risicobeheer

20. Risicocultuur

1. Een instelling ontwikkelt een geïntegreerde en organisatiebrede risicocultuur die berust op volledig inzicht in de risico's die gelopen worden en hoe deze risico's te beheren met inachtneming van haar risicotolerantie/-bereidheid.

Toelichting

Aangezien de bedrijfsactiviteiten van een instelling in hoofdzaak neerkomen op het nemen van risico's, is het essentieel dat risico's passend worden beheerd. Een gezonde en consistente risicocultuur binnen de gehele instelling is een belangrijk onderdeel van doeltreffend risicobeheer.

2. De risicocultuur van een instelling moet worden ontwikkeld aan de hand van beleid, voorbeelden, communicatie en opleiding van medewerkers over hun verantwoordelijkheden als het om risico's gaat.

3. Elk lid van de organisatie moet zijn of haar verantwoordelijkheden in verband met risicobeheer volledig kennen. Risicobeheer is niet uitsluitend een taak van risicospecialisten of werknemers in een controlefunctie. De verantwoordelijkheid voor het dagelijks risicobeheer berust in hoofdzaak bij de bedrijfseenheden, waarbij het leidinggevend orgaan toezicht uitoefent. Daarbij geldt dat de risico's overeenkomstig de risicotolerantie/-bereidheid van de instelling en het beleid, de procedures en de controles in dit verband moeten worden beheerd.
4. Een instelling moet beschikken over een holistisch kader voor risicobeheer dat zich uitstrekt over alle bedrijfs-, ondersteunings- en controle-eenheden, waarin de economische realiteit van haar risicoblootstellingen ten volle wordt erkend, en alle relevante risico's omvat (financiële en niet-financiële risico's, risico's zowel binnen als buiten de balans, en al dan niet van toeval afhankelijke of contractuele risico's). De werkingssfeer ervan moet zich niet beperken tot krediet-, markt-, liquiditeits- en operationele risico's; ook concentratie-, reputatie-, nalevings- en strategische risico's moeten eronder vallen.
5. Het kader voor risicobeheer moet de instelling in staat stellen geïnformeerde besluiten te nemen, op basis van informatie die is afgeleid uit de identificatie, meting, beoordeling en monitoring van risico's. De evaluatie van risico's moet geschieden van bovenaf en van onderop, door de gehele beheerketen heen en voor alle bedrijfsonderdelen, waarbij gebruik wordt gemaakt van consistente terminologie en onderling verenigbare methodieken binnen de gehele instelling en haar groep.
6. Het kader voor risicobeheer moet worden onderworpen aan onafhankelijk intern en extern onderzoek en regelmatig opnieuw worden getoetst aan de risicotolerantie/-bereidheid van de instelling, waarbij informatie wordt meegewogen afkomstig van de risicobeheerder en, waar van toepassing, het risicocomité. In aanmerking te nemen factoren zijn interne en externe ontwikkelingen, balans- en inkomstengroei, toenemende complexiteit van de bedrijfsactiviteiten van de instelling, het risicoprofiel en de werkstructuur, geografische expansie, fusies en overnames en de introductie van nieuwe producten of business lines.

21. Afstemming van beloningen op het risicoprofiel

1. Het beloningsbeleid van een instelling strookt met haar risicoprofiel en bevordert een deugdelijk en doeltreffend risicobeheer.

Toelichting

De onderhavige richtsnoeren bieden het *algemene* kader dat van toepassing is op de afstemming van het beloningsbeleid op het risicoprofiel van een instelling. *Specifieke* aspecten van het beloningsbeleid worden behandeld in de CEBT-richtsnoeren inzake beloningsbeleid van december 2010. Van instellingen wordt verwacht dat zij aan beide groepen richtsnoeren voldoen.

2. Het algehele beloningsbeleid van een instelling moet stroken met haar waarden, bedrijfsstrategie, risicotolerantie/-bereidheid en langetermijnbelangen. Dit beleid mag het nemen van buitensporige risico's niet aanmoedigen. Gegarandeerde variabele beloningen of ontslagvergoedingen waarbij falen wordt beloond stroken niet met een degelijke risicobeheersing of het beginsel van prestatiebeloning en moeten, als algemene regel, worden verboden.
3. Voor medewerkers wier beroepsactiviteiten het risicoprofiel van een instelling materieel beïnvloeden (bijv. leden van het leidinggevend orgaan, hogere leidinggevenden en risiconemende functies in bedrijfsonderdelen, medewerkers verantwoordelijk voor interne controle alsmede alle werknemers wier totale beloning hen in dezelfde beloningsschaal plaatst als werknemers in hogere leidinggevende en risiconemende functies), moet het beloningsbeleid voorzien in specifieke regelingen die verzekeren dat hun beloning is afgestemd op een degelijk en doeltreffend risicobeheer.
4. Werknemers in controlefuncties moeten gepast worden beloond op grond van hun doelen en prestaties en niet in verhouding tot de prestaties van de bedrijfseenheden die zij controleren.
5. Is de beloning op prestaties gebaseerd, dan moet de beloning plaatsvinden op grond van een combinatie van individuele en collectieve prestaties. Bij het bepalen van individuele prestaties moeten andere dan financiële prestaties in aanmerking worden genomen. Prestatiemetingen voor het toekennen van bonussen moeten correcties omvatten aangebracht voor alle soorten risico's alsmede de kosten van het gebruikte kapitaal en de vereiste liquiditeit.
6. De bonus dient in een evenredige verhouding te staan tot het basissalaris. Een aanzienlijke bonus moet niet worden betaald als contant voorschot maar moet een flexibel en uitgesteld deel bevatten dat voor risico gecorrigeerd is. Wat betreft het tijdstip waarop de bonus wordt uitbetaald, moet rekening worden gehouden met de onderliggende risicoperformance.

22. Het kader voor risicobeheer

1. Het kader voor risicobeheer van een instelling omvat beleid, procedures, limieten en controles die voorzien in adequate, tijdige en permanente identificatie, meting of beoordeling, monitoring, verkleining en rapportage van de risico's die zij loopt op het niveau van de instelling en de bedrijfsonderdelen.

2. Dit kader moet specifieke sturing geven aan de uitvoering van de strategieën van de instelling. In dit verband moeten zo nodig interne limieten worden vastgesteld en gehandhaafd die stroken met de risicotolerantie/-bereidheid, het deugdelijk functioneren, de financiële kracht en de strategische doelstellingen van de instelling. Het risicoprofiel van een instelling (d.w.z. het geheel van haar werkelijke en potentiële risicoblootstellingen) moet binnen deze limieten worden gehouden. Het kader voor risicobeheer moet waarborgen dat bij overschrijding van de limieten terstond actie wordt ondernomen en zorg wordt gedragen voor een passende follow-up.
3. Bij de identificatie en meting van risico's moet een instelling instrumenten ontwikkelen voor toekomstgerichte prognoses en ramingen, gebaseerd op resultaten uit het verleden, in aanvulling op werkzaamheden aan heersende blootstellingen. Deze instrumenten moeten de aggregatie van risicoblootstellingen bij alle business lines mogelijk maken en het identificeren van risicoconcentraties ondersteunen.
4. Met instrumenten voor toekomstgerichte prognoses (zoals scenarioanalyses en stresstests) moeten potentiële risicoblootstellingen onder een reeks ongunstige omstandigheden worden geïdentificeerd; instrumenten voor ramingen die zijn gebaseerd op resultaten uit het verleden, moeten een bijdrage leveren aan de toetsing van het werkelijke risicoprofiel aan de risicotolerantie/-bereidheid van de instelling en haar kader voor risicobeheer en voorts input leveren voor eventuele aanpassingen.

Toelichting
De richtsnoeren voor stresstests zijn te vinden op de website van de EBA.

5. De uiteindelijke verantwoordelijkheid voor risicobeoordeling berust uitsluitend bij de instelling, die haar risico's dus kritisch moet evalueren en zich niet uitsluitend moet verlaten op externe beoordelingen.

Toelichting
Zo moet een instelling een ingekocht risicomodel valideren en het vervolgens afstemmen op individuele omstandigheden om te zorgen voor een accurate en uitvoerige vastlegging en analyse van risico's. Externe risicobeoordelingen (met inbegrip van externe kredietratings of elders ingekochte risicomodellen) kunnen dienstig zijn bij het maken van een bredere risico-inschatting. Instellingen moeten zich bewust zijn van de draagwijdte van dergelijke beoordelingen.

6. Besluiten die bepalend zijn voor het niveau van de genomen risico's moeten daarom niet alleen gebaseerd zijn op kwantitatieve informatie of modeloutputs maar ook rekening houden met de praktische en conceptuele beperkingen van meeteenheden en modellen waarbij een kwalitatieve benadering wordt

gehanteerd (en gebruik wordt gemaakt van oordelen van deskundigen en kritische analysen). Op belangrijke tendensen en gegevens in de macro-economische omgeving moet uitdrukkelijk worden ingegaan om hun potentiële effect op blootstellingen en portefeuilles in kaart te brengen. Dit soort beoordelingen moet formeel worden geïntegreerd in materiële risicobesluiten.

Toelichting

Een instelling moet bedenken dat de resultaten van toekomstgerichte kwantitatieve beoordelingen en 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. uitsluiting van bepaalde relevante risico's) dan het gevolg van een excellente strategie of uitvoering van de zijde van de instelling.

7. Er moeten mechanismen voor regelmatige en transparante rapportage worden ingevoerd zodat het leidinggevend orgaan en alle relevante eenheden in een instellingen op tijd accurate, beknopte, begrijpelijke en zinvolle rapporten ontvangen en zij belangrijke gegevens kunnen uitwisselen over de identificatie, meting, beoordeling en monitoring van risico's. Het rapportagekader moet nauwkeurig omschreven en gedocumenteerd worden en door het leidinggevend orgaan worden goedgekeurd.
8. Als er een risicocomité is, moet deze regelmatig formele rapporten en informele kennisgevingen ontvangen van eventueel de risicobeheerder en risicodirecteur.

Toelichting

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

23. Nieuwe producten

1. Een instelling beschikt over een duidelijk gedocumenteerd beleid voor de goedkeuring van nieuwe producten. In dit beleid, dat door het leidinggevend orgaan wordt goedgekeurd, moet worden ingegaan op de ontwikkeling van nieuwe markten en significante veranderingen op bestaande markten.

2. Alle afwegingen moeten in dit beleid worden meegenomen alvorens nieuwe markten worden betreden, in nieuwe producten wordt gehandeld, een nieuwe dienst wordt gelanceerd of bestaande producten of diensten ingrijpend worden gewijzigd. In het beleid voor de goedkeuring van nieuwe producten moet een definitie worden gegeven van een nieuw product, een nieuwe markt of nieuwe bedrijfsactiviteiten. Deze definitie moet in de organisatie worden toegepast alsmede door de werknemers in interne functies die bij het besluitvormingsproces worden betrokken.
3. Dit beleid moet de grote thema's belichten die moeten worden aangepakt voordat een besluit genomen wordt. In dit verband moet het gaan om naleving van de voorschriften, prijsbepalingsmodellen, effecten op het risicoprofiel, kapitaaltoereikendheid en rentabiliteit, beschikbaarheid van adequate middelen voor front-, back- en middle-office en geschikte interne instrumenten en expertise om de gerelateerde risico's te begrijpen en te monitoren. Uit het besluit om een nieuwe activiteit te initiëren, moet duidelijk opgemaakt kunnen worden welke bedrijfseenheden en personen er verantwoordelijk voor zijn. Een nieuwe activiteit moet pas worden opgestart bij beschikbaarheid van voldoende hulpmiddelen om de risico's die eraan verbonden zijn te begrijpen en te beheersen.
4. De risicobeheerder moet betrokken worden bij de goedkeuring van nieuwe producten of bij ingrijpende wijzingen in bestaande producten. Zijn bijdrage moet onder andere bestaan uit een volledige en objectieve beoordeling van risico's die uit nieuwe activiteiten voortvloeien onder verschillende scenario's, van potentiële tekortkomingen in de kaders voor risicobeheer en interne controle, en van het vermogen van de instelling om nieuwe risico's doeltreffend te beheren. De risicobeheerder moet ook een duidelijk overzicht hebben van de uitrol van nieuwe producten (of van ingrijpende wijzigingen van bestaande producten) binnen alle verschillende business lines en portefeuilles. Voorts moet hij of zij bevoegd zijn om te verlangen dat wijzigingen van bestaande producten eerst behandeld worden in een formele procedure inzake het beleid voor de goedkeuring van nieuwe producten.

D. Interne controle

24. Het kader voor interne controle

1. Een instelling ontwikkelt en handhaaft een krachtig en coherent kader voor interne controle met specifieke onafhankelijke controlefuncties die door werknemers met de vereiste rang worden uitgeoefend.
2. Het kader voor interne controle in een instelling moet zorgen voor doeltreffende en efficiënte activiteiten, adequaat risicobeheer, behoedzame bedrijfsvoering, rapportage van betrouwbare financiële en niet-financiële gegevens – zowel intern als extern, en naleving van wet- en regelgeving, toezichtvereisten en de

interne voorschriften en besluiten van de instelling. Het kader voor interne controle moet zich uitstrekken over de gehele organisatie, ook over alle bedrijfs-, ondersteunings- en controle-eenheden. Het kader voor interne controle moet geschikt zijn voor de activiteiten van een instelling en voorzien in gedegen administratieve en boekhoudkundige procedures.

3. Voor de ontwikkeling van dit kader moet een instelling een duidelijke, transparante en gedocumenteerde besluitvormingsprocedure scheppen en zorgen voor een duidelijke toewijzing van verantwoordelijkheden en bevoegdheden om de naleving van interne voorschriften en besluiten te waarborgen. Om een krachtig kader voor interne controle binnen alle domeinen van de instelling ten uitvoer te leggen, moeten de bedrijfs- en ondersteuningseenheden allereerst verantwoordelijk worden gesteld voor de vaststelling en handhaving van het beleid en de procedures voor interne controle.
4. Een geschikt kader voor interne controle vereist tevens dat onafhankelijke werknemers in een controlefunctie nagaan of het beleid en de procedures worden gevolgd. Controlefuncties moeten een risicobeheer-, compliance- en auditfunctie omvatten.
5. Controlefuncties moeten op een passend hiërarchisch niveau zijn vastgesteld en werknemers in de betreffende functies moeten rechtstreeks rapporteren aan het leidinggevend orgaan. Zij moeten een onafhankelijke positie innemen tegenover de bedrijfs- en ondersteuningeenheden die zij monitoren en controleren, en organisatorisch van elkaar onafhankelijk zijn (aangezien zij verschillende functies uitoefenen). In minder complexe en kleinere instellingen kunnen taken van de risicobeheerder en compliance officer worden gecombineerd. De werknemers in een controlefunctie op het niveau van de groep moeten toezicht uitoefenen op de vervullers van deze functie bij dochterondernemingen.
6. Om als onafhankelijk te worden aangemerkt, moet een controlefunctie aan de volgende voorwaarden voldoen:

    a. werknemers in een onafhankelijke controlepositie verrichten geen taken die vallen onder de activiteiten die zij behoren te monitoren en controleren;

    b. de controlefunctie is organisatorisch gescheiden van de activiteiten die gemonitord en gecontroleerd moeten worden;

    c. de persoon die ter zake van de controlefunctie de hoogste positie bekleedt, is lager in rang dan een persoon die niet verantwoordelijk is voor het beheer van de activiteiten welke in het kader van de controlefunctie worden gemonitord en gecontroleerd. Deze persoon moet rechtstreeks rapporteren aan het leidinggevend orgaan en relevante comités en dient hun bijeenkomsten geregeld bij te wonen; en

    d. de beloning van personeel in een controlefunctie mag niet gekoppeld zijn aan de verrichting van activiteiten die vanuit de controlefunctie worden

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

7. Er moeten voldoende gekwalificeerde werknemers in een controlefunctie aanwezig zijn (in groepsondernemingen bij zowel de moeder- als dochterondernemingen). Het personeel moet op permanente basis gekwalificeerd zijn en passend worden opgeleid. Het moet daarnaast beschikken over geschikte datasystemen en ondersteuning en toegang hebben tot interne en externe informatie, nodig om hun verantwoordelijkheden na te komen.
8. Werknemers in controlefuncties moeten bij het leidinggevend orgaan regelmatig formeel verslag uitbrengen over grote vastgestelde gebreken. In deze verslagen moet terug te vinden zijn welke maatregelen zijn genomen naar aanleiding van eerdere bevindingen en, voor elk nieuw groot gebrek dat wordt geconstateerd, de daarmee gepaard gaande relevante risico's, een effectbeoordeling en aanbevelingen. Op basis van de conclusies van werknemers in een controlefunctie moet het leidinggevend orgaan tijdig en doeltreffend actie ondernemen om problemen te verhelpen.

25. De risicobeheerfunctie

1. Een instelling stelt een veelomvattende en onafhankelijke risicobeheerfunctie in.
2. Deze functie moet waarborgen dat elk groot risico voor de instelling door de desbetreffende eenheden van de instelling wordt geïdentificeerd en deugdelijk wordt beheerd, en dat bij het leidinggevend orgaan een holistisch perspectief op alle relevante risico's wordt ingediend. De werknemer in de risicobeheerfunctie, meer bepaald de risicobeheerder, moet belangrijke onafhankelijke informatie leveren alsmede analyses en deskundige oordelen over risicoblootstellingen. Daarnaast moet hij of zij advies uitbrengen over voorstellen en risicobeslissingen die zijn genomen door het leidinggevend orgaan en door de bedrijfs- en ondersteunende afdelingen waarin wordt uitgesproken of de beslissingen stroken met de risicotolerantie/-bereidheid van de instelling. Vanuit de risicobeheerfunctie kunnen voorstellen worden gedaan om het kader voor risicobeheer te verbeteren en mogelijkheden worden aangereikt voor het corrigeren van overtredingen van beleidsmaatregelen, procedures en limieten.
3. De risicobeheerfunctie dient organisatorisch centraal te staan en zodanig te zijn ingericht dat risicobeleid uitgevoerd en het kader voor risicobeheer gecontroleerd kan worden. Grote, complexe en doorontwikkelde instellingen kunnen overwegen om voor elke relevante business line een specifieke risicobeheerfunctie in te stellen. De instelling moet echter beschikken over een overkoepelende risicobeheerfunctie (met inbegrip van, waar nodig, een

risicobeheerfunctie bij de moederonderneming van een groep) van waaruit een holistisch perspectief op alle risico's wordt geboden.

4. De risicobeheerfunctie moet ten opzichte van de bedrijfs- en ondersteuningseenheden die worden gecontroleerd weliswaar een onafhankelijke, maar geen geïsoleerde positie innemen. De risicobeheerder moet beschikken over voldoende kennis van technieken en procedures inzake risicobeheer en van markten en producten. Wisselwerking tussen de operationele functies en de risicobeheerfunctie moet het gemakkelijker maken om te komen tot de beoogde situatie waarin alle werknemers van de instelling verantwoordelijkheid dragen voor risicobeheer.

26. De rol van de risicobeheerder

1. De risicobeheerder wordt in een vroeg stadium actief betrokken bij de uitwerking van de risicostrategie van een instelling en bij alle relevante beslissingen inzake risicobeheer. De risicobeheerder speelt een belangrijke rol bij de verwezenlijking van doeltreffende risicobeheerprocessen in de instelling.

De rol van de risicobeheerder bij de strategie en besluitvorming

2. De risicobeheerder moet het leidinggevend orgaan alle relevante risicogegevens verschaffen (bijv. door technische analyses over risicoblootstelling te verstrekken) op basis waarvan dit orgaan de risicotolerantie/-bereidheid van de instelling kan vaststellen.
3. De risicobeheerder moet ook de risicostrategie beoordelen, waaronder de voorgestelde streefcijfers van de bedrijfsafdelingen, en bij het leidinggevend orgaan advies uitbrengen alvorens een besluit genomen wordt. Streefcijfers, met inbegrip van kredietratings en het rendement van eigen vermogen, moeten geloofwaardig en samenhangend zijn.
4. De risicobeheerder moet verantwoordelijkheden voor de uitvoering van de strategie en het beleid op risicogebied van de instelling delen met alle bedrijfsafdelingen van de instelling. De bedrijfsafdelingen bepalen de relevante risicolimieten, maar de risicobeheerder moet er verantwoordelijkheid voor zijn dat de limieten stroken met de algehele risicotolerantie/-bereidheid van de instelling en dat er permanent op toegezien wordt dat er geen buitensporige risico's worden genomen.
5. De betrokkenheid van de risicobeheerder bij de besluitvorming moet ervoor zorgen dat risicobeoordelingen naar behoren in aanmerking worden genomen. De verantwoordingsplicht voor genomen beslissingen moet evenwel bij de bedrijfs- en ondersteuningseenheden en uiteindelijk bij het leidinggevend orgaan berusten.

De rol van de risicobeheerder bij transacties met betrokken partijen

6. De risicobeheerder moet waarborgen dat transacties met betrokken partijen worden getoetst en dat de werkelijke of potentiële risico's ervan voor de instelling geïdentificeerd en naar behoren beoordeeld worden.

De rol van de risicobeheerder in verband met de complexe juridische structuur

7. De risicobeheerder moet ernaar streven materiële risico's te identificeren die voortvloeien uit de complexe juridische structuur van de instelling.

Toelichting

Risico's kunnen een gebrek aan bestuurlijke transparantie zijn, operationele risico's als gevolg van onderling verweven en complexe financieringsstructuren, binnen de groep bestaande blootstellingen, "gevangen" zekerheden en het tegenpartijrisico.

De rol van de risicobeheerder bij wezenlijke veranderingen

8. De risicobeheerder moet evalueren in hoeverre wezenlijke veranderingen het vermogen van de groep beïnvloeden om zijn risicoprofiel te beheren en financiële middelen en kapitaal in te zetten onder normale en ongunstige omstandigheden.
9. Het is zaak de risicobeheerder te betrekken bij de evaluatie van het effect van wezenlijke veranderingen en buitengewone transacties op het risico voor de instelling en de groep als geheel voordat er besluiten over worden genomen.

Toelichting

Wezenlijke veranderingen of buitengewone transacties kunnen fusies en overnames zijn, het oprichten of de verkoop van dochterondernemingen of spv's, nieuwe producten, wijzigingen in systemen, het kader of de procedures voor risicobeheer en organisatorische veranderingen in de organisatie.

Zie de drie voormalige gemeenschappelijke richtsnoeren van de zogeheten "comités van niveau 3" – het Comité van Europese bankentoezichthouders (CEBT), het Comité van Europese toezichthouders op verzekeringen en bedrijfspensioenen (CETVB) en het Comité van Europese effectenregelgevers (CEER) van 2008 wat betreft de prudentiële beoordeling van verwervingen en vergrotingen van deelnemingen in de financiële sector, gepubliceerd op de website van de EBA. De risicobeheerder moet in een vroeg stadium actief worden betrokken bij het identificeren van belangrijke risico's (waaronder de mogelijke gevolgen van onvoldoende zorgvuldigheidsbetrachting waardoor risico's ná de fusie niet werden opgemerkt) in verband met wijzigingen in de structuur van de groep (zoals bij fusies en overnames) en moet zijn bevindingen rechtstreeks rapporteren aan het leidinggevend orgaan.

De rol van de risicobeheerder bij meting en beoordeling

10. De risicobeheerder moet ervoor zorgen dat internerisicometingen en -beoordelingen van een instelling een gepaste reeks scenario's bestrijken en berusten op voldoende voorzichtige aannames inzake afhankelijkheden en correlaties. Het gaat daarbij ook om kwalitatieve instellingsbrede opvattingen (en het deskundig oordeel) over de verhouding tussen risico en rendement en de bedrijfsomgeving waarin de instelling opereert.

De rol van de risicobeheerder bij het toezicht

11. De risicobeheerder moet waarborgen dat de bedrijfseenheden alle geïdentificeerde risico's doeltreffend kunnen monitoren. De risicobeheerder moet regelmatig toezien op het werkelijke risicoprofiel van de instelling en het toetsen aan de strategische doelstellingen en risicotolerantie/-bereidheid van de instelling teneinde het leidinggevend orgaan in staat te stellen om in zijn bestuursfunctie besluiten te nemen en in zijn toezichtfunctie zijn controlerende taak uit te oefenen.
12. De risicobeheerder moet tendensen analyseren en nieuwe of opkomende risico's als gevolg van veranderende omstandigheden en randvoorwaarden onderkennen. Hij of zij moet ook de werkelijke gevolgen van risico's vergelijken met de eerdere schattingen (back-testing) om de nauwkeurigheid en doelmatigheid van het risicobeheerproces te beoordelen en te verbeteren.
13. De risicobeheerder op groepsniveau moet toezien op de risico's die door de dochterondernemingen zijn aangegaan. Gevallen van strijdigheid met de goedgekeurde groepsstrategie moeten worden gerapporteerd aan het desbetreffende leidinggevend orgaan.

De rol van de risicobeheerder bij niet-goedgekeurde blootstellingen

14. De risicobeheerder moet naar behoren worden betrokken bij wijzigingen in de strategie van de instelling en de door haar geaccordeerde risicotolerantie/-bereidheid en limieten.
15. De risicobeheerder moet onafhankelijk een analyse maken van een schending of inbreuk (en van de oorzaak ervan). Daarnaast moet hij een juridische en economische analyse maken van de werkelijke kosten van beëindiging, beperking of afdekking van de blootstelling, afgezet tegen de potentiële kosten van handhaving ervan. De risicobeheerder moet de betrokken bedrijfseenheden in voorkomend geval informeren en mogelijke oplossingen aanbevelen.

Toelichting

De bestaande strategieën, risicotolerantie/-bereidheid of limieten kunnen botsen met nieuwe transacties, gewijzigde marktomstandigheden of een ontwikkeling in de strategie, het beleid of de procedures van de instelling als ze niet overeenkomstig worden aangepast.

16. De risicobeheerder moet een belangrijke rol spelen bij het waarborgen dat een besluit over zijn of haar aanbeveling op het relevante niveau wordt genomen, door de relevante bedrijfsafdelingen wordt nageleefd, en naar behoren aan het leidinggevend orgaan, het risicocomité en de bedrijfs- of ondersteuningseenheid wordt gerapporteerd.
17. Een instelling moet passende maatregelen nemen tegen interne en externe fraude en disciplinaire vergrijpen (inbreuk op interne procedures of overtreding van limieten).

Toelichting
Voor de toepassing van deze richtsnoeren wordt onder "fraude" zowel interne als externe fraude verstaan zoals omschreven in Richtlijn 2006/48/EG, bijlage X, deel 5. Hieronder vallen verliezen als gevolg van handelingen waarbij ten minste één interne partij betrokken is en waarmee wordt beoogd te frauderen, eigendommen te verduisteren of wet- en regelgeving of het ondernemingsbeleid te ontduiken of te omzeilen, met uitzondering van gebeurtenissen voortvloeiend uit ongelijkheid/discriminatie (interne fraude) en verliezen als gevolg van door een derde gestelde handelingen met de bedoeling te frauderen, eigendommen te verduisteren of de wet te ontduiken (externe fraude).

27. De risicodirecteur

1. Een instelling bekleedt een persoon, de risicodirecteur, met de exclusieve verantwoordelijkheid voor de risicobeheerfunctie en voor het toezicht binnen de gehele organisatie op het kader voor risicobeheer.
2. De risicodirecteur (of leidinggevende in een soortgelijke functie) is verantwoordelijk voor de verstrekking van uitvoerige en begrijpelijke informatie over risico's die het leidinggevend orgaan in staat stelt het algehele risicoprofiel van de instelling te begrijpen. Hetzelfde geldt voor de risicodirecteur van een moederonderneming met betrekking tot de groep als geheel.
3. De risicodirecteur moet beschikken over voldoende kennis, praktijkervaring, onafhankelijkheid en gezag op basis van anciënniteit om besluiten aan te vechten die van invloed zijn op de blootstelling van een onderneming aan risico's. Een instelling moet overwegen de risicodirecteur het recht te geven besluiten tegen te houden. De risicodirecteur en het leidinggevend orgaan of het relevante comité moeten rechtstreeks onderling kunnen communiceren over belangrijke risicoproblemen, waaronder ontwikkelingen die mogelijk niet stroken met de risicotolerantie/-bereidheid en risicostrategie van de instelling.
4. Indien een instelling de risicodirecteur het recht wil verlenen een vetorecht uit te spreken over beslissingen, moeten in haar risicobeleid de omstandigheden worden beschreven op grond waarvan de risicodirecteur hiertoe kan overgaan

alsmede de aard van de voorstellen (bijv. een kredietbeslissing of de vaststelling van een limiet). Het beleid moet een beschrijving geven van de escalatie- of beroepsprocedures en van de wijze waarop het leidinggevend orgaan wordt geïnformeerd.

5. Indien de kenmerken van een instelling – met name haar omvang, organisatie en de aard van de activiteiten – niet rechtvaardigen dat voor deze verantwoordelijkheid iemand speciaal wordt aangewezen, kan de functie worden vervuld door een andere hogere leidinggevende in de instelling, mits er geen sprake is van een belangenconflict.
6. De instelling moet beschikken over gedocumenteerde processen voor de toewijzing van de functie van risicodirecteur en voor de intrekking van zijn of haar verantwoordelijkheden. Eventuele vervanging van de risicodirecteur dient te geschieden met voorafgaande goedkeuring van het leidinggevend orgaan in zijn toezichtfunctie. In het algemeen moet ontslag of benoeming van een risicodirecteur worden bekendgemaakt en de toezichthoudende autoriteit moet op de hoogte worden gesteld van de daartoe strekkende redenen.

28. De compliancefunctie

1. Een instelling stelt een compliancefunctie in voor het beheer van het compliancerisico.
2. Een compliancebeleid wordt door een instelling goedgekeurd en ingevoerd en bekendgemaakt aan het voltallige personeel.

Toelichting
Het compliancerisico (het heersende of verwachte risico voor inkomsten en kapitaal dat voorvloeit uit het verzuim om wet- en regelgeving, voorschriften, overeenkomsten, voorgeschreven praktijken of ethische normen na te komen) kan leiden tot boetes, schade en/of de nietigverklaring van contracten en kan afbreuk doen aan de reputatie van een instelling.

3. Een instelling moet een permanente en doeltreffende compliancefunctie instellen en een persoon aanwijzen die binnen de gehele instelling en de groep deze functie uitoefent (compliance officer of hoofd compliance). In kleinere en minder complexe instellingen kan deze functie worden gecombineerd met of ondersteund door de functie van risicobeheerder of ondersteunende functies (bijv. HR-functies, juridische functies enz.).
4. De compliance officer moet ervoor zorgen dat het compliancebeleid wordt nageleefd en dat verslag wordt uitgebracht aan het leidinggevend orgaan en, indien van toepassing, de risicobeheerder over het beheer door de instelling van het compliancerisico. Het leidinggevend orgaan en de risicobeheerder moeten de conclusies van de compliance officer in aanmerking nemen bij de besluitvorming.

5. De compliance officer moet advies verstrekken aan het leidinggevend orgaan over wet- en regelgeving en voorschriften en normen waaraan de instelling moet voldoen. Daarnaast moet hij of zij het mogelijke effect beoordelen van veranderingen in het wetgevend en regelgevend kader dat op de activiteiten van de instelling van toepassing is.
6. De compliance officer moet ook verifiëren of nieuwe producten en nieuwe procedures voldoen aan het geldende juridische kader en aan bekende op handen zijnde wijzigingen in de wet- en regelgeving en toezichtvereisten.

Toelichting
Bijzondere zorgvuldigheid is geboden als de instelling bepaalde diensten verricht of structuren opzet namens klanten (bijv. optredend als agent bij de oprichting van een vennootschap of partnerschap, verlening van trusteediensten of de ontwikkeling van complexe financiële transacties voor klanten), die kunnen leiden tot specifieke uitdagingen op het vlak van interne governance en prudentiële bezorgdheden.

29. Interne-auditfunctie

1. De bekleder van de interne-auditfunctie, de interne auditor, beoordeelt het kader voor interne controle op doeltreffendheid en efficiëntie.
2. Hij of zij moet volledige toegang hebben tot relevante documenten en gegevens in alle operationele en controleafdelingen.
3. De interne auditor moet controleren of alle activiteiten en eenheden van een instelling (hieronder vallen ook de risicobeheerder en compliance officer) zich houden aan de beleidsmaatregelen en procedures. De interne-auditfunctie dient daarom niet met een andere functie te worden gecombineerd. De interne auditor moet tevens beoordelen of bestaande beleidsmaatregelen en procedures nog steeds geschikt zijn en aan de wettelijke en regelgevingsvereisten voldoen.
4. De interne auditor moet met name de integriteit van de processen controleren en daarbij de betrouwbaarheid waarborgen van de methoden en technieken, aannames en informatiebronnen die in de interne modellen van de instelling worden benut (bijv. risicomodellering en de waardering ten behoeve van de financieel-administratieve verantwoording en verslaglegging). Voorts moet hij of zij de instrumenten voor kwalitatieve risico-identificatie en -beoordeling controleren op kwaliteit en toepassing. Om de onafhankelijke positie van de interne auditor te versterken, moet hij of zij echter niet rechtstreeks worden betrokken bij het ontwerp en de selectie van modellen of andere instrumenten voor risicobeheer.
5. Het leidinggevend orgaan moet de interne auditors stimuleren zich te houden aan nationale en internationale professionele normen. Werkzaamheden in het kader van de interne-auditfunctie moeten worden verricht op basis van een

controleplan en gedetailleerde auditprogramma's waarbij een op risico's gebaseerde benadering wordt gehanteerd. Het controleplan moet door het accountantscomité en/of het leidinggevend orgaan worden goedgekeurd.

Toelichting
Een voorbeeld van bovengenoemde professionele normen zijn de standaarden zoals vastgesteld door het Institute of Internal Auditors.

6. De interne auditor rapporteert zijn bevindingen en suggesties voor relevante verbeteringen in de interne controles rechtstreeks aan het leidinggevend orgaan en/of (in voorkomend geval) zijn accountantscomité. Alle auditaanbevelingen moeten op de respectieve managementniveaus worden onderworpen aan een formele follow-upprocedure om de omzetting ervan te waarborgen en rapporteren.

E. Informatiesystemen en bedrijfscontinuïteit

30. Informatiesystemen en communicatie

1. Een instelling beschikt over doeltreffende en betrouwbare informatie- en communicatiesystemen die alle significante activiteiten bestrijken.

Toelichting
De besluitvorming van het management kan ongunstig worden beïnvloed door onbetrouwbare of misleidende gegevens afkomstig van systemen die gebrekkig zijn ontworpen en onvoldoende worden gecontroleerd. Een kritiek onderdeel van de activiteiten van een instelling bestaat derhalve uit het opzetten en onderhouden van informatie- en communicatiesystemen die het volledige gamma van activiteiten bestrijken. Deze informatie wordt normaliter langs al dan niet elektronische weg verstrekt. Een instelling moet zeer alert zijn op organisatorische en internecontrolevereisten in verband met de verwerking van gegevens in elektronische vorm en de noodzaak te zorgen voor een adequaat controlespoor. Dat geldt evenzeer voor IT-systemen die worden uitbesteed aan een IT-dienstverlener.

2. Informatiesystemen, met inbegrip van die systemen waarin elektronische gegevens worden bewaard en gebruikt, moeten veilig zijn, er moet onafhankelijk toezicht op worden uitgeoefend en de systemen moeten door geschikte noodvoorzieningen worden ondersteund. Een instelling moet zich bij de implementatie van IT-systemen houden aan algemeen aanvaarde IT-standaarden.

31. Beheer van de bedrijfscontinuïteit

1. Een instelling stelt de beleidslijnen vast voor een gedegen bedrijfscontinuïteitsbeheer dat op permanente basis kan worden uitgeoefend en verliezen door ernstige verstoringen van de bedrijfsactiviteiten kan beperken.

> Toelichting
>
> De bedrijfsvoering van een instelling is afhankelijk van verscheidene kritieke hulpmiddelen (bijv. IT-systemen, communicatiesystemen, gebouwen). Het doel van het bedrijfscontinuïteitsbeheer is de gevolgen te beperken van operationele, financiële, juridische en reputatiegevolgen en andere ingrijpende gevolgen van een ramp of langdurige onderbrekingen in het functioneren van deze hulpbronnen en, als gevolg daarvan, de verstoring van de normale bedrijfsprocedures van de instelling. Andere vormen van risicobeheer kunnen bestaan uit maatregelen die de kans op dergelijke incidenten verkleinen of de financiële gevolgen ervan overdragen op derde partijen (bijv. door het afsluiten van verzekeringen).

2. Om een gedegen bedrijfscontinuïteitsbeheer te kunnen vaststellen moet de instelling zorgvuldig het risico analyseren van blootstelling aan ernstige bedrijfsonderbrekingen en een beoordeling maken van de hieruit volgende potentiële effecten (in zowel kwantitatief als kwalitatief opzicht). Daarbij moeten interne en/of externe onderzoeken van gegevens en scenario's worden benut. Deze analyse moet alle bedrijfs- en ondersteuningseenheden alsmede de risicobeheerfunctie bestrijken, rekening houdend met hun onderlinge afhankelijkheid en verwevenheid. Voorts moet de bekleder van een specifieke onafhankelijke bedrijfscontinuïteitsfunctie actief bij de werkzaamheden worden betrokken. De resultaten van de analyse moeten bijdragen aan de bepaling van de herstelprioriteiten en doelstellingen van de instelling.

> Toelichting
>
> Wat betreft de functie voor het beheer van het operationele risico, zie ook Richtlijn 2006/48/EG, bijlage X, deel 3, punt 4, waarin een dergelijke onafhankelijke functie verplicht wordt gesteld voor AMA-instellingen; de taken in het kader van deze functie worden omschreven in de punten 615-620 van de validatierichtsnoeren (gepubliceerd in 2006), beschikbaar op de website van de EBA.

3. Op basis van bovengenoemde analyse dient een instelling over het volgende te beschikken:

    a. Noodplannen en bedrijfscontinuïteitsplannen die ervoor zorgen dat een instelling passend op noodsituaties reageert en in staat is haar

belangrijkste bedrijfsactiviteiten doorgang te laten vinden indien zich een onderbreking van de normale bedrijfsprocedures voordoet.

b. Herstelplannen voor kritieke hulpbronnen die de instelling in staat stellen de normale bedrijfsprocedures binnen een gepaste termijn te hervatten. Eventuele restrisico's voortkomend uit potentiële verstoringen in de bedrijfsvoering moeten stroken met de risicotolerantie/-bereidheid van de instelling.

4. Noodplannen, bedrijfscontinuïteitsplannen en herstelplannen moeten worden gedocumenteerd en nauwgezet ten uitvoer worden gelegd. De documentatie moet beschikbaar zijn in de bedrijfs- en ondersteuningseenheden en bij de risicobeheerder. Voorts moeten de documentatie worden opgeslagen in fysiek van elkaar gescheiden systemen en in noodgevallen gemakkelijk toegankelijk zijn. Er moet gezorgd worden voor gepaste opleiding. Plannen moeten regelmatig worden getest en bijgewerkt. Tekortkomingen of fouten in de testen moeten worden gedocumenteerd en geanalyseerd waarna de plannen worden herzien.

F. Transparantie

32. Aanreiken van middelen

1. Strategieën en beleidsmaatregelen worden aan al het relevante personeel in een instelling meegedeeld.
2. Het personeel van een instelling moet het beleid en de procedures die relevant zijn voor hun taken en verantwoordelijkheden begrijpen en naleven.
3. Bijgevolg moet het leidinggevend orgaan de relevante werknemers op duidelijke en samenhangende wijze inlichten en van recente informatie voorzien over de strategieën en beleidsmaatregelen, in ieder geval in de voor het personeel benodigde mate om hun taken te kunnen uitoefenen. De informatie kan worden aangereikt door middel van schriftelijke richtsnoeren, handboeken of andere middelen.

33. Transparantie van de interne governance

1. Een instelling zorg voor een transparant kader voor interne governance. Een instelling brengt haar huidige positie en toekomstperspectieven helder, evenwichtig, accuraat en tijdig voor het voetlicht.

Toelichting

Het doel van transparantie op het gebied van interne governance is alle relevante stakeholders van een instelling (waaronder de aandeelhouders, het personeel, klanten en het grote publiek) belangrijke informatie te verstrekken die zij nodig hebben om de doeltreffendheid van het leidinggevend orgaan als bestuur van de instelling te beoordelen.

Overeenkomstig artikel 72 van Richtlijn 2006/48/EG en artikel 2 van Richtlijn 2006/49/EC moeten EU-moederinstellingen en instellingen die onder de zeggenschap staan van een financiële EU-moederholding op geconsolideerde basis uitvoerige en zinvolle informatie bekendmaken ter beschrijving van hun interne governance. Het is een goede praktijk dat elke instelling informatie over hun interne governance op individuele basis verstrekt.

2. Een instelling dient in ieder geval de volgende gegevens aan het publiek bekend te maken:

   a. haar structuren en beleidsmaatregelen op het gebied van governance, met inbegrip van haar doelstellingen, organisatiestructuur, regelingen inzake interne governance, opbouw en organisatie van het leidinggevend orgaan waaronder opkomstgegevens, en het belonings- en stimuleringsmodel van de instelling;

   b. de aard en omvang, het doel en de economische essentie van transacties met aangesloten maatschappen en betrokken partijen, indien deze van wezenlijke invloed op de instelling zijn;

   c. de wijze waarop haar bedrijfs- en risicostrategie wordt opgezet (waarin ook de betrokkenheid van het leidinggevend orgaan een rol speelt) en te verwachten risicofactoren;

   d. haar opgerichte comités en hun mandaten en samenstelling;

   e. haar kader voor interne controle en hoe haar controlefuncties zijn georganiseerd, de belangrijkste taken die de werknemers in deze functies uitoefenen, de wijze waarop het leidinggevend orgaan op hun werkzaamheden toeziet en geplande wezenlijke veranderingen in deze functies; en

   f. materiële gegevens over haar financieel en bedrijfsresultaat.

3. Informatie over de huidige positie van de instelling moet stroken met de wettelijke openbaarmakingsvereisten. De informatie moet duidelijk, accuraat, relevant en toegankelijk zijn en tijdig worden verstrekt.
4. In gevallen waarin het waarborgen van een hoge nauwkeurigheidsgraad de vrijgave van spoedeisende informatie zou vertragen moet een instelling een passende afweging maken tussen spoed en nauwkeurigheid, met inachtneming

van de eis dat een waarheidsgetrouw en eerlijk beeld van de situatie wordt geschetst en een bevredigende verklaring wordt gegeven voor een vertraging. Deze verklaring mag niet worden gebruikt om verplichtingen inzake reguliere rapportages op te schuiven.

Titel III – Slotbepalingen en tenuitvoerlegging

34. Intrekking

Met de goedkeuring en bekendmaking van deze richtsnoeren inzake interne governance worden de volgende richtsnoeren ingetrokken: punt 2.1 van de CEBT-richtsnoeren inzake de uitoefening van bedrijfseconomisch toezicht (van 25 januari 2006, getiteld “Richtsnoeren inzake interne governance”), de overkoepelende beginselen van het CEBT voor het beloningsbeleid (van 20 april 2009) en de overkoepelende beginselen voor risicobeheer (van 16 februari 2010).

35. Toepassingsdatum

De bevoegde autoriteiten voeren deze richtsnoeren uit door ze uiterlijk 31 maart 2012 op te nemen in hun toezichtpraktijken. Na die datum moeten bevoegde autoriteiten de daadwerkelijke naleving van de richtsnoeren waarborgen.