Risicomanagement en risicoverslaggeving tegen de achtergrond van corporate governance

Cees de Groot

SAMENVATTING De kern van corporate governance is dat een beursgenoteerde vennootschap moet streven naar het creëren van langetermijnaandeelhouderswaarde. Daar hoort bij dat de vennootschap beschikt over een op haar situatie toegesneden intern risicobeheersings- en controlesysteem en zich rekenschap geeft van de noodzaak van risicoverslaggeving. Het bestuur van de vennootschap is voor beide verantwoordelijk. Uit de corporate-governancediscussie vloeien belangrijke inzichten voort over wat goed risicomanagement en goede risicoverslaggeving inhouden, en wat de plaats van de interne audit functie van de vennootschap daarbij kan zijn. Die inzichten komen maar zeer ten dele tot uiting in de Nederlandse corporate governance code. Die code zou dan ook op enkele punten moeten worden aangepast.

1 Inleiding

Corporate governance gaat over 'deugdelijk ondernemingsbestuur' (Schwarz en Steins Bisschop, 2004). Corporate-governanceregels zijn voor een belangrijk deel te vinden in codes (Dorresteijn en De Groot, 2004). De Nederlandse corporate governance code bevat een aantal principes (21) en een groot aantal best practice-bepalingen (113) die beursgenoteerde vennootschappen houvast moeten bieden bij het inrichten van hun 'corporate governance structuur' en hun 'corporate governance beleid' (preambule no. 7).

Mr. C. de Groot studeerde sociaal-economisch recht aan de Rijksuniversiteit Groningen. Daarna was hij als onderzoeker verbonden aan de afdeling Sociaal Recht van de Universiteit Leiden waar hij promoveerde op het onderwerp 'Netherlands labor and co-determination law in an EEC perspective'.
Hij is nu verbonden aan de afdeling Ondernemingsrecht van de Universiteit Leiden.

Een kenmerk van beursgenoteerde vennootschappen is dat zij een groot en verspreid aandelenbezit (kunnen) hebben. De aandeelhouders hebben dan geen 'grip' meer op het bestuur en de raad van commissarissen. Dit spanningsveld staat bekend als het *agency problem* (Kraakman, 2001). Het agency problem wordt des te klemmender in het licht van het feit dat de Nederlandse corporate governance code er van uitgaat dat beursgenoteerde vennootschappen moeten streven naar het creëren van aandeelhouderswaarde ('shareholder value') op lange termijn (preambule no. 3). Corporate governance probeert een antwoord te geven op het agency problem door het bestuur en de raad van commissarissen te verplichten tot transparantie, het afleggen van verantwoording en het waar mogelijk betrekken van de aandeelhouders bij besluitvorming (Van Olffen, 2000, p. 15). Bij het creëren van transparantie en het afleggen van verantwoording zijn de jaarrekening en het jaarverslag[1] belangrijke instrumenten. Goede corporate governance brengt ook mee dat een vennootschap zich bewust moet zijn van de risico's waaraan zij onderhevig is en daarover moet rapporteren. De Nederlandse corporate governance code gaat hierop in een aantal principes en best practice-bepalingen (hierna BP-bepalingen) in. Voor interne risico's bepaalt de code dat in de vennootschap een intern risicobeheersings- en controlesysteem aanwezig moet zijn (BP-bepaling II.1.3), en dat het bestuur in het jaarverslag moet verklaren dat dit systeem adequaat en effectief is en dat moet onderbouwen (BP-bepaling II.1.4). Voor externe risico's bepaalt de code dat het bestuur in het jaarverslag moet rapporteren over de gevoeligheid van de resultaten van de vennootschap ten aanzien van externe omstandigheden en variabelen (BP-bepaling II.1.5) (Renes, 2004). Deze regelingen hebben betrekking op het risicomanagement ('risk management') en de risicoverslaggeving ('risk reporting') van de vennootschap (Dassen, 2004; De Koning, 2004). De verklaring die het bestuur op grond van BP-

bepaling II.1.4 moet geven is het *in control statement* (Sampers, 2005). Van Leeuwen (2005) heeft erop gewezen dat dit statement vérstrekkend is omdat het betrekking heeft op het gehele interne risicobeheersings- en controlesysteem. De Amerikaanse Sarbanes-Oxley Act spreekt weliswaar over 'establishing and maintaining an adequate internal control structure and procedures for financial reporting', maar beperkt de af te leggen verklaring tot 'the effectiveness of the internal control structure and procedures […] *for financial reporting*' (section 404, cursivering toegevoegd)[2]. Wanneer het bestuur wil voldoen aan zijn verplichtingen op grond van de genoemde BP-bepalingen, kan het een beroep doen op de interne audit functie van de vennootschap. De Nederlandse corporate governance code geeft in principe V.3 dan ook aan dat de interne accountant een belangrijke rol kan spelen in het beoordelen en toetsen van de interne risicobeheersings- en controlesystemen. De code heeft voor beursgenoteerde vennootschappen grote betekenis: artikel 2:391 lid 5 BW maakt het mogelijk bij algemene maatregel van bestuur voorschriften te stellen over de inhoud van het jaarverslag en daarbij een gedragscode aan te wijzen die moet worden nageleefd[3]. De aangewezen gedragscode is de Nederlandse corporate governance code[4].

Deze bijdrage gaat over de vraag welke eisen corporate governance stelt aan goed risicomanagement en goede risicoverslaggeving. Eerst volgt een uiteenzetting over het belang van risicomanagement en risicoverslaggeving (paragraaf 2). Daarna komen de rol van het bestuur, de raad van commissarissen en de interne-auditfunctie aan de orde (paragraaf 3). Vervolgens wordt ingegaan op risicomanagement (paragraaf 4) en risicoverslaggeving (paragraaf 5) afzonderlijk. Paragraaf 6 gaat over de verhouding van de interne-auditfunctie van de vennootschap tot het bestuur en de raad van commissarissen. In paragraaf 7 staan enkele aanbevelingen tot aanpassing van de Nederlandse corporate governance code.

2 Het belang van risicomanagement en risicoverslaggeving

Het belang van risicomanagement en risicoverslaggeving kan duidelijk worden gemaakt door kort stil te staan bij de risico's waaraan een vennootschap en haar ondernemingsactiviteiten bloot kunnen staan. De risico's die een vennootschap loopt, kunnen op verschillende manieren worden gecategoriseerd (Leenaars, 2003; Meijer, 2003; Rijken, 2004; Vaassen, 2004). Op basis van al die risico's tezamen kan dan het risicoprofiel ('risk profile') van de vennootschap worden geschetst. Een voorbeeld van een verdeling zijn risico's in de sfeer van personeel (bijvoorbeeld ziekte), materieel (diefstal), financiën (betalingen) en informatie (hacking) (Overbeek, Roos Lindgreen en Spruit, 2005, p. 21). Een andere verdeling is die in financiële risico's, operationele risico's en overige risico's (Asaf, 2004, p. 188). Dit onderscheid komt ook naar voren in de Nederlandse corporate governance code die spreekt over risicoanalyses die de vennootschap moet maken met betrekking tot haar operationele en financiële doelstellingen (BP-bepaling II.1.3 onder a). Elders komen iets andere formuleringen voor. De Australische corporate governance code (die is opgesteld door de Australian Stock Exchange), de ASX Principles of good corporate governance and best practice recommendations, geeft aan dat het risicoprofiel van de vennootschap betrekking moet hebben op 'the material risks facing the company', waarbij 'Material risks include financial and non-financial matters' (recommendation 7.1, commentary and guidance)[5]. De hier aangebrachte beperking tot wezenlijke risico's komt ook naar voren in de Sarbanes-Oxley Act. Volgens die wet zijn de chief executive officer en de chief financial officer van de vennootschap veranwoordelijk voor 'establishing and maintaining internal controls' die moeten waarborgen dat zij op de hoogte worden gesteld van 'material information relating to the [vennootschap] and its consolidated subsidiaries' (section 302) (Emanuels, Van Leeuwen en Wallage, 2004). Financiële risico's zijn risico's die de financiële continuïteit van de vennootschap kunnen bedreigen. Operationele risico's zijn risico's die de operationele continuïteit van de ondernemingsactiviteiten kunnen bedreigen (Asaf 2004, p. 172). Beide soorten risico's kunnen voortvloeien uit interne en externe factoren (Asaf 2004, p. 124). Bedrijfsfraude is een (intern) financieel risico. Rente- en wisselkoersschommelingen en veranderende grondstoffenprijzen zijn (externe) financiële risico's. (Interne) operationele risico's zijn bijvoorbeeld het naar voren komen van een ernstige fout in het computersysteem dat de vennootschap gebruikt en een arbeidsconflict dat tot een werkstaking leidt. En (externe) operationele risico's zijn bijvoorbeeld toeleveringsproblemen of het wegvallen van een afnemer. Ook de overige risico's kunnen intern en extern zijn. Voorbeelden van deze overige risico's zijn het mislukken van een reclamecampagne en het falen van het fusie- en overnamebeleid (intern), en wijzigingen in fiscale regelgeving of in regelgeving op het gebied van het kartelrecht, en veranderingen in de voorkeuren van consumenten of in het gedrag van concurrenten

(extern). Financiële, operationele en overige risico's beïnvloeden elkaar. Risicomanagement moet daarom integraal risicomanagement zijn (Duffhues, 2002).

3 De spelers: het bestuur, de raad van commissarissen en de interne-auditfunctie

De Nederlandse corporate governance code maakt risicomanagement en risicoverslaggeving tot een verantwoordelijkheid van het bestuur van de vennootschap. Volgens principe II.1 is het bestuur verantwoordelijk voor het beheersen van de risico's die zijn verbonden aan de ondernemingsactiviteiten. De uitwerking hiervan in de BP-bepalingen III.1.3, III.1.4 en III.1.5 richt zich evenzeer op het bestuur. De rol van de raad van commissarissen is die van toezichthouder. Principe II.1 bepaalt dat het bestuur aan de raad van commissarissen en aan de auditcommissie van de raad moet rapporteren over het risicomanagement, en de interne risicobeheersings- en controlesystemen met de raad en de auditcommisie moet bespreken. Volgens BP-bepaling III.1.6 moet het toezicht van de raad van commissarissen onder meer de risico's omvatten die zijn verbonden aan de ondernemingsactiviteiten alsmede de opzet en de werking van de interne risicobeheersings- en controlesystemen (ook BP-bepaling III.5.4 bepaalt dat de auditcommissie haar toezicht onder meer moet richten op de werking van de interne risicobeheersings- en controlesystemen). En BP-bepaling III.1.8 verplicht de raad ten minste éénmaal per jaar een bespreking te wijden aan die risico's en aan de uitkomsten van de beoordeling door het bestuur van de opzet en werking van die systemen. Het valt op dat deze regelingen de raad van commissarissen en de auditcommissie wel bij het risicomanagement van de vennootschap betrekken, maar niet bij de risicoverslaggeving.

Veelal zal het bestuur de interne audit functie van de vennootschap een belangrijke rol willen geven bij het risicomanagement en (de voorbereiding van) de risicoverslaglegging (Diekman, 2005). Principe V.3 in de Nederlandse corporate governance code over de interne audit functie onderstreept dat ook. Daarvoor zijn verschillende redenen. Binnen het bestuur vervult de chief financial officer een sleutelfunctie (Asaf 2004, p. 6 en 10). Dit is een gevolg van het feit dat het financiële en operationele beleid van de vennootschap, en de keuzes die zij daarin maakt, niet los van elkaar kunnen worden gezien. Investeringsbeslissingen (zoals de beslissing om wel of niet een fabriek te bouwen) hebben bijvoorbeeld een financiële en een operationele kant. Ook het dividendbeleid is een financiële kwestie die operationele gevolgen heeft: de beslissing om behaalde winst te reserveren in plaats van als dividend uit te keren, geeft de vennootschap meer armslag in haar (operationele) fusie- en overnamebeleid. Andersom hebben operationele kwesties, zoals een bedrijfsvoering die leidt tot gebrekkige producten of milieuschade, financiële consequenties: dergelijke gebeurtenissen kunnen ertoe leiden dat de vennootschap op de balans voorzieningen moet opnemen. Het is deze verwevenheid van financiële en operationele aspecten die de rol van de chief financial officer zo belangrijk maakt. De chief financial officer zal zich ook intensief willen bezighouden met risicomanagement en risicoverslaglegging. De chief financial officer zal dat willen doen met behulp van de afdeling die onder hem/haar ressorteert. En de Nederlandse corporate governance code bepaalt dat de interne accountant 'functioneert onder de verantwoordelijkheid van het bestuur' (principe V.3). Dit zal vooral neerkomen op: onder de verantwoordelijkheid van de chief financial officer. Er is nog een reden om de interne-auditfunctie te betrekken bij het risicomanagement en (de voorbereiding van) de risicoverslaglegging. Deze reden is dat de interne-auditfunctie relevante kennis en ervaring heeft omdat zij zich bezighoudt met de interne en externe financiële verslaglegging (Overbeek, Roos Lindgreen en Spruit 2005, pp. 150-151). Zij is bekend met technieken als interviews en vragenlijsten en het verwerken van statistische gegevens, en heeft vaak taken op gebieden als archivering, logistiek en treasury, en het bewaken van de naleving van interne voorschriften en externe regelgeving (Renard, 2004, pp. 325, 34-37 en 40-41). Ook op het gebied van bedrijfsfraude heeft de interne-auditfunctie veelal ervaring met indicaties die haar op het spoor van fraude kunnen brengen, zoals transacties die worden aangegaan zonder de vereiste autorisatie, ongewoon hoge tekorten en een te geringe rotatie op gevoelige functies binnen de organisatie (Renard, 2004, pp. 120-121).

Ook de Engelse corporate governance code, de Combined code on corporate governance, stelt in een bijlage ('Guidance on internal control', ook wel 'The Turnbull guidance') expliciet dat 'Senior management and the board may desire objective assurance and advice on risk and control. An adequately resourced internal audit function (or its equivalent where, for example, a third party is contracted to perform some or all of the work concerned) may provide such assurance and advice' (no. 43)[6]. Het tussen haakjes geplaatste zinsdeel verwijst naar de situatie waarin de vennootschap geen interne-auditfunctie heeft. In zo'n geval eist de Combined code een andere oplossing ('its

equivalent'), én moet de vennootschap jaarlijks beoordelen of er een interne-auditfunctie moet komen (code provision C.3.5). Beide elementen komen in de Nederlandse corporate governance code niet voor.

4 Wat is risicomanagement?

De Nederlandse corporate governance code verlangt dat een beursgenoteerde vennootschap 'een op de vennootschap toegesneden' intern risicobeheersings- en controlesysteem heeft (BP-bepaling II.1.3). De code bevat slechts een korte aanduiding van de gewenste techniek van risicomanagement. Volgens BP-bepaling II.1.3 moet het interne risicobeheersings- en controlesysteem in ieder geval uit de volgende instrumenten bestaan: risicoanalyses, een gedragscode die op de website van de vennootschap wordt geplaatst, handleidingen voor de inrichting van de financiële verslaggeving en een systeem van monitoring en rapportering. De code werkt bijvoorbeeld niet uit wat de inhoud van de gedragscode moet zijn (De Groot, 2005). Wel wijst BP-bepaling V.4.3 onder C op het nut van informatietechnologie voor het interne risicobeheersings- en controlesysteem. Deze bepaling gaat over het verslag van de externe accountant en wijst op een aantal zaken die de externe accountant onder de aandacht van het bestuur en de raad van commissarissen kan brengen. Daarbij horen ook opmerkingen over de werking van de interne risicobeheersings- en controlesystemen, inclusief de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Risicomanagement is zonder computersystemen nauwelijks denkbaar (Roos Lindgreen, 2005). Het inzetten van geavanceerde computersystemen maakt het mogelijk sommige risico's vrijwel onmiddellijk ('in real time') te signaleren door deze systemen te laten reageren op afwijkingen van normale patronen (Asaf, 2004, p. 334).

De Nederlandse corporate governance code geeft dus slechts summiere indicaties over de manier waarop een vennootschap het risicomanagement moet inrichten. Dit is opvallend omdat voor risicomanagement wel standaarden zijn ontwikkeld. Zo'n standaard is het COSO Enterprise Risk Management – Integrated Framework (Van Leeuwen, 2005)[7]. Dit raamwerk, en ook de literatuur die over risicomanagement beschikbaar is, bevatten belangrijke opmerkingen over de techniek van risicomanagement (Kaptein, Rozekrans en De Groot, 2005). Allereerst is het van belang dat de risico's waaraan de vennootschap en haar ondernemingsactiviteiten blootstaan, worden onderkend en in kaart gebracht. Dit is risico-onderkenning ('risk identification') en risicobeschrijving ('risk description'). Vervolgens is het noodzakelijk de geconstateerde risico's te beoordelen ('risk assessment'). Risicobeoordeling gaat vooral om de vraag hoe groot de kans is dat een risico zich verwezenlijkt en hoe ernstig de gevolgen zijn wanneer dat risico zich verwezenlijkt (Renard, 2004, p. 147). De vennootschap moet adequate reacties formuleren op risico's die voldoende ernstig zijn ('risk responding'). Een adequate reactie op risico's kan verschillende vormen aannemen: bij sommige financiële risico's door gebruik te maken van financiële derivaten (futures, opties, swaps en dergelijke), bij sommige operationele risico's door verzekeringen te sluiten, en in sommige gevallen door eigen fondsvorming ('self-insurance') (Asaf, 2004, pp. 129-130, 135, 147, 166, 220 en 230). Soms is risicoreactie niet eens mogelijk of wenselijk (Overbeek, Roos Lindgreen en Spruit, 2005, p. 21). Omdat risicoreactie geld kan kosten wordt in dit verband ook de term 'risk finance' gebruikt. Risicocontrole ('risk control') houdt in dat de vennootschap moet beschikken over mechanismes die waarborgen dat de reacties van de vennootschap op geconstateerde risico's ook daadwerkelijk worden geïmplementeerd. Toegepast op de hiervoor gebruikte begrippen verwijst de term risicobeheersing in BP-bepaling II.1.3 naar risico-onderkenning, risicobeschrijving, risicobeoordeling en risicoreactie[8]. Risicobeheersing en risicocontrole samen kunnen dan als risicomanagement worden aangeduid.

5 Risicoverslaggeving

(Externe) verslaggeving speelt in het ondernemingsrecht een belangrijke rol. Het gaat daarbij in de eerste plaats om financiële verslaggeving. De financiële verslaggeving van de vennootschap vindt vooral plaats in de jaarrekening, het jaarverslag, de kwartaal- en/of halfjaarcijfers, en door het publiceren van ad hoc financiële informatie (BP-bepaling V.1.1). Inherent aan financiële verslaggeving is dat zij ook een beperkte risicoverslaggeving omvat. Adequate financiële verslaggeving geeft immers automatisch enig inzicht in de financiële risico's die de vennootschap loopt. Dit komt ook naar voren in de wet. Volgens art. 2:362 lid 1 BW moet de jaarrekening een zodanig inzicht geven dat een verantwoord oordeel kan worden gevormd omtrent het vermogen en het resultaat van de rechtspersoon, alsmede *voorzover de aard van een jaarrekening dat toelaat*, omtrent de solvabiliteit en liquiditeit. Uit de formulering van deze bepaling blijkt tegelijkertijd dat de jaarrekening, gegeven haar karakter, niet de plaats is voor een volledige verslaggeving van financiële risico's en nog

minder voor een integrale verslaggeving van alle financiële, operationele en overige risico's. Daarvoor is het jaarverslag een geschikter instrument (Meijer, 2003). Dat komt inmiddels (dat wil zeggen sinds de Wet uitvoering IAS-verordening, IAS 39-richtlijn en moderniseringsrichtlijn van 16 juli 2005)[9] ook tot uiting in Boek 2 BW. Volgens artikel 2:362 lid 8 BW *kan* een rechtspersoon de jaarrekening opstellen volgens de door de International Accounting Standards Board vastgestelde en door de Europese Commissie goedgekeurde standaarden, mits die rechtspersoon dan alle (voor hem van toepassing zijnde) vastgestelde en goedgekeurde standaarden toepast. Maar een beursgenoteerde vennootschap *moet* op grond van artikel 4 van de IAS-verordening de *geconsolideerde* jaarrekening opstellen volgens de IAS (Van Geffen, 2005; Van Helleman, 2005)[10]. Zowel voor vennootschappen waarop artikel 2:362 lid 8 BW van toepassing is, als voor vennootschappen die onder het bereik van artikel 4 van de IAS-verordening vallen, geldt artikel 2:391 BW. In lid 1 van dit artikel is nu opgenomen dat het jaarverslag een beschrijving van *de voornaamste risico's en onzekerheden* moet geven waarmee de rechtspersoon wordt geconfronteerd. Lid 3[11] bevat hierop nog een belangrijke aanvulling door te bepalen dat ten aanzien van het gebruik van *financiële instrumenten* door de rechtspersoon en voorzover zulks van betekenis is voor de beoordeling van zijn activa, passiva, financiële toestand en resultaat, de doelstellingen en het beleid van de rechtspersoon inzake risicobeheer moeten worden vermeld. Volgens deze bepaling moet ook aandacht worden besteed aan het beleid inzake de afdekking van risico's verbonden aan alle belangrijke soorten *voorgenomen transacties*, en aan de door de rechtspersoon gelopen *prijs-, krediet-, liquiditeits- en kasstroomrisico's*. Deze regelingen hebben de Nederlandse corporate governance code als het ware ingehaald. Die bepaalt wat betreft interne risico's alleen dat het bestuur in het jaarverslag moet ingaan op de werking van de interne risicobeheersings- en controlesystemen en op significante wijzigingen en geplande verbeteringen in die systemen (BP-bepaling II.1.4), en wat betreft externe risico's dat het bestuur moet rapporteren over de gevoeligheid van de resulaten van de vennootschap ten aanzien van externe omstandigheden en variabelen (BP-bepaling II.1.5).

6 De plaats van de interne-auditfunctie

De Nederlandse corporate governance code maakt het bestuur verantwoordelijk voor risicomanagement en risicoverslaggeving. De code sluit hier aan bij de praktijk. Asaf constateert dat 'Almost all of the leading global multinationals […] have placed the function of overseeing risk management policy at the board level' (Asaf, 2004, p. 123). Risicomanagement en risicoverslaggeving kunnen dan ook niet los worden gezien van het financiële en operationele beleid van de vennootschap en de keuzes die zij daarin maakt. Voor risicomanagement geldt immers dat een belangrijk onderdeel daarvan risicoreactie is. De beslissing hoe de vennootschap moet reageren op risico's maakt – ook al vanwege de kosten daarvan – deel uit van de keuzes van de vennootschap in haar totale financiële en operationele beleid. Maar adequaat risicomanagement (of het achterwege blijven daarvan) is ook bepalend voor de financiële continuïteit van de vennootschap en de operationele continuïteit van haar ondernemingsactiviteiten, en heeft daarom rechtstreeks invloed op de aandeelhouderswaarde. Ook risicoverslaggeving raakt de aandeelhouders rechtstreeks, omdat (potentiële) kapitaalverschaffers hun investeringsbeslissingen willen baseren op tijdige, volledige en juiste informatie. Het bestuur verkeert in dit opzicht in een lastige positie. Het is – in de woorden van de Nederlandse corporate governance code – enerzijds verantwoordelijk voor de realisatie van de doelstellingen van de vennootschap, de strategie en het beleid, en voor de resulatenontwikkeling (principe II.1), en is anderzijds verantwoordelijk voor risicomanagement en risicoverslaggeving. Het gevaar bestaat dat het bestuur de risico's van zijn financiële en operationele beleid (bewust of onbewust) onderschat en daardoor te weinig interesse heeft voor risicomanagement en risicoverslaggeving. Vandaar dat wel verdedigd wordt dat enerzijds financiële en operationele beslissingen en anderzijds beslissingen op het terrein van risicomanagement en risicoverslaggeving bij voorkeur gescheiden van elkaar moeten worden genomen (Asaf 2004, p. 124). Dit botst met principe V.3 in de code dat de interne accountant – die een belangrijke rol kan spelen in het beoordelen en toetsen van de interne risicobeheersings- en controlesystemen – functioneert onder de verantwoordelijkheid van het bestuur. Dit principe moet (uiteraard) niet worden gelezen als een aantasting van de onafhankelijke en professionele oordeelsvorming en advisering door de interne-auditfunctie. Maar het opent wel de mogelijkheid van beïnvloeding van de interne-auditfunctie door het bestuur, en geeft het bestuur de mogelijkheid de eigen inzichten en adviezen van de interne-auditfunctie eenzijdig naast zich neer te leggen. Een manier om dit te verhelpen, is het inbouwen van waarborgen die ertoe leiden dat de interne audit functie niet alleen wordt aangestuurd door het bestuur. Dat kan door de interne-

auditfunctie te plaatsten tussen het bestuur (en de chief financial officer) en de raad van commissarissen (en de auditcommissie). Verschillende codes bevatten daartoe aanzetten.
De Australische corporate governance code bepaalt dat de auditcommissie[12] 'should have access to the internal audit function without the presence of management'. Bovendien bepaalt de code dat 'In order to enhance the objectivity and performance of the internal audit function, companies should consider a second reporting line from the internal audit function to the […] committee' (recommendation 7.1, commentary and guidance). Deze oplossing – de 'second reporting line' van de interne audit functie naar de auditcommissie – was ook aangevoerd door Glasz en Fransen (2002). De Engelse Combined code on corporate governance gaat nog verder. De 'Guidance on audit committees' ('The Smith Guidance') bij deze code geeft aan dat de auditcommissie 'should approve the appointment or termination of appointment of the head of internal audit' (no. 4.11) en 'should ensure that the function has the necessary resources and access to information to enable it to fulfil its mandate, and is equipped to perform in accordance with appropriate professional standards for internal auditors' (no. 4.10). De Guidance voegt daaraan ook toe dat 'the audit committee should review and approve the statements included in the annual report in relation to internal control and the management of risk' (no. 4.7).[13]

7 Conclusie en aanbevelingen

Een beursgenoteerde vennootschap moet streven naar het creëren van langetermijnaandeelhouderswaarde. Risicomanagement en risicoverslaggeving zijn daarvoor onontbeerlijk. Uit de corporate-governance-discussie vloeien een aantal conclusies voort over hoe goed risicomanagement en goede risicoverslaggeving eruit kunnen zien. De regeling in Boek 2 BW (artikel 2:391 BW) is op dit punt recent aangepast. De Nederlandse corporate governance code bevat regels die beogen beursgenoteerde vennootschappen in aanvulling op de wet houvast te bieden. De code gaat soms te beperkt en soms op een betwistbare manier om met risicomanagement en risicoverslaggeving. Daarom kan de code op enkele punten worden verbeterd. De Monitoring Commissie Corporate Governance Code, die onder meer tot doel heeft leemtes of onduidelijkheden in de code te signaleren, zou hiertoe een voorzet kunnen geven. Te denken valt aan het volgende:

- In BP-bepaling II.1.3 kan worden bepaald dat het interne risicobeheersings- en controlesysteem van de vennootschap moet zijn gebaseerd op een modern en breed gedragen raamwerk[14], en aandacht moet besteden aan elementen als risico-onderkenning, risicobeschrijving, risicobeoordeling, risicoreactie en risicocontrole. Dit raamwerk kan het COSO Enterprise Risk Management – Integrated Framework zijn, maar dat hoeft niet. Als nadeel van dat raamwerk wordt de uitvoerigheid ervan genoemd (De Jong, 2005).
- Aan BP-bepaling II.1.4 kan worden toegevoegd dat de raad van commissarissen het in control statement moet goedkeuren.
- BP-bepaling II.1.5 kan inhouden dat het bestuur in het jaarverslag een beschrijving moet geven van de voornaamste risico's en onzekerheden waarmee de vennootschap en haar ondernemingsactiviteiten worden geconfronteerd (conform artikel 2:391 lid 1 BW), en – rekening houdend met de concurrentiegevoeligheid van bepaalde informatie – *aangeeft welke reacties het bestuur dienaangaande heeft genomen* (voor een aantal specifieke risico's geldt dan de aparte regeling van artikel 2:391 lid 3 BW).
- Principe V.3 kan luiden dat de interne audit functie van de vennootschap intensief betrokken moet zijn bij het risicomanagement en (de voorbereiding van) de risicoverslaggeving door het bestuur. Tevens kan dit principe inhouden dat het bestuur en de auditcommissie tezamen verantwoordelijk zijn voor deze werkzaamheden van de interne audit functie, en dat de interne audit functie daarover zowel aan het bestuur als aan de auditcommissie rapporteert. De gezamenlijke verantwoordelijkheid moet ten minste inhouden dat de benoeming en het ontslag van de interne accountant de goedkeuring behoeven van de auditcommissie en dat het budget van de interne audit functie door de auditcommissie moet worden goedgekeurd.
- Onder principe V.3 kan een BP-bepaling worden ingelast die bepaalt dat, wanneer de vennootschap geen interne audit functie heeft, het bestuur daarover in het jaarverslag uitleg moet geven. Deze bepaling kan ook inhouden dat de vennootschap in zo'n geval een volwaardig alternatief in het leven moet roepen voor het risicomanagement en (de voorbereiding van) de risicoverslaggeving (bijvoorbeeld het inschakelen van een extern bureau), waarbij principe V.3 in acht moet worden genomen.

Deze voorstellen leiden ertoe dat beursgenoteerde vennootschappen risicomanagement en risicoverslaggeving des te meer serieus moeten nemen. Ook geven deze voorstellen de interne audit functie een expliciete rol bij het risicomanagement en (de voorbereiding

van) de risicoverslaggeving. Door de voorstellen kan zij die rol bovendien in betrekkelijke onafhankelijkheid uitoefenen. ■

Literatuur

Asaf, S., (2004), *Executive corporate finance; the business of enhancing shareholder value*, Pearson Education Limited, Harlow.

Dassen, R., (2004), Risicobeheersing na Tabaksblat: de volgende stap?, in: *Maandblad voor Accountancy Bedrijfseconomie*, jg. 78, nr. 4, april, pp. 130-131.

Diekman, P.A.M., (2005), Rapporteren over interne controle; Sarbanes Oxley, section 404 en de rol van de interne accountant, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg., 79, nr. 10, oktober, pp. 512-521.

Dorresteijn, A.F.M. en C. de Groot, (2004), Corporate governance codes: origins and perspectives, in: *European Company Law*, 2004/ issue 2, pp. 43-56.

Duffhues, P.J.W., (2002), Recente ontwikkelingen in financieel risicomanagement, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 76, nr. 4, april, pp. 138-149.

Emanuels, J.A, O.C. van Leeuwen en Ph. Wallage, (2004), Internal control volgens Sarbanes-Oxley; overzicht en praktische betekenis, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 78, nr. 7/8, juli/augustus, pp. 348-355.

Geffen, C.J.A. van, (2005), Kanttekeningen bij de modernisering van het Nederlandse jaarrekeningenrecht, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, nr. 7/8, juli/augustus, pp. 334-342.

Glasz, J.R. en M.M. Fransen (2002), Audit committee: bewaker van goede governance, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 76, nr. 12, december, pp. 593-603.

Groot, C. de, (2005), Tussen corporate governance en arbeidsrecht: de integriteitscode, in: *Sociaal Maandblad Arbeid*, nr. 9, pp. 418-425.

Helleman, J. van, (2005), Goedkeuring van IFRS voor toepassing in Europa, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, nr. 7/8, juli/augustus, pp. 326-333.

Jong, E. de, (2005), Interne controle: the next banana skin?, in: *Ondernemingsrecht*, nr.14, pp. 463.

Kaptein, M., R. Rozekrans en R. de Groot, (2005), Integriteitklimaat als auditobject, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, nr. 10, oktober, p. 466-474.

Koning, W.F. de, (2004), Bestuurlijke informatieverzorging of interne beheersing?, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 78, nr. 7/8, juli/augustus, pp. 343-347.

Kraakman, R., (2001), The durability of the corporate form, in: *The twenty-first-century firm; changing economic organization in international perspective* (ed. P. DiMaggio), Princeton University Press, Princeton, pp. 147-160.

Leenaars, J.J.A., (2003), Risicomanagement van banken, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 77, nr. 7/8, juli/augustus, pp. 340-347.

Leeuwen, O.C. van, (2005), Sarbanes Oxley en Tabaksblat: dat valt tegen!, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, nr. 7/8, juli/augustus, pp. 324-325.

Meijer, J.W.M.K., (2003), Verslaggeving over risico's, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 77, nr. 3, maart, pp. 109-118.

Olffen, M. van, (2000), *Beschermingsmaatregelen in de 21e eeuw*, Kluwer, Deventer.

Overbeek, P., E. Roos Lindgreen en M. Spruit, (2005), *Informatiebeveiliging onder controle*, Pearson Education Benelux, Amsterdam.

Paape, L., H. Commandeur en G.J. van der Pijl, (2005), Internal audit on the rise; observaties uit de praktijk, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, nr. 6, juni, pp. 276-283.

Renard, J., (2004), *Théorie et pratique de l'audit interne*, Éditions d'Organisation, Paris.

Renes, R.M., (2004), Zonder interne beheersing geen corporate governance, in: *Accounting*, jg. 108, nr. 9, september, pp. 20-26.

Rijken, H.A., (2004), Risicomanagement is niet nieuw; de expliciete en gecoördineerde aanpak wel, in: *Accounting*, jg. 108, nr. 5, mei, pp. 8-14.

Roos Lindgreen, E.E.O., (2005), COBIT; opkomst, ondergang en opleving van een raamwerk voor informatiebeheersing, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, nr. 5, mei, pp. 206-211.

Sampers, P.A.M., (2005), Het 'in control statement'; eerste aanzet tot bestuursverklaring inzake interne beheersing voor Nederlandse beursfondsen, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, nr. 7/8, juli/augustus, pp. 361-369.

Schwarz, C.A. en B.T.M. Steins Bisschop, (2004), Transparantie en de corporate governance discussie, in: *Accounting*, jg. 108, nr. 9, september, pp. 2-5.

Vaassen, E.H.J., (2004), Enterprise risk management: een overzicht, in: *Accounting*, jg. 108, nr. 5, mei, pp. 2-7.

Noten

1 Het begrip jaarverslag is de wettelijke term voor het verslag van de Raad van Bestuur, ook wel bestuursverslag of directieverslag genoemd.

2 Zie voor de tekst van de Sarbanes-Oxley Act en verdere informatie www.sarbanes-oxley-forum.com.

3 Voorheen lid 4: vernummerd door de in noot 9 bedoelde wet.

4 Aangewezen bij Besluit van 23 december 2004, Staatsblad 2004, 747.

5 Zie www.asx.com.au > listed companies > corporate governance.

6 De Engelse Combined code on corporate governance is opgesteld door the Financial Reporting Council. Zie www.frc.org.uk > corporate governance.

7 COSO staat voor Committee of Sponsoring Organizations of the Treadway Commission. COSO is een samenwerkingsverband van vijf private organisaties. In de naam van COSO klinkt door dat COSO oorspronkelijk de National Commission on Fraudulent Financial Reporting (naar de toenmalige voorzitter 'Treadway Commission' genoemd) ondersteunde. Zie www.coso.org.

8 De trits risico-onderkenning, risicobeschrijving en risicobeoordeling kan in verband worden gebracht met de term risicoanalyses in BP-bepaling II.1.3 onder a.

9 Staatsblad 2005, 377, Kamerstukken 29 737. Het inwerkingtredingsbesluit is gepubliceerd in Staatsblad 2005, 378.

10 Verordening (EG) nr. 1606/2002 van het Europees Parlement en de Raad van 19 juli 2002 betreffende de toepassing van internationale

standaarden voor jaarrekeningen, PbEG 2002 L 243, pp. 1-4.

11 Vergelijk voor beursgenoteerde vennootschappen reeds IAS 32 (Financial instruments: disclosure and presentation), met name 51-95 (Disclosure): 56-59 (Risk Management Policies and Hedging Activities), goedgekeurd door de Europese Commissie bij Verordening (EG) nr. 2237/2004 van 29 december 2004, PbEG 2004 L 393, pp. 1-41.

12 Of een andere commissie, zoals een risk management committee.

13 Vergelijk voor de vraag hoe in de praktijk over dergelijke betrokkenheid van de raad van commissarissen wordt gedacht Paape, Commandeur en Van der Pijl, 2005.

14 Volgens de Verklaring van en toelichting op enkele begrippen die in de code zijn gebruikt, onder II.1.4, ligt het toch al in de rede dat bestuur aangeeft welk raamwerk het heeft gehanteerd.