December 2015

Beginselen voor ondernemingsbesturing, organisatie-inrichting en risicobeheersing

Brochure voor interne auditors in de financiële sector

Koninklijke Nederlandse Beroepsorganisatie van Accountants

NBA

Instituut van Internal Auditors Nederland

Deze brochure is geschreven door een werkgroep namens IIA Nederland en de NBA Ledengroep Intern en Overheidsaccountants, bestaande uit de volgende personen:

John Bendermacher, ABN AMRO Bank
Reinout Hoogendoorn, Nederlandse Waterschapsbank
René de Jong, Bank Nederlandse Gemeenten
Gertjan Langelaan, Van Lanschot Bankiers
Hans Moison, Great Too
Leen van der Plas, ING Bank
Vincent Wanders, Compliant & More

December 2015

Inhoud

1. Preambule

Aan ondernemingen in de financiële sector in Nederland worden veel eisen gesteld, ook op de aandachtsgebieden ondernemingsbesturing, organisatie-inrichting en risicobeheersing: nationale en internationale wet- en regelgeving, toezichtwet- en regelgeving voor bepaalde bedrijfstakken en codes voor corporate governance. Deze eisen zijn dikwijls gedetailleerd, betreffen veelal specifieke aandachtsgebieden of zijn bedoeld voor een bepaalde typologie van ondernemingen. Met een compact en toegankelijk overzicht van beginselen voor ondernemingsbesturing, organisatie-inrichting en risicobeheersing dat breed toepasbaar is, kan de inzichtelijkheid ervan worden vergroot en de naleving ervan worden verbeterd.

Het is niet mogelijk om eisen te formuleren die voor alle financiële ondernemingen van toepassing zijn. Daarvoor zijn de activiteiten, de omvang, de complexiteit, het risicoprofiel en het maatschappelijk belang te divers. Veel algemene uitgangspunten blijken niettemin op veel financiële ondernemingen toepasbaar. Met de in deze brochure opgenomen beginselen voor ondernemingsbesturing, organisatie-inrichting en risicobeheersing is getracht om dergelijke algemene uitgangspunten te formuleren. IIA Nederland (IIA NL) en de NBA Ledengroep Intern en Overheidsaccountants (NBA LIO) beogen daarmee de interne auditor bij het onderzoek van de governance, het risicobeheer en de beheersprocessen duidelijke beginselen mee te geven. Deze dienen per situatie te worden omgezet in een 'op maat'-referentiekader.

De beginselen zijn niet gebaseerd op een specifiek model of bepaalde veronderstellingen of paradigma's maar zijn de 'grootste gemene deler' van de op de desbetreffende ondernemingen van toepassing zijnde wet- en regelgeving, andere vereisten, theorieën en concepten. In specifieke omstandigheden zal moeten worden vastgesteld of wet- en regelgeving of andere vereisten verder gaan of strikter moeten worden toegepast dan deze beginselen. In dat geval gaan die vereisten voor de beginselen. De teksten na de beginselen zijn een toelichting op of een uitwerking van de beginselen.

2. Inleiding op de beginselen

2.1 De beginselen beschrijven op hoog abstractieniveau de eisen die op de genoemde deelaspecten redelijkerwijs aan een financiële onderneming[1] kunnen worden gesteld[2].

Beginselen kunnen op een gedetailleerd niveau worden uitgewerkt maar dat maakt deze minder goed toepasbaar. In de praktijk is maatwerk en flexibiliteit vereist. Een hoog abstractieniveau betekent dat de beginselen open zijn geformuleerd. Dat mag er in de praktijk niet toe leiden dat deze onvoldoende streng worden uitgelegd en toegepast. De beginselen zijn beperkt tot de genoemde deelaspecten en betreffen niet andere belangrijke aspecten van de bedrijfsvoering[3].

2.2 De beginselen zijn op basis van het proportionaliteitsbeginsel op de meeste financiële ondernemingen toepasbaar.

De meeste beginselen zijn zonder beperking toepasbaar op alle financiële ondernemingen. In een aantal gevallen kan op basis van de aard, de omvang, de activiteiten en de complexiteit van de onderneming worden geconcludeerd dat niet aan de beginselen behoeft te worden voldaan. In dat geval kan een onderneming, met redenen omkleed, hiervan afwijken, tenzij het gaat om verplichtingen die voortvloeien uit wet- en regelgeving.

2.3 De beginselen zijn opgesteld door het Instituut van Internal Auditors Nederland en de ledengroep Intern en Overheidsaccountants van de Nederlandse Beroepsorganisatie van Accountants.

De beginselen beogen de interne auditor bij het onderzoek van de governance, het risicobeheer en de beheersprocessen een duidelijk referentiekader te bieden en komen niet in de plaats van wet- en regelgeving of van bestaande codes. De beginselen dienen op maat en flexibel te worden toegepast.

3. Verantwoordelijkheden van de onderneming

3.1 Bepalen missie, kernwaarden, strategie en beleid

3.1.1 De onderneming bepaalt de missie, de kernwaarden, de strategie en het beleid en legt deze systematisch, inzichtelijk en toegankelijk vast. De gewenste cultuur, het daarbij vereiste gedrag en de risicobereidheid van de onderneming maken hiervan deel uit.

Met een duidelijke missie, verantwoorde kernwaarden, een duidelijk strategie en daaruit afgeleid effectief beleid worden de randvoorwaarden gecreëerd voor de bedrijfsvoering en de realisatie van de ondernemingsdoelstellingen. Om het personeel en andere betrokkenen te stimuleren en te motiveren is het van belang dat deze randvoorwaarden adequaat worden vastgelegd en overgedragen. Het creëren en handhaven van de juiste cultuur ('toon aan de top') en passend gedrag zijn van groot belang. De toepassing van alleen harde organisatorische beheersingsmaatregelen is onvoldoende. De risicobereidheid van de organisatie wordt duidelijk afgebakend om opportunisme bij de bedrijfsvoering te voorkomen. De risicobereidheid wordt vooraf door de raad van commissarissen goedgekeurd.

3.1.2 De onderneming houdt evenwichtig rekening met de belangen van personen en organisaties die bij de onderneming betrokken zijn.

Ondernemingen staan midden in de samenleving. Voorkomen moet worden dat het (financiële) belang op korte termijn van de onderneming, de aandeelhouders, het bestuur of het personeel een dominante rol speelt bij de besluitvorming. Daarom stelt de onderneming expliciet vast op welke wijze en in welke mate de belangen van alle partijen bij de besluitvorming worden betrokken en hoe deze worden gewogen en legt de risico's en belangenafweging vast. Daartoe behoren onder meer de maatschappelijke omgeving[4], cliënten[5], zakelijke relaties, personeel, vermogensverschaffers[6], fiscale autoriteiten en toezichthouders. De mate waarin bestuur en personeel tegemoetkomen aan deze uitgangspunten, speelt een belangrijke rol bij de beoordeling en de beloning.

3.1.3 De onderneming beoordeelt regelmatig[7], mede op basis van veranderende omgevingsfactoren, de strategie en het beleid en past deze aan wanneer dit nodig is of wenselijk wordt geacht. Daarbij worden zorgvuldige (goedkeurings-) procedures gehanteerd.

Ondernemingen kunnen in problemen komen of ten onder gaan doordat zij zich onvoldoende snel aanpassen aan veranderende omgevingsfactoren. Het is van groot belang, juist wanneer een onderneming een sterke marktpositie heeft en goede resultaten behaalt, om alert te zijn op veranderingen, waardoor verdienmodellen, producten en diensten aan het einde van hun levenscyclus raken en nieuwe verdienmodellen, producten en diensten zich aandienen of ontwikkeld moeten worden. Ondernemingen beschikken over flexibiliteit en aanpassingsvermogen om hierop in te spelen.

3.1.4 De onderneming zet de missie, de kernwaarden, de strategie en het beleid alsmede bijstellingen daarvan, effectief en efficiënt om in de inrichting van de ondernemingsbesturing, de organisatie, de risicobeheersing, bedrijfsplannen en budgetten.

De missie, de kernwaarden, de strategie en het beleid worden concreet geëffectueerd. In detail worden de uitgangspunten, die een abstract karakter kunnen hebben, omgezet in concrete organisatorische maatregelen, doelstellingen en procedures. Uit de verantwoording over de dagelijkse gang van zaken kan worden afgeleid of en in welke mate is voldaan aan de uitgangspunten en doelstellingen die met de formulering van de missie van de organisatie in grote lijnen zijn afgebakend. De relatie tussen de missie, de kernwaarden, de strategie, het beleid en de concrete middellangetermijndoelstellingen, plannen en budgetten is verifieerbaar. De onderneming zet de missie en kernwaarden tevens om in duidelijke doelstellingen op het gebied van de belangen van klanten en maatschappelijk verantwoord ondernemen.

3.2 Inrichten ondernemingsbesturing, organisatie en risicobeheersing

3.2.1 De onderneming richt de ondernemingsbesturing, de organisatie en de risicobeheersing in op basis van de missie, de kernwaarden, de strategie en het beleid.

De missie, de kernwaarden, de strategie en het beleid bieden voldoende houvast voor de inrichting van de ondernemingsbesturing, de organisatie en de risicobeheersing. Bij de uitwerking hiervan wordt de relatie tot de uitgangspunten geconcretiseerd en inzichtelijk gemaakt.

3.2.2 De ondernemingsbesturing, de organisatie-inrichting en de risicobeheersing dragen optimaal bij aan de realisatie van de strategie en het beleid.

Bij de inrichting van de ondernemingsbesturing, de organisatie en de risicobeheersing ziet de onderneming zich voor keuzes gesteld omdat veel alternatieven voorhanden zijn. Binnen het kader van economisch verantwoorde oplossingen kiest de onderneming voor het alternatief dat het meest effectief bijdraagt aan de realisatie van de strategie en het beleid.

3.2.3 De onderneming richt de ondernemingsbesturing, de organisatie-inrichting en de risicobeheersing onder meer op beheersing van de ondernemingsrisico's en integer handelen.

In de dynamiek van de dagelijkse bedrijfsvoering kan een zekere mate van opportunisme ontstaan wanneer zich kennelijk aantrekkelijke zakelijke proposities voordoen. Het is van groot belang om de zorgvuldige afwegingen die zijn gemaakt bij het bepalen van de voorwaarden voor risicobeheersing (risicobereidheid) en integer handelen voortdurend in het oog te houden. Incidentele afwijkingen hiervan zijn alleen na zorgvuldige afweging en goedkeuring toegestaan en worden gedocumenteerd.

3.2.4 De onderneming zet de ondernemingsbesturing, de organisatie-inrichting en de risicobeheersing om in een geïntegreerd stelsel van besturing, managementbeheersing en procesbeheersing.

Een deugdelijk, geïntegreerd stelsel van beheersingsmaatregelen is van groot belang voor de monitoring en beheersing van de bedrijfsvoering en de productie van inzichtelijke en controleerbare managementinformatie. Deze informatie is benodigd om de bedrijfsvoering in goede banen te leiden, te evalueren, bij te sturen en om er verantwoording over af te leggen.

3.2.5 Bij de inrichting van de besluitvormingsprocessen voorziet de onderneming in voldoende niveau van tegenwicht.

Een organisatie heeft voor verantwoorde besluitvorming tegenwicht nodig. Dit tegenwicht kan van meerdere niveaus en posities in en buiten de organisatie komen. De meerwaarde van tegenwicht wordt gevormd door de specifieke invalshoeken en belangen van elk der betrokkenen. De effectiviteit van tegenwicht wordt in belangrijke mate bepaald door de competenties van de betrokken personen. Bij de risicoanalyse voorafgaand aan belangrijke besluiten moet worden vastgesteld of hieraan voldoende tegemoet wordt gekomen.

3.2.6 De onderneming legt de ondernemingsbesturing, de organisatie-inrichting, de risicobeheersing en de administratieve procedures en maatregelen systematisch, inzichtelijk en toegankelijk vast in een raamwerk voor de beheersing van de bedrijfsvoering.

Met een raamwerk voor de beheersing van de bedrijfsvoering werkt een onderneming op een gestructureerde en beheerste manier aan de realisatie van haar doelen en kan dat zichtbaar maken aan haar maatschappelijke omgeving, cliënten, zakelijke relaties, personeel, vermogensverschaffers en toezichthouders. De risico's worden dusdanig adequaat gemonitord en beheerst dat de risico's binnen de kaders van de risicobereidheid vallen. Het risico op financieel nadeel en reputatieschade blijft binnen de door de onderneming acceptabel geachte grenzen.

3.2.7 De onderneming beoordeelt regelmatig de ondernemingsbesturing, de organisatie-inrichting en de risicobeheersing en past deze aan wanneer dit wenselijk wordt geacht.

Een onderneming die succesvol wil blijven beoordeelt en verbetert zichzelf voortdurend. Een proces van continue verbetering is in de organisatie ingebed en krijgt door het cyclische karakter voortdurend aandacht. Het betreft monitoring van de opzet en de effectieve werking van het raamwerk voor de beheersing van de bedrijfsvoering door alle geledingen van de organisatie[8].

3.3 Verantwoording

3.3.1 De onderneming legt verantwoording af aan personen en organisaties die bij de onderneming betrokken zijn. Daartoe behoren onder meer de maatschappelijke omgeving, cliënten, zakelijke relaties, personeel, vermogensverschaffers en toezichthouders.

Een onderneming legt verantwoording af aan verschaffers van risicodragend kapitaal en crediteuren maar ook aan het personeel - of hun vertegenwoordigers in de ondernemingsraad of de vakbond - dat voor het inkomen afhankelijk is van de onderneming. De maatschappelijke verantwoordelijkheid van de onderneming betreft ook partijen die een minder directe relatie hebben met de onderneming of daarvan niet direct afhankelijk zijn. De onderneming komt tegemoet aan de verantwoordelijkheid die hieruit voortvloeit, in aanvulling op de formele verplichtingen die bestaan tot externe verslaggeving. De verantwoording betreft een geïntegreerde rapportage van financiële informatie en niet-financiële informatie. De verantwoording bevat specifieke verklaringen van het bestuur van de onderneming over de beheersing van de bedrijfsvoering[9], de naleving van gedragsregels en codes en het handelen in overeenstemming met wettelijke vereisten of vereisten van toezichthouders.

4. Ondernemingsbesturing

4.1 Bestuur

4.1.1 Het bestuur is verantwoordelijk voor de onderneming, de missie, de kernwaarden, de strategie, het beleid, de ondernemingsbesturing, de organisatie-inrichting en de risicobeheersing.

De formele verantwoordelijkheid en aansprakelijkheid van bestuurders wordt bepaald door wettelijke voorschriften voor rechtspersonen en andere van toepassing zijnde wet- en regelgeving. Voorts kunnen corporate governance codes en andere gedragscodes relevant zijn. De onderneming analyseert de van toepassing zijnde wet- en regelgeving en gedragscodes en verwerkt de bepalingen als minimumvereisten in het bestuursreglement.

4.1.2 De samenstelling van het bestuur doet recht aan de ervaring en de expertise die benodigd is voor het bestuur als geheel om de verantwoordelijkheid voor de onderneming te dragen en de bestuurstaak naar behoren uit te voeren.

Het aantal, de diversiteit en complementariteit van de bestuursleden en de ervaring en expertise van de individuele bestuursleden zijn passend en geschikt voor de taak van het bestuur als geheel. Bestuurders zijn voldoende beschikbaar om de werkzaamheden uit te voeren. Een bestuursfunctie is doorgaans een voltijdsfunctie.

4.1.3 Het bestuur bepaalt de taakverdeling en de werkwijze en legt deze vast in een bestuursreglement.

Door de taakverdeling en de werkwijze af te spreken en vast te leggen ontstaat niet alleen duidelijkheid voor de individuele bestuursleden over hetgeen van hen verwacht wordt, maar ook voor de onderneming en de raad van commissarissen. De taakverdeling en werkwijze worden zo veel mogelijk afgestemd op de verantwoordelijkheid van het bestuur als geheel, de organisatiestructuur en functiescheidingen binnen de organisatie. Het bestuur heeft een voorzitter.

4.1.4 Binnen het bestuur wordt de verantwoordelijkheid voor de risicobeheersing, voor de financiële functie en voor de commerciële functie gescheiden[10].

In de dynamiek van de dagelijkse bedrijfsvoering kan een zekere mate van opportunisme ontstaan wanneer zich kennelijk aantrekkelijke zakelijke proposities voordoen. Het is van groot belang om de zorgvuldige afwegingen die zijn gemaakt bij het bepalen van de voorwaarden voor risicobeheersing (risicobereidheid) en integer handelen voortdurend in het oog te houden. Om deze reden wordt de verantwoordelijkheid voor de risicobeheersing en de verantwoordelijkheid voor de financiële functie binnen het bestuur altijd gescheiden van de verantwoordelijkheid voor de commerciële functie. Financiële ondernemingen hebben een hoger risicoprofiel en een groot maatschappelijk belang. Daarom wordt ook de verantwoordelijkheid voor de risicobeheersing en de verantwoordelijkheid voor de financiële functie binnen het bestuur gescheiden.

4.1.5 Het bestuur draagt de missie, de kernwaarden, de strategie, het beleid, de cultuur, de normen en de waarden van de onderneming uit, onder meer door voorbeeldgedrag.

Het is niet ondenkbaar dat de zorgvuldig geformuleerde uitgangspunten van de organisatie in de dynamiek van alledag uit het zicht raken en dat de leiding en het personeel zich daardoor niet, niet altijd of niet geheel in lijn met deze uitgangspunten gedragen. Daardoor kan de organisatie uit de koers raken en niet coherent opereren. Het is essentieel dat de missie, de kernwaarden, de strategie, het beleid, de cultuur, de normen en de waarden continue onder de aandacht van het bestuur en het personeel worden gebracht door gedragscodes, opleiding en training, informatievoorziening en tijdens de dagelijkse werkzaamheden.

4.1.6 Het bestuur vermijdt elke (schijn van) verstrengeling van privébelangen en zakelijke belangen van de onderneming.

Er mag geen enkele twijfel bestaan over het feit dat het bestuur alleen handelt in het belang van de onderneming en de partijen die daarbij betrokken zijn, binnen de grenzen van wet- en regelgeving. Bestuurders zijn aanspreekbaar op voorbeeldgedrag dat verder gaat dan de gecodificeerde afspraken over voorkoming van belangenverstrengeling. Hiertoe worden onder meer regels gesteld voor (een verbod op of voorafgaande goedkeuring van) financieringen aan bestuurders, andere transacties met bestuurders, privébeleggingen en nevenfuncties. Bestuurders bevestigen ten minste jaarlijks aan de compliance-functie of de raad van commissarissen in detail dat zij in overeenstemming met de gestelde regels hebben gehandeld en zullen handelen.

4.1.7 Het bestuur verstrekt de commissarissen tijdig de informatie die relevant is voor de uitoefening van hun taken.

De raad van commissarissen is voor een adequate taakuitoefening mede afhankelijk van de informatie die door het bestuur wordt verstrekt. Deze informatie dient tijdig te worden verstrekt, ruim voor vergaderingen van de raad van commissarissen en zo nodig ad hoc. De informatie dient toegankelijk te zijn (inzichtelijk en informatief, op de juiste wijze geaggregeerd) en volledig maar beperkt tot hetgeen noodzakelijk is voor een adequate taakuitoefening. Desgewenst verzoekt de raad van commissarissen de interne auditfunctie om onderzoek te doen naar de betrouwbaarheid en relevantie van de informatie die wordt verstrekt.

4.1.8 Het bestuur vergadert regelmatig en doet schriftelijk verslag van zijn vergaderingen in notulen.

De frequentie van de vergaderingen is passend voor de activiteiten van de onderneming en de ontwikkelingen en risico's die zich voordoen. De notulen vermelden in elk geval de deelnemers aan het overleg, wie verhinderd waren, de agenda, de afwikkeling van de vorige vergadering en de eerdere actiepunten, de belangrijkste overwegingen die hebben geleid tot besluiten, de besluiten en de nieuwe actiepunten. Bij de onderwerpen wordt vermeld welk bestuurslid op welke wijze een inbreng of bijdrage heeft geleverd. Uit de notulen blijkt of sprake was van voldoende discussie en tegenwicht bij de besluitvorming.

4.1.9 Het bestuur neemt deel aan een maatwerk programma van permanente educatie dat alle relevante aspecten van de bestuurstaak omvat.

Het programma van permanente educatie wordt afgestemd op de specifieke behoefte van het bestuur en de organisatie en bevat onderwerpen betreffende de bedrijfstak waarin de onderneming actief is, macro-economische ontwikkelingen, wet- en regelgeving, compliance, risicobeheersing, automatisering, personeelsaangelegenheden e.d. Bij voorkeur wordt het programma verzorgd door deskundigen van de organisatie en van buiten de organisatie.

4.2 Raad van commissarissen

4.2.1 De raad van commissarissen is verantwoordelijk voor het toezicht op de onderneming als geheel, het bestuur en de benoeming en het ontslag van bestuurders. De raad van commissarissen behartigt de belangen van alle belanghebbenden evenwichtig.

De formele verantwoordelijkheid en aansprakelijkheid van commissarissen wordt bepaald door wettelijke voorschriften voor rechtspersonen en andere van toepassing zijnde wet- en regelgeving. Voorts kunnen corporate governance codes en andere gedragscodes relevant zijn. De onderneming analyseert de van toepassing zijnde wet- en regelgeving en gedragscodes en verwerkt de bepalingen als minimumvereisten in het reglement van de raad van commissarissen. Om de onafhankelijkheid van de commissarissen te waarborgen houden zij geen financiële belangen in de onderneming.

4.2.2 De samenstelling en de diversiteit van de raad van commissarissen doet recht aan de ervaring en de expertise die benodigd is voor de raad van commissarissen als geheel om de verantwoordelijkheid voor het toezicht op het bestuur te dragen en de toezichtstaak naar behoren uit te voeren.

Het aantal, de diversiteit en complementariteit van de commissarissen en de ervaring en expertise van de individuele commissarissen zijn passend voor de toezichttaak[11]. De commissarissen zijn voldoende beschikbaar om de werkzaamheden uit te voeren. De raad van commissarissen bepaalt het aantal leden van de raad, dat minimaal drie is, en stelt beperkingen aan de aard en het aantal commissariaten en bestuursfuncties die de leden mogen vervullen. Bij de benoeming van voormalig bestuurders als commissaris wordt terughoudendheid betracht en in voorkomend geval een 'afkoelingsperiode' in acht genomen. De voorzitter van de raad van commissarissen is geen voormalig bestuurder van de onderneming.

4.2.3 De raad van commissarissen bepaalt de taakverdeling en de werkwijze en legt deze vast in het reglement van de raad van commissarissen.

Door de taakverdeling en de werkwijze af te spreken en vast te leggen ontstaat niet alleen duidelijkheid voor de individuele commissarissen over hetgeen van hen verwacht wordt,

maar ook voor het bestuur, de aandeelhouders en andere belanghebbenden. De taakverdeling en werkwijze worden zo veel mogelijk afgestemd op de verantwoordelijkheid van de raad van commissarissen als geheel. De raad van commissarissen heeft een voorzitter.

4.2.4 De raad van commissarissen kan[12] uit zijn midden commissies voor specifieke aandachtgebieden benoemen, zoals een corporate governance-commissie[13], auditcommissie[14], risicocommissie[15], benoemingscommissie[16] en beloningscommissie[17]. Deze commissies verdiepen zich in de specifieke onderwerpen, informeren de raad van commissarissen hierover, doen voorstellen aan de raad van commissarissen en bereiden besluitvorming van de raad van commissarissen voor.

De benoeming van commissies voor specifieke aandachtgebieden doet recht aan het feit dat bepaalde onderwerpen meer specialistische aandacht vragen. Binnen de commissies worden deze onderwerpen diepgaand behandeld. De commissies komen zo vaak bijeen als nodig is. Zij kunnen informatie inwinnen bij specialisten die zij voor hun vergadering uitnodigen, bijvoorbeeld medewerkers van de onderneming, bestuurders, de actuaris, de accountant of derden.

4.2.5 De raad van commissarissen vergadert regelmatig en doet schriftelijk verslag van zijn vergaderingen in notulen en in het verslag van de raad van commissarissen in de externe verslaggeving.

De frequentie van de vergaderingen is passend voor de activiteiten van de onderneming en de ontwikkelingen en risico's die zich voordoen. De notulen vermelden in elk geval de deelnemers aan het overleg, wie verhinderd waren, de agenda, de afwikkeling van de vorige vergadering en de eerdere actiepunten, de belangrijkste overwegingen die hebben geleid tot besluiten, de besluiten en de nieuwe actiepunten. Bij de onderwerpen wordt vermeld welke commissaris op welke wijze een inbreng of bijdrage heeft geleverd.

4.2.6 De raad van commissarissen of de uit zijn midden benoemde auditcommissie, is betrokken bij de besluitvorming over aanstelling, beoordeling, beloning en ontslag van de leiding van de interne auditfunctie.

De interne auditfunctie is onafhankelijk en interne auditors functioneren objectief bij het uitvoeren van hun werkzaamheden. Om dat te bewerkstelligen en eventuele belemmeringen weg te nemen wordt de leiding van de interne auditfunctie niet zonder instemming van de raad van commissarissen of de auditcommissie door het bestuur aangesteld, beoordeeld, beloond of ontslagen.

4.2.7 De raad van commissarissen neemt deel aan een maatwerk programma van permanente educatie dat alle relevante aspecten van de toezichtstaak omvat.

Het programma van permanente educatie wordt afgestemd op de specifieke behoefte van de raad van commissarissen en bevat onderwerpen betreffende de bedrijfstak waarin de

onderneming actief is, macro-economische ontwikkelingen, wet- en regelgeving, compliance, risicobeheersing, automatisering, personeelsaangelegenheden e.d. Bij voorkeur wordt het programma verzorgd door deskundigen van de organisatie en van buiten de organisatie.

4.2.8 De raad van commissarissen evalueert ten minste een maal per jaar zijn eigen functioneren en het functioneren van uit zijn midden benoemde commissies.

Het doel van de evaluatie is een kritische beoordeling van het functioneren. Deze evaluatie kan het functioneren van de raad van commissarissen bevorderen en ertoe bijdragen dat bij (her)benoeming de juiste keuzes worden gemaakt. Het heeft de voorkeur om een dergelijke evaluatie periodiek te laten uitvoeren door een onafhankelijke partij van buiten de organisatie.

5. Organisatie-inrichting en risicobeheersing

5.1 Maatregelen organisatie-inrichting en risicobeheersing

Algemene uitgangspunten

5.1.1 De maatregelen voor de organisatie-inrichting en de risicobeheersing zijn afgestemd op de aard, de omvang, de activiteiten en de complexiteit van de onderneming.

Deze maatregelen betreffen onder meer de cultuur en het gedrag, aanstellen, belonen en beoordelen van personeel, verdeling van functies en taken, gedragscodes, risicocomités, informatie en communicatie, drie verdedigingslinies en maatregelen voor noodsituaties. De organisatie-inrichting en risicobeheersing kunnen niet worden gebaseerd op een of enkele van deze aspecten omdat dat onvoldoende garanties biedt voor de adequate werking van beheersingsmaatregelen. Er is sprake van een geïntegreerd raamwerk voor de beheersing van de bedrijfsvoering. Alleen een benadering waarbij de onderneming alle aspecten inbedt in de organisatie biedt door de complementariteit van de maatregelen voldoende zekerheid.

5.1.2 De onderneming beschikt over een adequate beheercyclus met regelmatige rapportage en analyse die zo nodig tot bijsturing leidt.

De beheercyclus is het proces van (strategische) planning, via uitvoering en bijsturing naar verantwoording. De beheercyclus vormt de basis voor de interne beheersing en de externe verantwoording van de onderneming.

De beheercyclus kent doorgaans de volgende of vergelijkbare stappen:
- Bepalen van de strategische opties;
- Analyse van sterkten, zwakten, kansen en bedreigingen;
- Meerjarenplan- en begroting;
- Jaarplan en begroting;
- Operationele uitvoering en beheersing;
- Monitoring en testen;
- Rapportages en analyses;
- Vergelijking met markt en concurrenten.

Bijsturing vindt plaats op strategisch niveau (bestuurlijk, zoals missie, kernwaarden, strategie, beleid), tactisch niveau (managementbeheersing, zoals meerjarenplannen en -begroting) en operationeel niveau (procesbeheersing, zoals jaarplannen, begroting, budget, monitoring, testen en rapportage).

5.1.3 De onderneming stimuleert de juiste cultuur en goed gedrag door voorbeeldgedrag van het bestuur en leidinggevenden. Adequaat functionerende soft controls en gedragsgerichte beheersingsmaatregelen zijn een essentieel onderdeel van het raamwerk voor de beheersing van de bedrijfsvoering. Cultuur en gedrag maken onderdeel uit van de beoordelingscriteria van het bestuur en het personeel en van het beloningsbeleid.

De zogenoemde harde beheersingsmaatregelen zijn niet altijd voldoende effectief wanneer deze niet gedragen worden door de juiste cultuur en goed gedrag. Hiertoe wordt vaak onderscheid gemaakt tussen de formele en de informele beheersingsmaatregelen. De informele beheersingsmaatregelen hebben te maken met het gedrag van bestuurders en personeel en de zogenoemde zachte beheersingsmaatregelen, soft controls. Deze moeten zijn ingebed in de organisatie en de dagelijkse procesgang. Het bewustzijn van het belang van cultuur en gedrag voor de interne beheersing wordt gestimuleerd, bijvoorbeeld door trainingen. De effectieve werking wordt gemonitord en er wordt intern over gerapporteerd. Het beloningsbeleid wordt vooraf door de raad van commissarissen goedgekeurd.

5.1.4 De onderneming beschikt over een onafhankelijk vertrouwelijk meldpunt[18] voor mogelijk illegaal, onethisch of onprofessioneel gedrag voor personeel, cliënten, zakelijke relaties en derden. De behandeling van meldingen is gescheiden van de afdelingen of de medewerkers die het betreft. Het bestuur en de raad van commissarissen worden periodiek geïnformeerd door het meldpunt over het aantal en de aard en de afhandeling van de meldingen.

Een dergelijk meldpunt draagt preventief en repressief bij aan de handhaving van de juiste cultuur en goed gedrag. Meldingen worden tijdig en adequaat behandeld en onder de aandacht van het bestuur gebracht zodat zo nodig correctieve actie kan worden ondernomen. Dit kan bijstelling van procedures en maatregelen betreffen maar ook sancties die aan personen worden opgelegd. De privacy van de melder (klokkenluider of 'whistleblower') wordt hierbij beschermd, door geheimhouding.

Personeel

5.1.5 De onderneming bepaalt duidelijke functieprofielen en competentiecriteria voor de belangrijkste (groepen van) functies en stelt personeel aan dat hieraan voldoet.

De onderneming stelt medewerkers met de juiste kwalificaties (opleiding, ervaring, competenties, integriteit) op de juiste posities aan en voorziet hiermee in de capaciteitsbehoefte. De medewerkers zijn gemotiveerd om de ondernemingsdoelstellingen te realiseren en daarmee te voldoen aan de verwachtingen die betrokkenen daarvan hebben.

5.1.6 Het functioneren van medewerkers wordt periodiek getoetst aan de hand van de missie, de kernwaarden, de strategie en het beleid van de onderneming en de prestatie-indicatoren voor de afdeling en het individu, zoals vastgelegd in functieprofielen. Het beloningsbeleid is hierop afgestemd.

De ondernemingsdoelstellingen worden op duidelijke wijze omgezet in taken, bevoegdheden en prestatie-indicatoren van afdelingen en individuen, zodat bij beoordeling relevante uitkomsten over het presteren worden gegenereerd. De prestaties en de beloning van medewerkers dient minimaal een maal per jaar te worden geëvalueerd om het gewenste gedrag te stimuleren. Perverse prikkels in de beloningsafspraken worden niet gebruikt. Variabele beloning wordt terughoudend toegepast en is alleen gericht op het realiseren van de ondernemingsdoelstellingen op lange termijn. Medewerkers in de risicobeheerfunctie, de compliance-functie en de interne auditfunctie ontvangen geen variabele beloning die afhankelijk is van de (financiële) prestaties van de onderneming.

5.1.7 De onderneming voorziet in procedures en maatregelen om de continuïteit van kritieke functies te waarborgen.

De onderneming treft maatregelen waardoor grote afhankelijkheid van een of enkele personen wordt gereduceerd. De onderneming heeft voor zogenoemde sleutelposities een opvolgingsplan waarin kortdurende, middellange en permanente vervanging is geregeld.

Functies en taken

5.1.8 De onderneming verdeelt duidelijk en coherent functies, taken, verantwoordelijkheden en bevoegdheden en stemt rapportagelijnen daarop af. De onderneming stemt de verdeling van functies, taken, verantwoordelijkheden en bevoegdheden af op de activiteiten van de onderneming, de benodigde capaciteit en de competentiecriteria.

De juiste verdeling van functies, taken, verantwoordelijkheden en bevoegdheden draagt in belangrijke mate bij aan het efficiënt en effectief functioneren van de onderneming. Deze verdeling is niet statisch. Flexibiliteit in de personele structuur en bezetting is belangrijk voor de ontwikkeling van een onderneming en de doorstroming van talent. Functies, taken, verantwoordelijkheden en bevoegdheden worden duidelijk vastgelegd, zijn actueel en geven richting aan de werkzaamheden van medewerkers.

Functiescheidingen

5.1.9 De onderneming past toereikende functiescheidingen toe om in een beheerste en integere bedrijfsvoering te voorzien.

Met de juiste functiescheidingen tussen personen en afdelingen, worden belangentegenstellingen binnen de onderneming gecreëerd die bijdragen aan het effectief functioneren van de beheersingsmaatregelen. Het is van belang dat deze belangentegenstellingen niet door samenspanning of fraude worden doorbroken.

5.1.10 Primair worden ten minste beschikkende[19], bewarende[20], controlerende[21], registrerende[22] en uitvoerende functies[23] gescheiden.

Wanneer dit type functies door dezelfde persoon of dezelfde afdelingen wordt vervuld, bestaat niet de functiescheiding waarnaar een organisatie streeft. Concessies aan het principe van primaire functiescheidingen worden zo veel mogelijk vermeden. De bewarende functie heeft een bredere werking dan alleen fysieke bewaring. Hierbij kan ook worden gedacht aan de bewaking van financiële activa, waaraan geen posten zonder goede reden en ongeautoriseerd mogen worden onttrokken. In een sterk geautomatiseerde omgeving van een moderne onderneming vindt dit onder meer zijn weerslag in toegangsrechten tot systemen voor gegevensverwerking en -opslag waarmee de bedrijfsprocessen worden ondersteund of waarmee de bedrijfsprocessen worden vormgegeven.

5.1.11 Secundair worden functies gescheiden wanneer functievermenging binnen een afdeling onvermijdelijk is, door taken bij verschillende personen onder te brengen.

Deze situatie is binnen een kleine organisatie niet altijd te vermijden. In dat geval wordt binnen de desbetreffende afdeling gekozen voor personen die op maximale organisatorische afstand tot elkaar staan. Hierbij kan ook worden gedacht aan het zogenoemde vier-ogen-principe.

Administratie, informatie en communicatie

5.1.12 De onderneming beschikt over middelen en procedures om gegevens over de bedrijfsprocessen en de rechten en verplichtingen die daaruit voortvloeien, juist, tijdig en volledig vast te leggen, te verwerken en beschikbaar te stellen.

De gegevens en informatie zijn van groot belang voor de bedrijfsvoering, de risicobeheersing, de managementinformatie en de externe verantwoording daarover. Informatie en datacommunicatie zijn in het huidige informatietijdperk van levensbelang voor een onderneming. Het belang van goede en tijdige investeringen in de ICT[24] is groot[25].

5.1.13 De onderneming waarborgt de continue beschikbaarheid, betrouwbaarheid en integriteit van de gegevens. De onderneming neemt maatregelen om te voorkomen dat gegevens oneigenlijk worden gebruikt of worden misbruikt.

Omdat informatie zo belangrijk is, vergaren en bewaren ondernemingen steeds meer gegevens en voldoen daarbij aan de wettelijke bewaarplicht en privacywetgeving. Wanneer deze gegevens onjuist worden gebruikt of bij onbevoegden terecht komen, kan dat reputatieschade tot gevolg hebben. De bewaking van de privacy en integriteit is daarom cruciaal.

5.1.14 De gegevens zijn toegankelijk en worden juist, tijdig en volledig bewerkt tot actuele, betrouwbare en geïntegreerde financiële en niet-financiële informatie die benodigd is voor (inzicht in) de bedrijfsvoering, de risicobeheersing en de verantwoording die hierover wordt afgelegd. De informatie is eenvoudig te herleiden tot de brongegevens.

De kwaliteit van informatie is in belangrijke mate afhankelijk van de kwaliteit van de gegevens waarop deze is gebaseerd. Om te bewerkstelligen dat gegevens en informatie van adequate kwaliteit zijn is een gestructureerde aanpak noodzakelijk. Een dergelijke aanpak raakt het verzamelen en analyseren van gegevens (de inhoud, de structuur en de relatie met andere gegevens), het standaardiseren, formaliseren, actualiseren en verbeteren van gegevens, de inrichting van een kwaliteitsproces en monitoren van en rapporteren over de gegevenskwaliteit. De informatie heeft de nodige diepgang en mate van detaillering en is tijdig beschikbaar. De kwaliteit en inzichtelijkheid moet zonder twijfel zijn. Om aanvullende analyses mogelijk te maken zijn de informatie-elementen te herleiden tot brongegevens. Bij voorkeur wordt gebruik gemaakt van databases waarin alle entiteiten, attributen en relaties worden samengevoegd waarbij als laatste stap de beoogde informatie hieruit wordt afgeleid.

5.1.15 De onderneming heeft op alle gewenste niveaus inzicht in de gang van zaken en de risico's van de bedrijfsonderdelen, ook in hun samenhang, dat nodig is om de bedrijfsprocessen en de risico's te beheersen.

Om adequate beheersing en bijsturing van de bedrijfsprocessen mogelijk te maken beschikt de onderneming op zijn minst over actueel, tijdig en volledig inzicht in alle ontwikkelingen, posities en risico's. Dit vraagt om goede samenwerking tussen de bedrijfsonderdelen die verantwoordelijk zijn voor de primaire bedrijfsprocessen (de gebruikers van de gegevens en informatie) en de bedrijfsonderdelen die de gegevens en informatie bewerken en aanleveren (zoals IT, afdelingsadministraties en de afdelingen controlling, risicomanagement en compliance).

5.1.16 De onderneming kan tijdig voldoen aan informatiebehoeften met informatie die aan de daaraan te stellen eisen voldoet.

De capaciteit en flexibiliteit van systemen en procedures maken het mogelijk dat met een aantal relatief eenvoudige handelingen aan reguliere maar ook ad hoc informatieverzoeken van de onderneming en derden, zoals toezichthouders, kan worden voldaan, zonder dat aan de kwaliteit concessies worden gedaan.

Drie verdedigingslinies

5.1.17 De onderneming toetst en beoordeelt systematisch de interne beheersing. Dit gebeurt door het lijnmanagement (eerste verdedigingslinie), bedrijfsonderdelen met als specifieke taak de adequate beheersing van risico's (monitoring en testen door risicobeheersing en de compliance-functie als tweede verdedigingslinie) en de interne auditfunctie (derde verdedigingslinie).

Het model met drie verdedigingslinies[26] is een breed geaccepteerd model om risicobeheersing en monitoring in te richten en taken en verantwoordelijkheden voor de risicobeheersing toe te wijzen. Dit model verankert de effectiviteit van de risicobeheersing. Het model is met name geschikt voor ondernemingen met een hoger risicoprofiel, zoals financiële ondernemingen.

5.1.18 Naast de reguliere hiërarchische rapportagelijnen, beschikken de tweede en de derde verdedigingslinies over functionele rapportagelijnen naar specifieke risicocomités, (de voorzitter van) het bestuur, de auditcommissie of de raad van commissarissen.

De effectiviteit van het functioneren van de tweede en de derde verdedigingslinie wordt vergroot wanneer zij de mogelijkheid hebben om ook direct te rapporteren aan de organen die verantwoordelijk zijn voor het toezicht op dagelijks beleid. Soms worden deze rapportagelijnen alleen ingericht als escalatielijn. Dat heeft niet de voorkeur omdat daarmee een drempel wordt opgeworpen om informatie te verschaffen.

Maatregelen voor noodsituaties

5.1.19 De onderneming beschikt over een bedrijfscontinuïteitsplan. Dit bedrijfscontinuïteitsplan wordt regelmatig getest.

Een bedrijfscontinuïteitsplan bevat maatregelen waarmee de bedrijfsvoering kan worden voortgezet wanneer deze door calamiteiten (niet beschikbaar zijn van personeel, bedrijfslocaties, nutsvoorzieningen, ICT, informatie, leveranciers, logistiek etc.) wordt bedreigd.

De onderneming besteedt in het bedrijfscontinuïteitsplan aandacht aan:
- Preventie;
- Alternatieve bedrijfsvoering;
- Verzekeringen.

Het bedrijfscontinuïteitsplan wordt regelmatig getest om de effectiviteit te toetsen en het bewustzijn bij de medewerkers op het gewenste niveau te houden.

5.1.20 De onderneming beschikt over een herstelplan.

Een herstelplan bevat maatregelen waarmee de onderneming, de bedrijfsvoering en de financiële positie worden verbeterd wanneer deze in noodsituaties zijn verslechterd.

5.1.21 De onderneming beschikt over een afwikkelingsplan.

Een afwikkelingsplan bevat maatregelen voor een ordelijke afwikkeling van de onderneming wanneer herstel onwaarschijnlijk is, teneinde de verliezen voor derden te minimaliseren.

5.2 Primaire bedrijfsprocessen

5.2.1 De onderneming beschikt over procedures en beheersingsmaatregelen die het ongestoord, betrouwbaar en integer functioneren van de bedrijfsprocessen waarborgen.

De eerste en belangrijkste waarborgen voor het ongestoord, betrouwbaar en integer functioneren van de bedrijfsprocessen worden in de zogenoemde lijnorganisatie getroffen. Daarbij worden de belangrijkste risico's in kaart gebracht en de maatregelen waarmee deze risico's worden gereduceerd. Het is primair de taak van de lijnorganisatie om risico te onderkennen, te signaleren, te monitoren en te beheersen[27].

5.2.2 De onderneming richt de procedures en beheersingsmaatregelen onder meer op het beheersen van de bedrijfsprocessen en de bedrijfsrisico's, het bewaken van de integriteit van medewerkers en klanten om te voorkomen dat het vertrouwen in de onderneming of in de sector wordt geschaad, en het zekerstellen van de soliditeit van de onderneming.

De beheersing gaat verder dan alleen de juiste operationele procesgang binnen de organisatie. Hiermee wordt tevens voorkomen dat de onderneming onverantwoorde posities of risico's inneemt, dat de onderneming of de bedrijfstak (reputatie)schade oploopt door ongewenst gedrag van medewerkers of ongewenste transacties door klanten of dat de rentabiliteit of de solvabiliteit van de onderneming op lange termijn wordt aangetast.

5.2.3 De onderneming maakt gebruik van autorisatieprocedures, limietstellingen en limietbewaking die zijn afgestemd op de aard, de omvang, het risicoprofiel en de complexiteit van de werkzaamheden van de onderneming.

De risico's kunnen onder meer worden beperkt door transacties en posities te laten autoriseren volgens een getrapte autorisatieprocedure, gebruik van limieten voor posities in bepaalde activa en uitzettingen op tegenpartijen, en bewaking van de naleving van deze maatregelen.

5.2.4 De onderneming toetst binnen de lijnorganisatie regelmatig de effectiviteit van de belangrijke beheersingsmaatregelen.

De eerste en belangrijkste waarborgen voor het ongestoord, betrouwbaar en integer functioneren van de bedrijfsprocessen worden in de lijnorganisatie getroffen. Daarom is het ook de verantwoordelijkheid van de lijnorganisatie om de effectiviteit van de belangrijke beheersingsmaatregelen regelmatig te toetsen. De tweede verdedigingslinie kan hierbij een faciliterende en monitorende rol vervullen. De uitkomsten van deze toetsing kunnen bijdragen aan de oordeelsvorming van het management en het bestuur ter onderbouwing van een 'in control statement', bijvoorbeeld in het kader van financiële verslaggeving.

5.2.5 Bij uitbesteding van werkzaamheden draagt de onderneming er zorg voor dat deze adequaat kunnen worden beheerst.

Uitbesteding van werkzaamheden mag niet leiden tot onacceptabele bedrijfsrisico's. De voorwaarden van uitbesteding, de verantwoordelijkheden van de betrokken partijen, de wijze waarop risico's worden beheerst en hoe hierover verantwoording wordt afgelegd, worden vastgelegd in een overeenkomst van dienstverlening. De onderneming blijft uiteindelijk verantwoordelijk voor de kwaliteit van de werkzaamheden die door de dienstverlener worden uitgevoerd en ziet hierop toe. Zo nodig wordt voorzien in de mogelijkheid voor de onderneming of haar toezichthouders om ter plaatse bij de dienstverlener onderzoek te doen.

5.2.6 De onderneming beschikt over een klachtenprocedure voor cliënten en relaties. De klachtenafhandeling is gescheiden van de afdelingen of medewerkers die het betreft. Het bestuur en de raad van commissarissen worden periodiek geïnformeerd door het meldpunt over het aantal en de aard van de klachten.

Een dergelijke klachtenprocedure draagt preventief en repressief bij aan de handhaving van ongestoorde, betrouwbare en integere bedrijfsvoering. Klachten worden tijdig en adequaat behandeld en onder de aandacht van het bestuur gebracht zodat zo nodig correctieve actie kan worden ondernomen. Dit kan bijstelling van procedures en maatregelen betreffen maar ook sancties die aan personen worden opgelegd.

5.3 Risicobeheerfunctie en compliance-functie

Risicobeheerfunctie

5.3.1 De onderneming beschikt over een onafhankelijke risicobeheerfunctie.

De risicobeheerfunctie is ten minste onafhankelijk van functies die verantwoording afleggen over de commerciële of financiële prestaties.

5.3.2 De risicobeheerfunctie bewaakt de effectieve werking van de risicobeheersing in de lijnorganisatie en adviseert over beleid om deze risicobeheersing te optimaliseren.

De risicobeheersing vindt primair in de lijnorganisatie plaats. De risicobeheerfunctie adviseert het bestuur beleidsmatig over de optimale inrichting van de risicobeheersing. De risicobeheerfunctie stelt de kaders voor de risicobeheersing en monitort of de risicobeheersing toereikend gebeurt.

5.3.3 De risicobeheerfunctie identificeert, meet en evalueert systematisch de risico's waaraan de onderneming wordt of kan worden blootgesteld. De risicobeheerfunctie houdt hierbij rekening met de risico's die voortvloeien uit de (macro-economische) omgeving waarin zij opereert.

De risico's waaraan de onderneming wordt blootgesteld zijn onder meer afhankelijk van de aard van de activiteiten, de omvang, de regionale spreiding en de jurisdicties waarin de onderneming werkzaam is. Deze risico's zijn niet statisch.

Risicocategorieën en aandachtsgebieden kunnen zijn:

- Strategisch (o.a. macro-economische ontwikkelingen, vergrijzing, opkomende markten, energieprijzen, consumentenvraag, markttoetreders, maatschappelijk verantwoord ondernemen);
- Financieel (o.a. liquiditeit, rentabiliteit, solvabiliteit, markt- en tegenpartijrisico, financieringskosten, toezichtvereisten);
- Operationeel (o.a. verstoring van processen door het falen van mensen of ICT-systemen, uitbesteding, juridische overeenkomsten, fraude, toegang tot gegevens en systemen, inbraak).

5.3.4 De risicobeheerfunctie rapporteert rechtstreeks aan het bestuurslid dat risicobeheersing in portefeuille heeft en de voorzitter van de raad van commissarissen of de voorzitter van de risicocommissie.

Het is belangrijk dat de risicobeheerfunctie voldoende onafhankelijk kan functioneren en dat de bevindingen en de conclusies van de risicobeheerfunctie aan het juiste niveau binnen de organisatie worden gerapporteerd zonder dat deze worden gefilterd en afgezwakt door het lijnmanagement. Daarom wordt de rapportagelijn aan de raad van commissarissen of de voorzitter van de risicocommissie niet alleen voor escalaties gebruikt.

5.3.5 De risicobeheerfunctie beschikt over een actueel mandaat waarin haar taken, bevoegdheden en verantwoordelijkheden beschreven zijn en een deskundigheidsniveau en vaardigheden die passen bij de risico's van de onderneming.

Het functioneren van de risicobeheerfunctie en de eisen die daaraan worden gesteld, worden stevig ingekaderd. Daarbij horen taakstellende eisen aan de ervaring, expertise en competenties van de medewerkers, de kwantitatieve en kwalitatieve bezetting van de functie en een daarop afgestemd budget. Het mandaat wordt periodiek, bij voorkeur jaarlijks, herzien op actualiteit.

5.3.6 De risicobeheerfunctie heeft onbelemmerde toegang tot alle relevante activiteiten, functionarissen, locaties en informatie van de onderneming.

De risicobeheerfunctie kan haar taken alleen adequaat uitoefenen wanneer zij onbelemmerd toegang heeft tot de activiteiten, functionarissen, locaties en informatie die daartoe benodigd is.

Compliance-functie

5.3.7 De ondernemingen beschikt over een onafhankelijke compliance-functie.

De compliance-functie is ten minste onafhankelijk van functies die verantwoording afleggen over de commerciële of financiële prestaties.

5.3.8 De compliance-functie bewaakt de effectieve werking van de beheersing van compliance-risico's in de lijnorganisatie en adviseert over beleid om deze beheersing te optimaliseren.

De beheersing van compliance-risico's vindt primair in de lijnorganisatie plaats. De compliance-functie adviseert het bestuur beleidsmatig over de optimale inrichting van de beheersing van compliance-risico's. De compliance-functie stelt de kaders voor de beheersing van compliance-risico's en monitort of dit toereikend gebeurt.

5.3.9 De compliance-functie identificeert, meet en evalueert systematisch de risico's van niet-naleving van wet- en regelgeving en (interne) gedragscodes.

De risico's waaraan de onderneming wordt blootgesteld zijn onder meer afhankelijk van de aard van de activiteiten, de omvang, de regionale spreiding en de jurisdicties waarin de onderneming werkzaam is. Deze risico's zijn niet statisch.

5.3.10 De compliance-functie rapporteert rechtstreeks aan het bestuurslid dat compliance in portefeuille heeft en de voorzitter van de raad van commissarissen of de desbetreffende commissie van de raad van commissarissen.

Het is belangrijk dat de compliance-functie voldoende onafhankelijk kan functioneren en dat de bevindingen en de conclusies van de compliance-functie aan het juiste niveau binnen de organisatie worden gerapporteerd zonder dat deze worden gefilterd en afgezwakt door het lijnmanagement. Daarom wordt de rapportagelijn aan de raad van commissarissen niet alleen voor escalaties gebruikt.

5.3.11 De compliance-functie beschikt over een actueel mandaat waarin haar taken, bevoegdheden en verantwoordelijkheden beschreven zijn en een deskundigheidsniveau en vaardigheden die passen bij de compliance-risico's van de onderneming.

Het functioneren van de compliance-functie en de eisen die daaraan worden gesteld, worden stevig ingekaderd. Daarbij horen taakstellende eisen aan de ervaring, expertise en competenties van de medewerkers, de kwantitatieve en kwalitatieve bezetting van de functie en een daarop afgestemd budget. Het mandaat wordt periodiek, bij voorkeur jaarlijks, herzien op actualiteit.

5.3.12 De compliance-functie heeft onbelemmerd toegang tot alle relevante activiteiten, functionarissen, locaties en informatie van de onderneming.

De compliance-functie kan haar taken alleen adequaat uitoefenen wanneer zij onbelemmerd toegang heeft tot de activiteiten, functionarissen, locaties en informatie die daartoe benodigd is.

5.4 Interne auditfunctie

5.4.1 De onderneming beschikt over een onafhankelijke interne auditfunctie die voldoet aan het normenkader van het Instituut van Internal Auditors Nederland en eisen van wet- en regelgeving en toezichthouders[28].

De term 'interne auditfunctie' betekent volgens de definitie van de IIA 'een onafhankelijke, objectieve functie die zekerheid verschaft en adviesopdrachten uitvoert, om meerwaarde te leveren en de operationele activiteiten van de organisatie te verbeteren. De interne auditfunctie helpt de organisatie haar doelstellingen te realiseren door met een systematische, gedisciplineerde aanpak de effectiviteit van de processen van risicomanagement, beheersing en governance te evalueren en te verbeteren.' Bij veel organisaties en bij onder toezicht staande ondernemingen is dit een reëel vereiste. Indien de interne auditfunctie ontbreekt, dienen bestuur en raad van commissarissen jaarlijks te evalueren of hieraan behoefte bestaat.

5.4.2 De interne auditfunctie toetst, in aanvulling op de werkzaamheden van de eerste en de tweede verdedigingslinie, de opzet, het bestaan en de werking van de ondernemingsbesturing, de organisatie-inrichting en de risicobeheersing, verstrekt hierover assurance en adviseert het bestuur en de raad van commissarissen of de auditcommissie over verbeteringen.

De interne auditfunctie verschaft het bestuur en het seniormanagement assurance op basis van het hoogste niveau van onafhankelijkheid en objectiviteit binnen de organisatie. De interne auditfunctie verstrekt assurance over de effectiviteit van de ondernemingsbesturing, de organisatie-inrichting en de risicobeheersing. De interne auditfunctie verstrekt bij voorkeur een oordeel over het object van onderzoek als geheel[29] en beperkt zich niet tot een opsomming van mogelijke verbeteringen. Dit omvat mede de wijze waarop de eerste en de tweede verdedigingslinie hun doelstellingen realiseren. De reikwijdte van de werkzaamheden rond de ondernemingsbesturing kan beperkt zijn tot de onderneming en het bestuur, waarbij de raad van commissarissen en de auditcommissie buiten beschouwing blijven.

5.4.3 De interne auditfunctie rapporteert rechtstreeks aan de voorzitter van het bestuur en de voorzitter van de raad van commissarissen of de voorzitter van de auditcommissie.

Het is belangrijk dat de interne auditfunctie volstrekt onafhankelijk kan functioneren, dat deze zelfstandig audits kan initiëren en dat de bevindingen en de conclusies van de interne

auditfunctie aan het juiste niveau binnen de organisatie worden gerapporteerd, zonder dat conclusies worden gefilterd en afgezwakt door het lijnmanagement. Daarom wordt de rapportagelijn aan de raad van commissarissen of de auditcommissie niet alleen voor escalaties gebruikt.

5.4.4 De interne auditfunctie beschikt over een actueel mandaat waarin haar taken, bevoegdheden en verantwoordelijkheden beschreven zijn en een deskundigheidsniveau en vaardigheden die passen bij de risico's van de onderneming. Dit mandaat is goedgekeurd door de raad van commissarissen of de auditcommissie.

Het functioneren van de interne auditfunctie en de eisen die daaraan worden gesteld, worden stevig ingekaderd. Daarbij horen taakstellende eisen aan de ervaring, expertise en competenties van de medewerkers, de kwantitatieve en kwalitatieve bezetting van de functie en een daarop afgestemd budget. Het mandaat wordt periodiek, bij voorkeur jaarlijks, herzien op actualiteit.

5.4.5 De interne auditfunctie heeft onbelemmerde toegang tot alle relevante activiteiten, functionarissen, locaties en informatie van de onderneming.

De interne auditfunctie kan haar taken alleen adequaat uitoefenen wanneer zij onbelemmerd toegang heeft tot de activiteiten, functionarissen, locaties en informatie die daartoe benodigd is.

5.4.6 De interne auditfunctie stelt een risicoanalyse op voor het gehele object van audit en een daaruit afgeleid auditplan, stemt deze af met de externe accountant en legt deze jaarlijks ter afstemming voor aan het bestuur en ter goedkeuring aan de raad van commissarissen of de auditcommissie.

De afstemming van de risicoanalyse en het auditplan met de externe accountant kan bijdragen aan de kwaliteit ervan. De interne auditfunctie functioneert primair ten behoeve van het bestuur en de raad van commissarissen of de auditcommissie. De raad van commissarissen of de auditcommissie speelt een belangrijke rol bij het beoordelen en accorderen van het functioneren van de interne auditfunctie. Om deze redenen zijn het bestuur en de raad van commissarissen of de auditcommissie nauw betrokken bij de afstemming, de beoordeling en de goedkeuring van de risicoanalyse en het auditplan van de interne auditfunctie.

5.4.7 De interne auditfunctie voert het auditplan uit, doet op basis van de werkzaamheden aanbevelingen aan het bestuur en stelt vast of aan deze aanbevelingen gevolg wordt gegeven.

De interne auditfunctie toetst de realiteit aan de normen die de onderneming zichzelf heeft gesteld of die de interne auditfunctie, zo nodig in overleg met de onderneming, bepaalt als toetsingskader. Daaruit vloeien bevindingen en aanbevelingen voort voor verbetering van

de ondernemingsbesturing, de organisatie-inrichting en de risicobeheersing. Deze kunnen variëren van waardevolle maar niet-noodzakelijke suggesties tot aanbevelingen waarvan het belangrijk is dat deze onverwijld worden overgenomen en worden doorgevoerd. De interne auditfunctie ziet erop toe dat hiernaar gehandeld wordt door het bestuur en informeert de raad van commissarissen of de auditcommissie hierover. De afwikkeling van de aanbevelingen wordt door de interne auditfunctie periodiek gemonitord en gerapporteerd aan het bestuur en de raad van commissarissen of de auditcommissie.

5.4.8 De interne auditfunctie rapporteert ten minste per kwartaal en ten minste jaarlijks in samengevatte vorm aan de raad van commissarissen of de auditcommissie over haar werkzaamheden, de aanbevelingen aan het bestuur en of aan deze aanbevelingen gevolg is gegeven.

Zo nodig brengt de interne auditfunctie met hogere frequentie informatie onder de aandacht van de raad van commissarissen of de auditcommissie. De interne auditfunctie woont de vergaderingen van de raad van commissarissen of de auditcommissie (ten dele) bij om toelichting te geven op de rapporten en om vragen van de commissarissen te beantwoorden. De raad van commissarissen of de auditcommissie bespreekt periodiek de werkzaamheden van de interne auditfunctie en de aanbevelingen aan het bestuur met de interne auditfunctie zonder dat het bestuur daarbij aanwezig is.

6. Verantwoording

6.1 De onderneming komt op passende en inzichtelijke wijze tegemoet aan de informatiebehoefte van de maatschappelijke omgeving, cliënten, zakelijke relaties, personeel, vermogensverschaffers en toezichthouders.

Een deel van deze informatiebehoefte en de verantwoording daarover is niet gecodificeerd of in voorschriften of regels vastgelegd. Het is de verantwoordelijkheid van de onderneming om niettemin op gepaste wijze te voorzien in de informatiebehoefte van betrokkenen op de volgende aandachtsgebieden:

- De strategie;
- Het bedrijfs- en verdienmodel;
- De behartiging van het klantbelang;
- De ondernemingsbesturing en naleving van codes;
- Het beloningsbeleid;
- De bedrijfsrisico's en de risicobeheersing;
- De continuïteit;
- Naleving van wet- en regelgeving;
- Voldoen aan toezichtvereisten;
- Maatschappelijk verantwoord ondernemen.

Voetnoten

1. Hiermee wordt bedoeld een organisatorisch verband met of zonder rechtspersoonlijkheid, gericht op duurzame deelname aan het economisch verkeer met behulp van arbeid en kapitaal en met het oogmerk om winst te behalen.

2. Deze beginselen zijn in grote lijnen gebaseerd op algemeen aanvaarde beginselen voor de kwaliteit van het ondernemingsbestuur, het risicobeheer en de beheersprocessen, waaronder:
   - The Principles of Corporate Governance - Organisation for Economic Co-operation and Development;
   - Internal Control Framework - Committee of Sponsoring Organizations of the Treadway Commission;
   - De Nederlandse Corporate Governance Code;
   - Enhancing corporate governance for banking organisations - Basel Committee on Banking Supervision;
   - Guidelines on Internal Governance - European Banking Authority;
   - The internal audit function in banks - Basel Committee on Banking Supervision;
   - De Wft en lagere regelgeving; en
   - De Code Banken en de Governance Principes voor verzekeraars.

3. Bijvoorbeeld het personeelsbeleid, de IT-architectuur, het kantorennet, de marketing etc.

4. 'Maatschappelijk verantwoord ondernemen', 'corporate social responsibility'.

5. 'Klantbelang centraal'.

6. Crediteuren, banken, andere financiers, aandeelhouders.

7. De periodiciteit is afhankelijk van individuele omstandigheden maar het is doorgaans wenselijk om dit ten minste jaarlijks te doen.

8. Onder meer de zogenoemde drie verdedigingslinies die hierna worden behandeld.

9. 'In control statement'.

10. De CFO en de CRO mogen geen commerciële verantwoordelijkheden hebben. Soortgelijke overwegingen spelen een rol bij de besluitvorming over commissariaten bij groepsmaatschappijen.

11. De raad van commissarissen beschikt over ervaring en expertise op onder meer de volgende aandachtsgebieden:
    - Bestuur, organisatie, communicatie;
    - Producten, diensten en markten van de onderneming;
    - Beheerste en integere bedrijfsvoering, risicobeheersing;
    - Financiële informatie en verantwoording;
    - Evenwichtige en consistente besluitvorming.

12. De noodzaak van benoeming van commissies voor specifieke aandachtsgebieden is mede afhankelijk van de omvang en de complexiteit van de organisatie en haar activiteiten. Commissies kunnen worden samengevoegd wanneer de omvang en de complexiteit van de organisatie en haar activiteiten dat toestaan.

13. De corporate governance-commissie heeft als aandachtsgebieden het toezicht op en de evaluatie van de ondernemingsbesturing als geheel en de rapportage daarover in het jaarverslag en aan de algemene vergadering van aandeelhouders, en adviseert de raad van commissarissen over verbeteringen.

14. De auditcommissie heeft als aandachtsgebieden de administratieve organisatie en interne beheersing, ICT, interne audit en de (controle van de) financiële verslaggeving. De auditcommissie vervult een specifieke rol bij de benoeming, de beoordeling en het ontslag van de leiding van de interne auditfunctie en de benoeming (advies aan de aandeelhouders) en de bezoldiging van de accountant.

15. De risicocommissie heeft als aandachtsgebieden de risicobereidheid, het risicoprofiel, de (systemen voor) risicobeheersing, risicorapportages en externe verslagging over risico's en risicobeheersing.

16. De benoemingscommissie heeft als aandachtsgebieden de selectie en benoeming van bestuurders en commissarissen, het toezicht op benoeming door het bestuur van hoger management, de beoordeling van de omvang en de samenstelling van het bestuur en de raad van commissarissen en de beoordeling van het functioneren van het bestuur als geheel en de raad van commissarissen als geheel.

17. De beloningscommissie heeft als aandachtsgebieden voorstellen voor het beloningsbeleid voor de bestuurders, toezicht op het door het bestuur gevoerde beloningsbeleid, de beoordeling van het functioneren van individuele bestuurders en de beloning van individuele bestuurders.

18. In de praktijk komt dikwijls een intern meldpunt of vertrouwenspersoon voor en een extern meldpunt voor delicate onderwerpen als een klokkenluidersregeling.

19. Bijvoorbeeld verstrekken van opdrachten, aangaan van verplichtingen, goedkeuren van transacties, verlenen van kwijting.

20. Bijvoorbeeld opslag en bewaring van waardepapieren en geldmiddelen maar ook debiteurenbewaking.

21. Bijvoorbeeld afdelingscontrole, verbijzonderde interne controle, de afdeling controlling.

22. Bijvoorbeeld vastlegging van transacties door dealing room, boekhouding, debiteurenadministratie.

23. Bijvoorbeeld planning, facturering, verwerking van betalingen.

24. ICT kan ook van groot strategisch belang zijn voor ondernemingen omdat hun concurrentievoordeel hierop is gebaseerd. Sommige bedrijven opereren in een netwerk of keten met

andere bedrijven waarbij de samenwerking op basis van ICT van belang is. Kleine bedrijven zien ICT steeds meer als commodity zonder de beheersmaatregelen expliciet aan de orde te stellen.

25. Zie ook: Control Objectives for Information and related Technology (COBIT-framework)

26. Zie IIA (Global) Position Paper: The three lines of defense in effective risk management and control, January 2013.

27. Zie ook: Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management - Integrated Framework (COSO-ERM)

28. Voor onder toezicht staande financiële ondernemingen stelt de toezichtwetgeving (Wet op het financieel toezicht en lagere regelgeving) eisen aan de interne auditfunctie. De Nederlandsche Bank hanteert de principes van het Bazelse Comité voor het Toezicht op Banken voor interne auditors bij banken als norm. Ook gedragscodes kunnen vereisten voor de interne auditfunctie bevatten.

29. Niet wanneer zogenoemde 'overeengekomen specifieke werkzaamheden' worden uitgevoerd.