Versteviging van risicomanagement in het perspectief van de herziening van de Nederlandse Corporate Governance Code

Mr. H. Koster *

In dit artikel gaat de auteur in op de voorgestelde wijzigingen van de Nederlandse Corporate Governance Code op het terrein van risicomanagement. De auteur is positief over de voorgestelde wijzigingen. Wel zijn nog enkele verbeteringen mogelijk.

1 Inleiding

Op 11 februari 2016 heeft de Monitoring Commissie Corporate Governance Code (hierna: de Commissie) een consultatiedocument (hierna: het consultatiedocument) met voorstellen voor herziening van de Nederlandse Corporate Governance Code (hierna: de Code) gepubliceerd.[1] De consultatieperiode bedroeg acht weken en liep tot 6 april 2016. De bedoeling is dat nog in 2016 een aangepaste Code wordt vastgesteld en aan het kabinet wordt verzonden, met het verzoek om de aangepaste Code wettelijk te verankeren. In dat geval zou de Code vanaf het boekjaar beginnend op of na 1 januari 2017 in werking treden. Bij het opstellen van de herzieningsvoorstellen is onder andere rekening gehouden met de suggesties afkomstig van de betrokken partijen en andere belanghebbenden. Verder zijn relevante actuele nationale en internationale ontwikkelingen waar mogelijk meegenomen. Ten slotte zijn er bij overlap of strijdigheid met wet- en regelgeving principes en best practice bepalingen geheel of gedeeltelijk geschrapt. In het consultatiedocument worden onder meer diverse wijzigingen voorgesteld op het terrein van risicomanagement. In dit artikel bespreek ik de voorstellen op dit laatstgenoemde terrein. Ik sluit af met enkele conclusies.

2 Enkele algemene lijnen en ontwikkelingen

In het kader van corporate governance is er de laatste jaren steeds meer aandacht voor risicomanagement. In het consultatiedocument is er ook meer attentie voor langetermijnwaardecreatie en cultuur.[2] Voor beide is risicomanagement van belang. Over langetermijnwaardecreatie wordt voorgesteld om vast te leggen in principe 1.1 dat het bestuur verantwoordelijk is voor de continuïteit van de vennootschap en de met haar verbonden onderneming en zich richt op de langetermijnwaardecreatie van de vennootschap en de met haar verbonden onderneming.[3] Voor langetermijnwaardecreatie is een goed risicomanagement van groot belang. Afwezigheid van goed risicomanagement kan allerlei negatieve effecten hebben en bijvoorbeeld tot reputatieschade leiden. Ik citeer een voorbeeld uit de Financial Times:

> 'Two reports into what went wrong with SocGen's internal controls painted a damning picture of weak procedures, poor implementation and bad management.'[4]

Voor het bestuur en de raad van commissarissen betekent de focus op langetermijnwaardecreatie, zo lees ik in het consultatiedocument, dat zij zich bij de uitoefening van de hun toebedeelde taken dienen te richten op langetermijnwaardecreatie en daarbij aandacht te hebben voor kansen en risico's, en in dat kader de belangen van alle bij de vennootschap betrokken stakeholders dienen mee te wegen. Wat cultuur betreft is de Commissie van mening dat de Code hier nadrukkelijker aandacht aan moet besteden. Cultuur speelt volgens de Commissie een belangrijke rol bij het functioneren van de onderneming en de mate waarin zij bijdraagt aan de langetermijnwaardecreatie van de vennootschap en de met haar verbonden

* Mr. H. Koster is verbonden aan het Departement Rechtsgeleerdheid van de Universiteit Utrecht.

1. Het consultatierapport met voorstellen voor herziening van de Code is te vinden op de website van de Commissie.
2. Zie hierover ook F.G.K. Overkleeft & J.H.L. Beckers, Het consultatievoorstel voor een herziene code en langetermijnwaardecreatie: alleen 'jam tomorrow' of ook 'jam today'?, MvO 2016, afl. 3, p. 43-46.
3. De term langetermijnwaardecreatie lijkt verwantschap te hebben met het door de Hoge Raad in zijn Cancun-uitspraak gegeven criterium: 'Indien aan de vennootschap een onderneming is verbonden, wordt het vennootschapsbelang in de regel vooral bepaald door het bevorderen van het bestendige succes van deze onderneming.' Zie HR 4 april 2014, NJ 2014/286.
4. Zie H. Weitzman, Hunt is stepped up for the rogue traders, Financial Times 20 oktober 2008.

 doi: 10.5553/MvO/245231352016001101002

onderneming.[5] In dit kader zijn het enkel opstellen van interne regels en het inrichten van reguliere controle op naleving onvoldoende.[6] Het bestuur en de raad van commissarissen worden geacht op een actieve en betrokken wijze invulling te geven aan het implementeren en stimuleren van een cultuur van openheid en aanspreekbaarheid binnen de aan de vennootschap verbonden onderneming.[7] Er wordt bijvoorbeeld voorgesteld om in best practice bepaling 2.5.2 op te nemen dat het bestuur de voorzitter van de raad van commissarissen informeert over signalen en (vermoedens van) materiële misstanden. Het is belangrijk dat mensen de weg weten te vinden om misstanden aan de kaak te stellen en zich voldoende comfortabel voelen om dat te doen.[8] De Nederlandsche Bank heeft eerder zeven elementen genoemd die leidend zijn voor een integere cultuur: belangenafweging/evenwichtig handelen, consistent handelen, bespreekbaarheid, voorbeeldgedrag, uitvoerbaarheid, handhaving en transparantie.[9] Zoals hiervoor aangestipt, is risicomanagement voor zowel langetermijnwaardecreatie als cultuur van belang. Wel dient men te beseffen dat ook het beste risicomanagementsysteem niet kan voorkomen dat er geen fraude en ander onwenselijk gedrag plaatsvinden.[10] Ook is van belang, zoals Blom het treffend formuleerde:

> 'Verwacht niet te veel van regels. (...) Cultuurveranderingen worden niet door regels bewerkstelligd, maar door de overtuiging dat men op een andere manier moet werken.'[11]

Om risicozoekend gedrag in de hand te houden zijn vooral cultuur en de 'toon aan de top' van belang. Aan regels en controlemechanismen evenals de bepaling van de risicobereidheid komt hierbij een ondersteunende rol toe. De echte uitdaging is om de regels en controlemechanismen te laten leven, waardoor deze meer worden dan afvinkvereisten waaraan voldaan moet worden. In dit kader is ook van belang dat het gedrag van mensen wordt beïnvloed door gedragsmatige biases. Dit wordt ook wel aangeduid als 'cognitieve bias' of 'denkfout'. Een denkfout is een gedragsafwijking in de beoordeling, waarbij conclusies over andere mensen of situaties op een onlogische manier worden getrokken. Individuen creëren hun eigen subjectieve sociale realiteit, met behulp van hun eigen waarneming.[12] In het kader van risicomanagement is van belang dat bij managers sprake kan zijn van een bepaalde mate van overmoedigheid.[13] Overmoed kan zich op verschillende wijzen uiten, zoals door het 'beter dan gemiddeld' gevoel, de neiging om successen als een beoogd gevolg van het eigen handelen aan te merken en mislukkingen als pech waar niemand iets aan kan doen. Daarnaast noem ik de illusie van controle en onrealistisch optimisme.[14] De bias kan toenemen als de taak moeilijker is en er geen directe signalen zijn die bevestigen dat de genomen beslissing juist is of niet.[15] Ook is van belang dat personen elkaar kunnen beïnvloeden, waardoor een standpunt wordt opgegeven,[16] immers 'fighting groupthink is a lonely place'.[17] Een bias hoeft overigens niet te betekenen dat sprake is van niet-integer handelen, zoals het geval is bij handelen dat wordt beïnvloed door een kortetermijnbonusdoelstelling, ijdelheid of *peer pressure*.[18] Bij risicomanagers, interne auditors, compliancemanagers en de externe accountant zou er daarom meer aandacht moeten komen voor cultuur en biases. Dat geldt overigens ook voor commissarissen en bestuurders. Het is belangrijk om de betrokken personen bewust te maken van het belang van deze aspecten.[19] Zelfevaluatie, training en extern kritisch onderzoek naar de beoordelings- en besluitvormingsstructuur kunnen hierbij behulpzaam zijn. Daarnaast kunnen een effectief diversiteitsbeleid en het benoemen van managers van buiten hierbij ook helpen. Dit alles is ook van belang voor goed risicomanagement. Voor een goed risicomanagement zijn voorts de interne audit-, risicomanagement- en compliancefunctie van belang. In de volgende paragraaf ga ik nader in op deze functies.

3 De interne audit-, risicomanagement- en compliancefunctie

Over de taak van de interne auditfunctie bestaat (nog) geen duidelijk beeld. In de praktijk bepaalt de organisatie het takenpakket van de interne auditfunctie. In de huidige Nederlandse Corporate Governance Code is bepaald dat de interne auditfunctie verantwoording aflegt aan het bestuur. Het lijkt in dat kader dan wenselijk dat de interne auditfunctie rechtstreeks aan de voorzitter van het bestuur rapporteert en met name

5. Zie het consultatiedocument, p. 37.
6. Zie het consultatiedocument, p. 37.
7. Zie het consultatiedocument, p. 37.
8. Zie het consultatiedocument, p. 38.
9. DNB, De 7 elementen van een integere cultuur. Beleidsvisie en aanpak gedrag en cultuur bij financiële ondernemingen 2010-2014, 2009.
10. In het onderzoeksrapport over Barclays wordt opgemerkt: 'Good governance increases the possibility that good decisions will be made, but it does not make it certain that all decisions will be good ones.' Zie A. Salz, The Salz review: An independent review of Barclays' business practices, 3 april 2013, p. 100-101.
11. Kamerstukken II 2010/11, 31980/32013, 17, p. 6.
12. Zie H. Bless, K. Fiedler & F. Strack, Social cognition: How individuals construct social reality, Hove/New York: Psychology Press 2004, p. 2.
13. Zie L.F. Ackert & R. Deaves, Behavioral finance. Psychology, decision-making and markets, Mason, OH: South-Western, Cengage Learning 2010.
14. U. Malmendier & G. Tate, Does overconfidence affect corporate investment? CEO overconfidence measures revisited, European Financial Management (11) 2005, afl. 5, p. 650-651.
15. D.A. Moore & T.G. Kim, Myopic social prediction and the solo comparison effect, Journal of Personality and Social Psychology (85) 2003, afl. 6, p. 1131-1133.
16. Moore & Kim 2003.
17. Citaat van VS Senator Edmond G. Ross.
18. Bij de recente Volkswagenkwestie lijkt bijv. sprake te zijn geweest van het opleggen van onhaalbare doelen, waardoor men koos voor het schrijven van software om de zaken anders – insidercyberfraude – dan in overeenstemming met de werkelijkheid voor te wenden. In mei 2005 hadden VW-technici aan senior VW-managers laten weten: '[I]t will be impossible [for EA 189 engine; HK] to comply with US [Nox; HK] emissions standards using [VW's; HK] current technology.'
19. H. Shefrin, Ending the management illusion. How to drive business results using the principles of behavioral finance, New York: McGraw-Hill 2008.

niet aan de Chief Financial Officer.[20] In de volgende paragraaf zal ik overigens verdedigen dat de interne auditfunctie onder de auditcommissie zou moeten vallen. De externe accountant en de auditcommissie worden betrokken bij het opstellen van het werkplan van de interne auditor en nemen kennis van de bevindingen van de interne auditor. Interne auditors zijn verantwoordelijk voor het uitvoeren van onderzoeken of 'audits'.[21] Eind jaren dertig van de vorige eeuw waren in Nederland Philips Gloeilampenfabrieken NV en de Nederlandse Spoorwegen de eerste bedrijven die een interne auditfunctie kenden. De primaire taak was destijds het verrichten van een financiële audit.[22] Een dergelijke audit richt zich op de betrouwbaarheid van de financiële verslaglegging. Een belangrijke stap voor interne audit was de oprichting van het Institute of Internal Auditors (hierna: IIA) in de Verenigd Staten in 1941. Volgens de IIA is interne audit:

> 'An independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.'[23]

In het eerste rapport van de Nederlandse IIA-afdeling wordt gewezen op de verschuiving van financiële audits naar operationele audits.[24] Een andere belangrijke organisatie is de Internationale Organisatie voor Standaardisatie (hierna: ISO). Dit is een samenwerkingsverband tussen nationale standaardenorganisaties. De ISO-organisatie ontwikkelt en publiceert normen zoals de ISO 31000 richtlijn voor risicobeheersing en de ISO 19600 richtlijn voor compliancemanagement.[25] Een andere relevante organisatie is het Committee of Sponsoring Organizations of the Treadway Commission (hierna: COSO). COSO gaat onder meer in zijn *guidance* in op het 'three lines of defense'-model, waarmee de buitenwereld kan worden getoond dat de onderneming 'in control' is.[26] De eerste lijn is het bestuur, dat in eerste instantie de verantwoordelijkheid draagt voor risicobeheersing.[27] De tweede lijn betreft de functie in de organisatie die naleving van regels controleert en het risicoraamwerk opzet en uitvoert. Hierbij kan worden gedacht aan de compliance officers en de risicomanagers. De interne audit vormt de derde lijn.

De compliancefunctie ziet erop toe dat de wetten, reglementen en gedragsregels worden nageleefd.[28] Compliance gaat over de identificatie van de risico's die kunnen ontstaan wanneer niet wordt voldaan aan compliancevereisten in relatie tot de activiteiten, producten en diensten. De aldus geïdentificeerde risico's worden afgezet tegen en getoetst aan de tevoren vastgestelde risicobereidheid (*risk appetite*). Dit betreft overigens geen eenmalig proces. Het is per definitie dynamisch. Door de toename van de extraterritoriale werking van wet- en regelgeving is compliance de laatste jaren in belang toegenomen.[29] In de praktijk lijkt er daarbij een trend te bestaan waarbij compliance steeds meer gericht is op dossiervorming. Dit ook als reactie op onder meer Amerikaanse en Britse regels waarbij veel waarde wordt toegekend aan een goed werkend compliancesysteem.[30] Van belang is uiteraard dat naast dossiervorming de nadruk moet liggen op het creëren van een integere cultuur. De laatste jaren ontstaat voorts steeds meer een tendens dat in veel van de belangrijke markten voor Nederlandse multinationals wordt verwacht dat bedrijven beschikken over een effectief complianceprogramma. Onderdeel hiervan is nogal eens dat zij hun zakenpartners en 'third party agents' aan due diligence-onderzoek dienen te onderwerpen en complianceclausules opnemen in hun contracten.

Risicomanagement ten slotte is de functie die gaat over de tenuitvoerlegging van het risicobeheersysteem. Dit is het geheel van strategieën, processen en procedures die nodig zijn voor de opvolging van de risico's of combinaties van risico's waaraan de instelling is blootgesteld of blootgesteld zou kunnen zijn, met uitzondering van het compliancerisico.[31]

20. Zo ook J. Strikwerda, De Nederlandse Corporate Governance Code, Assen: Van Gorcum 2012, p. 200.
21. Zie L.P.L. de Bruijn, De juridische positie van de internal auditor in Nederland (diss. Rotterdam), 2010.
22. A. Goudeket, De interne accountant, Maandblad voor Accountancy en Bedrijfseconomie, mei 1956.
23. Zie website IIA.
24. Zie hierover W.H.A. Swinkels, Exploration of a theory of internal audit (diss. Amsterdam UvA), 2012.
25. Zie hierover C.J.L. De Wannemaeker, De nieuwe ISO-compliancerichtlijn: een geïntegreerde benadering van compliance stevig verankerd in de nieuwste ISO-managementsystematiek, TvCo, december 2014.
26. Zie over het model IIA Position Paper, The three lines of defense in effective risk management and control, 2013. Zie hierover ook W.J. Pauw, Governance is mensenwerk, TvCo, december 2014.
27. Zie ook C.F. van der Elst, The risk management duties of the board of directors, <www.ssrn.com>.
28. Zie over compliance ook S.J. Griffith, Corporate governance in an era of compliance, <www.ssrn.com>. Zij schrijft: 'Compliance is the new corporate governance. The compliance function is the means by which firms adapt behavior to legal, regulatory, and social norms. Formerly, this might have been conceived as a typical governance matter to be handled at the discretion of the board of directors. Compliance, however, does not fit traditional models of corporate governance. It does not come from the board of directors, state corporate law, or federal securities law. Compliance amounts instead to an internal governance structure imposed upon the firm from the outside by enforcement agents. This insight has important implications, both practical and theoretical, for corporate law and corporate governance.'
29. Zie ook M.M.A. van Daelen & W.H.A. Swinkels, Compliance in de corporate sector: volop in beweging!, TvCo, oktober 2013.
30. Op grond van art. 7 van de Engelse Bribery Act 2010 kunnen bedrijven ook worden vervolgd voor omkoping, tenzij het bedrijf 'had in place adequate procedures designed to prevent persons associated with the commercial organisation from undertaking such conduct'. In Duitsland is het bestuur van Siemens AG succesvol aansprakelijk gesteld wegens 'Einrichtung eines mangelhaften Compliance-Systems zur Verhinderung von Schmiergeldzahlungen' (LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10).
31. Zie Circulaire FSMA-2013-08 van 23 april 2013.

 doi: 10.5553/MvO/245231352016001101002

Er is de nodige regelgeving op dit terrein.[32] Zo is in de aanbeveling van de Europese Commissie van 15 februari 2005 (2005/162/EG)[33] opgenomen dat de auditcommissie de raad van bestuur/raad van commissarissen bij dient te staan bij de beoordeling, ten minste eenmaal per jaar, van de interne controle- en risicobeheersystemen om ervoor te zorgen dat de voornaamste risico's (waaronder risico's in verband met de naleving van de vigerende wetgeving en voorschriften) naar behoren worden onderkend, beheerd en openbaar gemaakt. Dat geldt ook voor het waarborgen van de efficiëntie van de interne auditfunctie, met name door aanbevelingen te doen betreffende de selectie, benoeming, herbenoeming en het ontslag van het hoofd van de interne auditafdeling en betreffende het budget van deze afdeling, en door de reactie van het bestuur op zijn bevindingen en aanbevelingen te toetsen. Daarnaast volgt uit artikel 19 van Richtlijn 2013/34/EU[34] dat het bestuursverslag een getrouw overzicht geeft van de ontwikkeling en de resultaten van de bedrijfsactiviteit en van de positie van de onderneming, alsmede een beschrijving van de voornaamste risico's en onzekerheden waarmee zij geconfronteerd wordt. Voorts is op grond van artikel 20 van deze richtlijn een beschrijving vereist van de belangrijkste kenmerken van de interne controle- en risicobeheersystemen van de onderneming in verband met het proces van financiële verslaggeving.

In de praktijk kan er dus naast de interne auditfunctie een risicomanagementfunctie zijn evenals een compliancefunctie. Deze functies zullen geregeld moeten samenwerken, maar er zijn grenzen, bijvoorbeeld als de interne auditfunctie een oordeel moet geven over de kwaliteit van risicomanagementprocessen en *assurance* moet verschaffen aan het management dat risico's correct worden geëvalueerd. Ook is verdedigd dat compliance en risicomanagement gescheiden afdelingen moeten zijn.[35] Een argument tegen samenvoeging is dat moet worden voorkomen dat compliancerisico's minder belangrijk worden gevonden dan andere risico's. Uiteraard moet er waar mogelijk sprake zijn van afstemming tussen en samenwerking van de compliancefunctie met de risicomanagementfunctie en de interne auditfunctie. Maar een andere visie, te weten integratie van risicomanagement en compliance, is eveneens verdedigd.[36] In de literatuur is verder verdedigd dat de verantwoordelijkheid voor de compliancefunctie bij het bestuur moet liggen.[37] Dat lijkt ook voor het risicomanagement te gelden.[38] Daarnaast komt een rechtstreekse rapportagelijn met de auditcommissie voor.[39] Voorts zou kunnen worden verdedigd dat de compliancefunctie aan de risicomanagementfunctie moet rapporteren. Dit omdat compliance een van de vier risicodimensies is, naast de strategische, operationele en rapportagerisico's. In de praktijk is de compliancefunctie soms onderdeel van juridische zaken. Het is overigens de vraag of dit wenselijk is. Verder wordt compliance ook gecombineerd met ethiek.[40] Ik sluit deze paragraaf af met de conclusie dat de rol, vormgeving en onderlinge afbakening van de interne audit-, risicomanagement- en compliancefunctie nog niet (volledig) is uitgekristalliseerd.[41] In de volgende paragraaf licht ik toe hoe dit mijns inziens vormgegeven kan worden.

4 De voorstellen voor het verstevigen van risicomanagement

Voor risicomanagement is een goed samenspel tussen het bestuur, de raad van commissarissen en de auditcommissie van belang. Ook de interne auditfunctie, risicomanagementfunctie, compliancefunctie en de externe accountant vervullen hierbij een belangrijke rol.[42] Voor aandeelhouders is het volgens de Commissie van belang dat zij een redelijke mate van inzicht verkrijgen in de opzet en werking van de interne risicobeheersings- en controlesystemen.[43] In principe 1.2 van het voorstel wordt als kernbeginsel vastgelegd dat de vennootschap over adequate interne risicobeheersings- en controlesystemen dient te beschikken. Het bestuur is verantwoordelijk voor het vaststellen van de risicobereidheid en het beheersen van de risico's verbonden aan de strategie en de activiteiten van de vennootschap. Het ligt daarom voor de hand dat de risicomanagement- en compliancefunctie onder verantwoordelijkheid van het bestuur vallen. Van belang voor risicomanagement zijn verder risicoassessment, implementatie en evaluatie. Zoals besproken in paragraaf 2 heeft risicomanagement

32. Zie ook C.F. van der Elst & M.M.A. van Daelen, Risk management in European and American corporate law, <www.ssrn.com>.
33. Aanbeveling betreffende de taak van niet bij het dagelijks bestuur betrokken bestuurders of commissarissen van beursgenoteerde ondernemingen en betreffende de comités van de raad van bestuur of van de raad van commissarissen.
34. Richtlijn betreffende de jaarlijkse financiële overzichten, geconsolideerde financiële overzichten en aanverwante verslagen van bepaalde ondernemingsvormen, tot wijziging van Richtlijn 2006/43/EG van het Europees Parlement en de Raad en tot intrekking van Richtlijnen 78/660/EEG en 83/349/EEG van de Raad.
35. Zie J. van Vulpen & A. Morée, Compliance & risk management – samenwerken of samenvoegen?, TvCo, december 2014 en W. Lieve, Compliance & risk management: living apart together, TvCo, december 2014.
36. Zie S.N. Heidema & W.H.A. Swinkels, compliance en risicomanagement: hoog tijd om te integreren, TvCo, december 2014.
37. Zie A.J.J.P.B.M. Kersten, Compliance at banks, company law and financial markets law observations on whether the law sheds adequate light on ownership (diss. Rotterdam), 2014, p. 39-40.
38. Zie Van Vulpen & Morée 2014.
39. Zie Van Daelen & Swinkels 2013.
40. Zie S.W.B. Boerma & W. Lieve, Het portret: interview met Carlos Desmet, compliance officer bij Royal Dutch Shell, TvCo, oktober 2013.
41. Zie hierover ook G.P. Miller, The law of governance, risk management and compliance, New York: Wolters Kluwer 2014, p. 107.
42. Zo houdt de voorgestelde best practice bepaling 1.5.5 in dat de raad van commissarissen onverwijld wordt geïnformeerd door het bestuur en de externe accountant over materiële onregelmatigheden binnen de vennootschap, waaronder begrepen onregelmatigheden met betrekking tot de integriteit van de financiële verslaggeving. De raad van commissarissen houdt toezicht op proportioneel en onafhankelijk onderzoek naar de geconstateerde onregelmatigheden en een adequate opvolging van eventuele aanbevelingen tot herstelacties. Om de onafhankelijkheid van het onderzoek te borgen heeft de raad van commissarissen de mogelijkheid om zelf een onderzoek te initiëren naar geconstateerde onregelmatigheden en dit onderzoek aan te sturen. Daarnaast is de auditcommissie het eerste aanspreekpunt voor de externe accountant wanneer deze onregelmatigheden constateert bij de uitvoering van zijn opdracht (best practice bepaling 1.7.5).
43. Zie consultatiedocument, p. 11.

ook een link met de twee nieuwe kernwaarden in de voorgestelde Code, langetermijnwaardecreatie en cultuur. Ik denk dat het aanbeveling verdient om deze relatie meer expliciet te verwoorden in de Code. Zo zou aan best practice bepaling 1.1.1 over visie en strategie voor langetermijnwaardecreatie kunnen worden toegevoegd dat daarbij ook aandacht besteed moet worden aan risicomanagement. Voor cultuur zou in best practice bepaling 2.5.3 kunnen worden toegevoegd dat het bestuur: 'vi. [zich ervan] vergewist (...) dat cultuur als kernwaarde wordt ingepast in het risicomanagement van de vennootschap'.

Daarnaast wordt in het consultatiedocument de positie van de interne auditfunctie verstevigd, onder meer door een intensivering van de betrokkenheid van de auditcommissie bij het functioneren van de interne auditfunctie en het inbouwen van waarborgen voor een effectieve uitvoering van haar werkzaamheden. De interne auditfunctie blijft evenwel onder de verantwoordelijkheid van het bestuur vallen. Wel wordt voorgesteld dat voor zowel de benoeming als het ontslag van de leidinggevende interne auditor goedkeuring nodig is van de voorzitter van de auditcommissie. Ook wordt het oordeel van de auditcommissie betrokken bij de beoordeling van het functioneren van de interne auditfunctie. In bijvoorbeeld Duitsland, Frankrijk en in het Verenigd Koninkrijk valt de interne auditfunctie onder de verantwoordelijkheid van de auditcommissie. De Commissie meent dat het risico hierbij is dat de taak van de interne auditfunctie dan te veel wordt losgekoppeld van de interne risicobeheersings- en controlesystemen van de vennootschap.[44] Alhoewel dat een verdedigbaar standpunt lijkt, heeft het denk ik toch de voorkeur als de interne auditfunctie aan de auditcommissie rapporteert.[45] Zo geldt dat als er een risicomanagementfunctie en/of compliancefunctie is, die direct of indirect aan het bestuur rapporteert, het niet voor de hand ligt dat de interne auditfunctie ook aan het bestuur rapporteert, onder meer omdat de interne auditfunctie een oordeel moet geven over de kwaliteit van risicomanagementprocessen en *assurance* moet verschaffen dat risico's correct worden geëvalueerd. Overigens hoeft dit niet te betekenen dat de interne auditfunctie functioneel buiten de operationele organisatie geplaatst wordt. De personele invulling en de beoordeling van het functioneren van de interne auditfunctie zouden echter door de desbetreffende auditcommissarissen moeten plaatsvinden. Verder wordt voorgesteld dat de interne auditfunctie direct toegang heeft tot de externe accountant en daarnaast tevens tot de auditcommissie als geheel.[46] De eerste suggestie lijkt mij vanzelfsprekend. Toegang tot de auditcommissie ligt ook voor de hand. Overigens zou dit op een meer natuurlijke wijze gewaarborgd zijn als de interne auditfunctie onder de verantwoordelijkheid van de auditcommissie wordt geplaatst.[47]

In dit kader kan ook worden gewezen op de voorgestelde best practice bepaling 1.5.5, waarin is vastgelegd dat de raad van commissarissen onverwijld wordt geïnformeerd door het bestuur en de externe accountant over materiële onregelmatigheden binnen de vennootschap, waaronder begrepen onregelmatigheden met betrekking tot de integriteit van de financiële verslaggeving. Mocht de interne auditfunctie materiële onregelmatigheden tegenkomen, dan geldt dus geen onverwijlde informatieplicht jegens de raad van commissarissen. Het lijkt mij dat een dergelijke informatieplicht ook voor de interne auditfunctie zou moeten gelden. Dit zou alsnog moeten worden toegevoegd.

Er worden ook belangrijke wijzigingen voorgesteld met betrekking tot de 'in control'-verklaring. Ten eerste gaan niet-financiële aspecten van ondernemen ook onder de 'in control'-verklaring vallen. Ten tweede wordt voorgesteld dat het bestuur in het bestuursverslag een verklaring aflegt met een duidelijke onderbouwing dat de verwachting is dat de continuïteit van de vennootschap voor de komende twaalf maanden gewaarborgd is.[48] Deze bepaling kan naar mijn mening worden geschrapt. Op basis van artikel 2:384 lid 3 van het Burgerlijk Wetboek (BW) geldt dat het bestuur bij het opstellen van de jaarrekening moet beoordelen of de vennootschap in staat zal zijn going concern voortgezet te worden. Dat lijkt mij voldoende. Het bepaalde in Best practice bepaling 1.5.3, waarin is vastgelegd dat de auditcommissie in het verslag dat zij uitbrengt aan de raad van commissarissen aandacht besteedt aan de verwachting of de continuïteit van de vennootschap voor de komende twaalf maanden is gewaarborgd, kan mijns inziens eveneens komen te vervallen. In de voorgestelde best practice bepaling 1.5.2 is verder vastgelegd dat de interne auditor en de externe accountant in beginsel aanwezig zijn bij de vergaderingen van de auditcommissie.

In principe 1.6 wordt voorgesteld dat de raad van commissarissen de voordracht tot benoeming van de externe accountant doet aan de algemene vergadering en toezicht houdt op het functioneren van de externe accountant. De auditcommissie vervult een leidende rol in de voorbereiding van de besluitvorming van de raad van commissarissen.

44. Zie consultatiedocument, p. 13.
45. Zo ook L. Paape, Corporate governance. The impact on the role, position, and scope of services of the internal audit function (diss. Rotterdam), 2007.
46. Zie over de auditcommissie ook H.H. Kersten, De rol van de auditcommissie bij het toezicht door de raad van commissarissen op risicobeheer, Ondernemingsrecht 2016/14.
47. In de 'Resource guide to the U.S. Foreign Corrupt Practices Act by the Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission' uit 2012 wordt hierover opgemerkt: 'In appraising a compliance program, DOJ and SEC also consider whether a company has assigned responsibility for the oversight and implementation of a company's compliance program to one or more specific senior executives within an organization. Those individuals must have appropriate authority within the organization, adequate autonomy from management, and sufficient resources to ensure that the company's compliance program is implemented effectively. Adequate autonomy generally includes direct access to an organization's governing authority, such as the board of directors and committees of the board of directors (e.g., the audit committee).'
48. Dit kan een aanknopingspunt voor corporate litigation vormen.

 doi: 10.5553/MvO/245231352016001101002

Daarnaast rapporteert de auditcommissie jaarlijks aan de raad van commissarissen over het functioneren van en de ontwikkelingen in de relatie met de externe accountant en geeft advies aan de raad van commissarissen over benoeming, herbenoeming of ontslag van de externe accountant en bereidt de selectie van de externe accountant voor.[49] Eveneens doet de auditcommissie een voorstel aan de raad van commissarissen voor de opdracht voor controle van de jaarrekening aan de externe accountant.[50] Het bestuur begeleidt en faciliteert dit en de raad van commissarissen stelt de opdracht vast.[51] Verder volgt bij een tussentijds vertrek van de externe accountant een persbericht waarin de reden van het tussentijds vertrek wordt toegelicht.[52] Voorts geldt op grond van de voorgestelde best practice bepaling 1.7.6 dat de auditcommissie inzage krijgt in materiële wijzigingen die de externe accountant op verzoek van het bestuur heeft aangebracht in de concept-managementletter dan wel het concept-accountantsverslag.

In paragraaf 3 ben ik ingegaan op de interne auditfunctie, risicomanagementfunctie en compliancefunctie. Opvallend is dat er in het consultatiedocument en de voorgestelde Code wel aandacht is voor de interne auditfunctie, maar niet voor de risicomanagementfunctie en ook niet voor de compliancefunctie. In elk geval zou in de Code kunnen worden bepaald dat de vennootschap toelicht of zij over een risicomanagementfunctie en/of een compliancefunctie beschikt, en als dat het geval is, op welke wijze de rol, structuur en onderlinge afbakening van deze functies zijn vormgegeven.

5 Conclusie

In dit artikel ben ik ingegaan op de voorgestelde wijzigingen van de Code op het terrein van risicomanagement. Het betreft mijns inziens veelal nuttige voorstellen. Het consultatiedocument roept echter ook nog enkele vragen op. Ook zijn er bepalingen die heroverweging verdienen. Daartoe heb ik enkele suggesties gedaan. Zo zou kunnen worden benadrukt in de Code dat er een relatie is tussen risicomanagement én langetermijnwaardecreatie en cultuur. Ook verdient het de voorkeur als de interne auditfunctie aan de auditcommissie rapporteert. Daarnaast zou moeten worden bepaald dat mocht de interne auditfunctie materiële onregelmatigheden tegenkomen, er dan een onverwijlde informatieplicht jegens de raad van commissarissen bestaat. Ten slotte is het opvallend dat er in het consultatiedocument en de voorgestelde Code wel aandacht is voor de interne auditfunctie, maar niet voor de risicomanagementfunctie en ook niet voor de compliancefunctie. Ik meen dat daar nog eens naar gekeken zou kunnen worden. In elk geval zou kunnen worden bepaald dat de vennootschap toelicht of zij over een risicomanagementfunctie en/of een compliancefunctie beschikt, en als dat het geval is, op welke wijze de rol, structuur en onderlinge afbakening van deze functies zijn vormgegeven.

49. Best practice bepaling 1.6.1. De auditcommissie betrekt de visie van het bestuur hierbij.
50. Best practice bepaling 1.6.2.
51. De belangrijkste conclusies van de auditcommissie over de voordracht en de uitkomsten van het selectieproces van de externe accountant worden aan de algemene vergadering van aandeelhouders meegedeeld. Indien de raad van commissarissen het advies van de auditcommissie inzake benoeming van de externe accountant niet overneemt, worden de argumenten hiervoor meegedeeld aan de algemene vergadering en vermeld in het verslag van de raad van commissarissen (best practice bepaling 1.6.3).
52. Best practice bepaling 1.6.4.