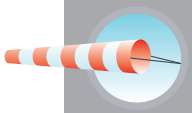
Risicomanagement: een hype?

Wat betekent het voor bestuurders en commissarissen?

NIVRA Accountants in Business

NIVRA-debatbijeenkomsten 2009

Antonio Vivaldistraat 2-8
Postbus 7984
1008 AD Amsterdam
T 020 301 03 01
E nivra@nivra.nl
I www.nivra.nl



Inhoudsopgave

Voorwoord

Geachte lezer,

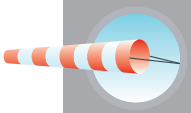
Als bestuurder (of commissaris) draagt u de verantwoordelijkheid voor de continuïteit van uw organisatie. Uw organisatie heeft te maken met een steeds complexere omgeving en steeds hogere verwachtingen van aandeelhouders, klanten, externe toezichthouders en maatschappij.

Het is aan u om ervoor te zorgen dat een adequate inrichting van governance en risicomanagement de lange termijn waardecreatie van uw organisatie ondersteunt.

Deze handreiking geeft een goed inzicht in het hoe en waarom van risico-management. Het is mijn stellige overtuiging dat de handreiking een nuttige bijdrage kan leveren in het verder versterken van uw organisatie.

Als voorzitter van de Monitoring Commissie Corporate Governance Code beveel ik u deze handreiking dan ook van harte aan.

Drs. Jos Streppel



1 Inleiding

Risicomanagement als onderdeel van *good governance* staat weer volop in de belangstelling en niet in de laatste plaats dankzij de kredietcrisis.

Er hangt een zweem van mystiek en complexiteit om het vakgebied. Het lijkt een terrein van experts en technische risicomanagers waarbij de nadruk ligt op formele structuren, het afvinken van checklijsten en het maken van berekeningen (dit laatste met name in de financiële sector). De aldus geleverde (schijn)zekerheid heeft ons jammer genoeg niet behoed voor de huidige crisis. Heeft risicomanagement wel zin?

Vanuit vele hoeken wordt er over het belang van risicomanagement geschreven en gesproken, maar het is voor organisaties zeker niet altijd duidelijk wat er vanuit een governancegedachte mee wordt bedoeld en wat van bestuurders en commissarissen verwacht wordt. Daarnaast is het niet altijd duidelijk wat risicomanagement kan opleveren.

Onze primaire doelgroep bestaat uit bestuurders, het senior management en de commissarissen van de grotere organisaties, beursgenoteerd en niet-beursgenoteerd alsmede publieke sector. Wij hebben ons mede gebaseerd op het discussion paper *Risk Management and internal control systems* dat het NIVRA in het najaar 2007 heeft gepubliceerd[1]. Daar waar wij spreken over commissarissen, worden ook leden van Raden van Toezicht of soortgelijke organen bedoeld.

Om meer duidelijkheid te verschaffen, schetsen wij het belang van risicomanagement vanuit zowel maatschappelijke ontwikkelingen als de impulsen vanuit de individuele organisatie (hoofdstuk 2). In hoofdstuk 3 gaan wij in op de vraag hoe risicomanagement kan worden vormgegeven, vanuit het perspectief van de bestuurder en commissarissen.

[1] Deze discussion paper is in oktober 2007 aangeboden aan de toenmalige voorzitter van de Monitoring Cie. (Jean Frijns) en is toegestuurd aan de CFO's van alle Nederlandse beursgenoteerde ondernemingen. In de discussion paper worden voorstellen gedaan voor de nadere invulling van risicomanagement inclusief de bijbehorende verantwoordelijkheden en de wijze waarop verantwoording wordt afgelegd door de organisatie. De directe aanleiding werd gevormd door de onduidelijkheid over de invulling van best practice bepaling II.1.4 uit de Code Tabaksblat die een zgn. In control statement van het bestuur verlangt.

Wij geven een praktisch handvat en een benchmark om te bepalen welke elementen een volwassen organisatie op het gebied van risicomanagement zou moeten inrichten. Deze benchmark is opgesteld door de “Breakfast groep Risk Management”.

We maken hierbij onderscheid tussen de instrumentele componenten van risicomanagement enerzijds en de gedragscomponenten anderzijds (inclusief de impact van beloningen en de invloed van het gedrag van bestuurders).

We vertalen de verschillende verwachtingen ten aanzien van goed risicomanagement voor bestuurders en commissarissen naar concreet te stellen vragen over toepassing in de praktijk daarvan en in mindere mate naar de verantwoording hierover in bijvoorbeeld het jaarverslag.

Wij willen de bestuurders en commissarissen die bereid zijn geweest de draft versie van dit stuk te reviewen en ons van commentaren te voorzien hartelijk bedanken. Tevens willen wij de leden van de “Breakfast groep Risk Management” hartelijk bedanken voor de input van de maturity benchmark Risico Management. De deelnemers van de Breakfast groep Risk Management zijn: Mirjam Bakker (Aegon), Cees Dekker (SHV Holdings), Eugene Houthooft (Maxeda), Cyriel Mintjes (Corio), Dick Oude Alink (Akzo), Tsjerk-Friso Roelfzema (TomTom), Ton Teitsma (Mediq), Walter van Damme (Kardan), Reinier van Elk (Ahold), Dion Velthyzen (Koninklijke Vopak), Albert Weenink (Randstad), Sander Weisz (USG People) en Simone Heidema (voorzitter, CPI Governance) en hebben deze input op persoonlijke titel gegeven.

Wij hopen met dit document een bijdrage te kunnen leveren aan het versterken van risicomanagement. Uiteraard zijn wij beschikbaar voor eventuele vragen, opmerkingen en suggesties van uw kant.

De NIVRA-werkgroep Corporate Governance
Simone Heidema (Managing Partner CPI Governance) – Voorzitter
John Bendermacher (Director Internal Audit Robeco)
Jan Droogsma (Auditdienst Ministerie van Verkeer en Waterstaat)
Wilmar de Munnik (Manager Beleid, Strategie en Onderzoek Stichting WoonFriesland)
Johan Scheffe (Vaktechnisch medewerker Beleid & Innovatie NIVRA)

2 Waarom risicomanagement?

2.1 Inleiding

In dit hoofdstuk gaan we in op het waarom van risicomanagement. Is risicomanagement een hype. In onze ogen niet. Risicomanagement is een onderdeel van goed bestuur en naar onze stellige overtuiging een belangrijk middel om de continuïteit van organisaties te waarborgen. Organisaties en hun bestuurders en commissarissen krijgen hiervoor zowel impulsen van ontwikkelingen in de maatschappij (paragraaf 2.2) als uit de eigen organisatie (paragraaf 2.3).

2.2 Maatschappelijke ontwikkelingen

In de afgelopen jaren is de maatschappij diverse malen verrast door tegenvallende resultaten van private en publieke organisaties. In een aantal van deze situaties werden de tegenvallende resultaten ook nog verhuld door verslaggevingfraude. Daarnaast ontstond steeds meer het besef dat financiële verslaggeving die met name gericht is op het verleden en de stand van zaken op het moment van het opmaken van het jaarverslag, de maatschappij onvoldoende informatie verschaft. Onder andere over de robuustheid van de organisatie, het beleid dat bestuurders voorstaan en is gerealiseerd en, voor zover van toepassing, de winstgevendheid van de organisatie. De maatschappij is daarnaast ook geïnteresseerd in de cultuur en integriteit van de organisatie en van haar bestuurders en commissarissen. We hebben het hier niet alleen over de belangen van de aandeelhouders, maar ook over die van werknemers, leveranciers, klanten, omwonenden, de overheid etc.

De maatschappij verwacht van organisaties dat bestuurders tijdig inspelen op maatschappelijke ontwikkelingen, dat ze de hiermee gepaard gaande risico's in afdoende mate beheersen, dat commissarissen dit bewaken en dat bestuurders hierover rapporteren in jaarverslagen. Van de laatsten wordt verwacht dat zij verklaren dat de financiële verslaggeving in overeenstemming is met wet- en regelgeving en dat onderliggende systemen goed werken. Bovendien wordt verwacht dat ze rapporteren over het algemene risicoprofiel van de organisatie en de risico's die aan de strategie en de dagelijkse bedrijfsvoering zijn verbonden, en daarbij aangeven in hoeverre deze risico's zijn afgedekt.

Van de commissarissen verwacht de maatschappij dat zij aangeven over welke onderwerpen is gesproken met de bestuurders en dat zij hun eigen functioneren periodiek evalueren.

"We stellen tegenwoordig veel hogere eisen aan het expliciet maken en de verantwoording van risico's. (...). Het belang is evident. Daarom heeft het me verbaasd dat daar aanvankelijk zo weinig reactie op is gekomen. Iedereen fixeerde zich maar op de beloning. Maar risico's identificeren en ze onder controle hebben, is veel belangrijker" [2]

Een specifiek punt dat naar aanleiding van de kredietcrisis bijzondere belangstelling heeft gekregen van de politiek en de beleggers, is het beloningsbeleid en de hoogte van bonussen. Deze elementen kunnen zowel positieve als negatieve effecten hebben op het functioneren van risicomanagement.

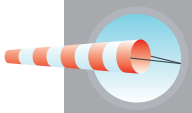
Vorengenoemde maatschappelijke verwachtingen zijn opgenomen in regelgeving, codes en rapportages inzake Corporate Governance, zoals De Nederlandse Corporate Governance Code (Tabaksblat/Frijns), de Transparantie Richtlijn van de EU, de Kabinetsvisie op de financiële sector, de Code Banken, het Verbond van verzekeraars, de principes voor een beheerst beloningsbeleid van de AFM/DNB, de Sabanes Oxley-wetgeving en de Dow Jones Sustainability Index. Standard & Poor's neemt de kwaliteit van het risicomanagementsysteem mee als criterium bij het bepalen van de Credit Rating van de desbetreffende organisatie.

In de vennootschap is een op de vennootschap toegesneden intern risicobeheersings- en controlesysteem aanwezig. Als instrumenten van het interne risicobeheersings- en controlesysteem hanteert de vennootschap in ieder geval:

- risicoanalyses van de operationele en financiële doelstellingen van de vennootschap;
- een gedragscode, die op de website van de vennootschap wordt geplaatst;
- handleidingen voor de inrichting van de financiële verslaggeving en de voor de opstelling daarvan te volgen procedures; en
- een systeem van monitoring en rapporting. [3]

[2] De regels en het spel, Morris Tabaksblat.

[3] De Nederlandse Corporate Governance Code, II.1.3



"Risicomanagement moet steviger zijn geborgd in de governancestructuur van de onderneming. De raad van bestuur moet een collectieve verantwoordelijkheid kunnen dragen voor het risicomanagement. Het algemeen management van de onderneming moet zich meer dan nu bewust zijn van de balans tussen risico en rendement. Gehanteerde risicomodellen moeten daartoe transparanter, beter uitlegbaar en zo mogelijk simpeler worden. Via 'terugtesten' moeten de bestaande modellen op houdbaarheid worden getoetst. (...)" [4]

De zogenaamde risicobereidheid *(risk appetite)* krijgt hierin een steeds prominentere en explicietere plek. Ook zijn er duidelijke (maatschappelijke) ontwikkelingen waarin – vanuit een echte lange termijn waardecreatie – breder wordt gekeken dan alleen naar rendement. De zogeheten ESG (Environmental, Social en Governance) principles zie je steeds vaker benoemd worden. Ook Eumedion heeft in haar missie een voorstel gedaan om de context te verbreden: *"All relevant ES risks and opportunities affecting companies from an investors' perspective"*.

In de kaders zijn een aantal relevante passages uit deze regelgeving, codes en rapportages opgenomen.

"De raad van bestuur, en binnen de raad van bestuur primair de voorzitter van de raad van bestuur, is verantwoordelijk voor het vaststellen, uitvoeren, monitoren en waar nodig bijstellen van het algehele risicobeleid van de bank. De risicobereidheid wordt op voorstel van de raad van bestuur tenminste jaarlijks ter goedkeuring aan de raad van commissarissen voorgelegd. Tussentijdse materiële wijzigingen van de risicobereidheid worden eveneens ter goedkeuring aan de raad van commissarissen voorgelegd" [5]

2.3 Ontwikkelingen op organisatieniveau

Organisaties worden geconfronteerd met een steeds complexere omgeving en steeds hogere verwachtingen van aandeelhouders, klanten, externe toezichthouders en maatschappij. Deze verwachtingen veranderen steeds sneller en wijzen niet altijd dezelfde richting op. Het is aan de bestuurders en commissarissen om ervoor te zorgen dat een adequate inrichting van

[4] **Position paper** Verzekeraars trekken lessen uit kredietcrisis **5 februari 2009**

[5] Nederlandse Vereniging van Banken

governance en risicomanagement de lange termijn waardecreatie van de organisatie ondersteunt.

Uit verschillende onderzoeken en praktijkstudies blijkt dat organisaties de langetermijnwaarde van risicomanagement helder voor ogen hebben. Als één van de belangrijkste voordelen wordt het verkleinen van potentiële verliezen gezien. Maar het identificeren van kansen waar het nemen van bewuste risico's juist de prestaties van de organisatie ondersteunt, is eveneens een belangrijke impuls. Strategie kan de risicobereidheid van een organisatie bepalen maar risicobereidheid kan ook van invloed zijn op de strategie.

Risicomanagement wordt hierdoor steeds beter ingezet ten behoeve van adequate besluitvorming. Consequenties van risico's worden inzichtelijk gemaakt zodat een weloverwogen besluit genomen kan worden. Dit is ook in het kader van de verantwoording (vanuit een good-governancegedachte) een belangrijk aspect, niet alleen richting commissarissen, maar ook richting andere stakeholders zoals kapitaalverschaffers, externe toezichthouders en werknemers. Een belangrijke waarde heeft risicomanagement ook ter ondersteuning van een betere cash flow (lees efficiency in processen en verlaging van reparatiekosten).

Voor goed risicomanagement is het belangrijk dat er sprake is van een leercyclus met een open organisatiecultuur die ervaringen gebruikt om het in de toekomst nog beter te doen. Alleen op deze wijze kan risicomanagement een bijdrage leveren aan goed ondernemerschap.

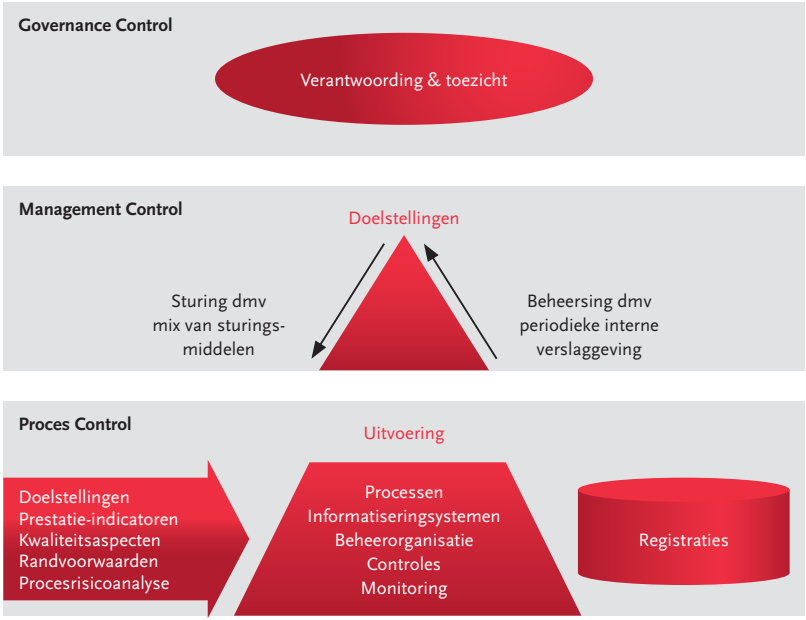
Door het groeiende besef van het belang van governance en risicomanagement, hebben veel ondernemingen de laatste jaren projecten opgestart op het gebied van interne beheersing en risicomanagement; denk aan Sarbanes Oxley, Tabaksblat, Basel II (bij banken), SAS-70, het Tax Control Framework en gerelateerde projecten op het gebied van procesdocumentatie. Soms werd zelfs per project afzonderlijke monitoring ingericht. Veelal ging het hier echter om meer van hetzelfde, alsof je meerdere keren 'in control' kunt zijn. Het opzetten van adequaat geïntegreerd risicomanagement voorkomt dubbel werk.

2.4 Conclusie

Impulsen vanuit de maatschappij alsmede inzichten vanuit de eigen organisatie hebben effectief risicomanagement hoog op de agenda van organisaties gezet.

Niet zozeer vanuit een compliance-gedachte of vanuit de gedachte een verklaring te moeten afgeven, maar juist gedacht vanuit de strategische en (lange termijn-)doelstellingen van de organisatie.

In het volgende hoofdstuk schetsen we de belangrijkste aspecten van risicomanagement vanuit het perspectief van de organisatie, bestuurders en commissarissen. Heldere en praktische taal kan de brug slaan tussen enerzijds bestuurders en commissarissen/toezichthouders en anderzijds tussen bestuurders en hun senior management. Daarmee wordt effectief risicomanagement bevorderd.



Figuur 1: Governance en interne beheersing (www.ciad.nl)

3 Hoe zit risicomanagement in elkaar?

3.1 Inleiding

Vanuit maatschappelijke invloeden is er steeds meer aandacht voor risicomanagement. Afhankelijk van de branche waarin een organisatie actief is, vertaalt die aandacht zich in meer of mindere mate in codes en raamwerken waaraan veelal via het 'comply or explain'-principe voldaan dient te worden.

Organisaties en hun interne en externe toezichthouders hebben daarom belang bij goede invulling van risicomanagement. Een sterke interne governancestructuur en adequaat risicomanagement dat geïntegreerd is in de gehele bedrijfsvoering, dragen bij aan het 'in control' zijn van de organisatie bij het in continuïteit nastreven van haar strategische doelstellingen en – niet onbelangrijk – het zich kunnen verantwoorden daaromtrent, al dan niet gekoppeld aan een eventuele verklaring.

Wij realiseren ons dat risicomanagement een containerbegrip is dat varieert van strategische risico's tot het terrein van administratieve organisatie en interne controle (AO/IC). In dit stuk zijn wij uitgegaan van de definitie (COSO ERM):

> *Ondernemingsrisicomanagement is een proces dat bewerkstelligd wordt door het bestuur van de onderneming, het management en ander personeel en wordt toegepast bij het formuleren van de strategie en binnen de gehele onderneming, ontworpen om potentiële gebeurtenissen die invloed kunnen hebben op de onderneming te identificeren en om risico's te beheren zodat deze binnen de risicoacceptatiegraad vallen, om een redelijke zekerheid te bieden ten aanzien van het behalen van de ondernemingsdoelstellingen.*

3.2 Samenhang en elementen van risicomanagement

Het is van groot belang de inherente risico's die verbonden zijn aan de bedrijfsvoering, te kennen op basis van een gedegen risicoanalyse van zowel financiële als niet-financiële risico's. Tot het laatste horen bijvoorbeeld ook gebrek aan geleverde kwaliteit, in strijd handelen met de regelgeving, handelen buiten het stakeholdersmandaat, etc. Deze risico's leiden vaak tot een ernstige imagoschade waarbij sterk afbreuk wordt gedaan aan het realiseren van de strategische doelstellingen.

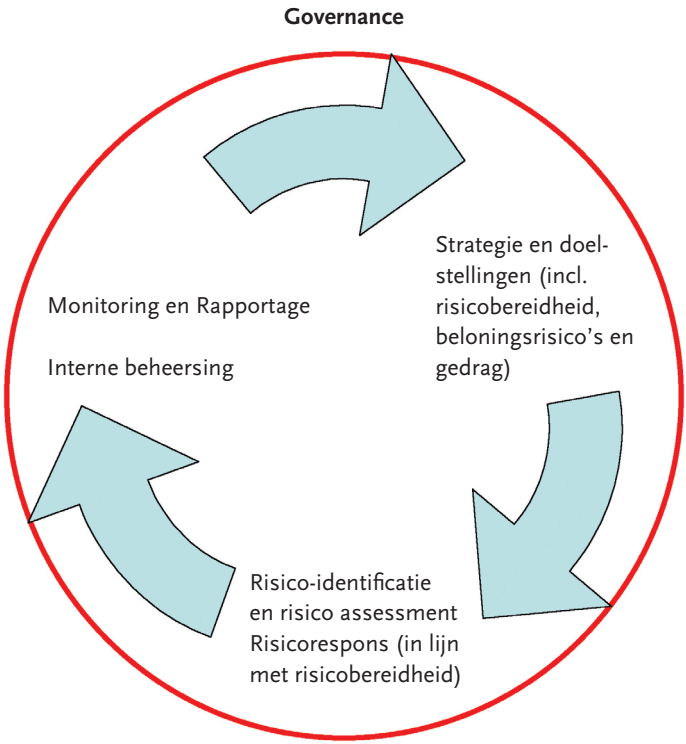
Van belang is om deze risico's te beheersen tot op het niveau dat door bestuurders en hun commissarissen acceptabel wordt geacht, in balans met haar (strategische) doelstellingen en wat maatschappelijk aanvaardbaar wordt geacht. Daarvoor zal de onderneming een effectief stelsel van interne beheersingsmaatregelen opzetten op zowel management- als op operationeel niveau en in een optimale mix van zogenaamde harde maatregelen en zachte maatregelen (ook wel soft controls genoemd).

Harde maatregelen
Meten en rapporteren
Risicocommissie
Richtlijnen en procedures
Risicolimieten
Gedocumenteerde processen
Auditprocessen
Systemen

Zachte maatregelen
Risicobewustzijn
Mensen
Kennis en vaardigheden
Beloningen
Integriteit
Cultuur en waarden
Vertrouwen en communicatie

Figuur 2: Balans tussen harde en zachte maatregelen (Anne Maddoc, Royal District Nursing Service of South Australia Inc. courtesy of James Lam & Associates 2005)

De effectiviteit van beheersingsmaatregelen en het gewenste gedrag vergt een bepaalde mate van monitoring. Tijdige besluitvorming en continue sturing zijn daarbij evident. In onderstaande figuur zijn deze elementen schematisch weergegeven.



Figuur 3: Risicomanagement en de samenhang in de stappen

De kracht van risicomanagement zit in de samenhang en inbedding van bovengenoemde stappen en elementen, in de totale organisatie (zie figuur 3); een geïntegreerd risicobouwwerk. De verklaring in het jaarverslag terzake adequate risicomanagement systemen wordt daarmee geen eenzijdig doel, maar een resultante van krachtig en geïntegreerd risicomanagement, primair ingericht door bestuurders en commissarissen om hun verantwoordelijkheden voor een gezonde bedrijfsvoering te kunnen dragen.

3.3 Rollen en praktische handvatten m.b.t. risicomanagement

Risicomanagement is management. Ook al wordt soms nog wel gedacht dat deze verantwoordelijkheid "gedelegeerd" kan worden, bij de meeste organisaties is het duidelijk dat risicomanagement een integraal onderdeel uitmaakt van bestuurdersverantwoordelijkheid. Onder het kopje "Uw agenda ten aanzien van risicomanagement" geven we een aantal vragen die bestuurders en commissarissen zich zouden kunnen stellen, waarbij de rollen, verantwoordelijkheden en activiteiten van de betrokkenen in de dynamiek van risicomanagement

beknopt worden uitgewerkt. Deze zijn te koppelen aan de benchmark die verder is uitgewerkt in paragraaf 3.5.

Uw agenda ten aanzien van risicomanagement

Governance

- ☐ Is risicomanagement een wezenlijk onderdeel van het management en zijn de risico-afwegingen verwerkt in informatiestromen en besluitvorming?
- ☐ Is een risicocommissie ingesteld om het bestuur te ondersteunen in het maken van beleid en het toezien op de ontwikkelingen op het gebied van risicomanagement?
- ☐ Is het beleid van de bestuurders en commissarissen erop gericht om voorbeeldgedrag te tonen en om beloningsrisico's (de zogenaamde perverse prikkels) uit de weg te gaan ?
- ☐ Op welke wijze wordt binnen uw organisatie aandacht besteed aan integriteit?

Strategie en doelstellingen

- ☐ Wat is het risicobeleid en is dit duidelijk gecommuniceerd naar de belangrijkste stakeholders?
- ☐ Wat is de ratio achter het risicoprofiel van uw organisatie?
- ☐ Is de risicobereidheid geformuleerd en vastgesteld? Is deze doorvertaald naar de organisatie (in de risicotoleranties en stuurvariabelen)? En is deze in balans met het geprognosticeerde rendement?
- ☐ Zijn zowel de risico's die samenhangen met variabele beloning op verschillende niveaus in de organisatie afgewogen en wordt het gewenste (risico)gedrag door het beloningsbeleid ondersteund?

Risico-identificatie & -assessment

- ☐ Is er sprake van een ondernemingsbrede, top down risicoanalyse en –weging waarin alle inherente risico's zijn meegenomen?
- ☐ Wordt de risicoanalyse periodiek geactualiseerd en heroverwogen?
- ☐ Is de risicoanalyse binnen de raad van bestuur besproken en goedgekeurd?
- ☐ Wat zijn de belangrijkste risico's; zijn ook strategische, concentratie- en systeemrisico's (h)erkend?

Risicorespons

- ☐ Wordt er, mede vanuit de gewenste managementinformatie, tijdige actie en/of besluitvorming ondernomen, zodat (achteraf) geen ongewenste risico's worden gelopen? Een bewust besluit om een risico te lopen (in lijn met de risicobereidheid) is ook een besluit.

- ☐ Is de mate van risicobereidheid vertaald in risicotoleranties en restricties?

Interne beheersing

- ☐ Worden de basisrisico's binnen de processen (basis-AO/IC) voldoende beheerst? Hierbij valt niet alleen te denken aan de 'technische' interne beheersingsmaatregelen zoals processen (design en documentatie in verband met continuïteit) en systemen (beveiliging, continuïteits-management), maar juist ook de beheersing die uitgaat van mensen (kwaliteit, kwantiteit).

- ☐ Zijn interne beheersingsmaatregelen geïmplementeerd in een cultuur waarin het vanzelfsprekend is om ze uit te voeren (internal control awareness)?

- ☐ Wordt er binnen uw organisatie voldoende aandacht geschonken aan integriteit?

Monitoring

- ☐ Op welke wijze wordt de effectieve werking van de interne beheersings-maatregelen (bestaan en werking) gemonitored?

- ☐ Wordt voor de monitoring met name gesteund op de activiteiten van bijvoorbeeld afdelingen als Internal Audit, (Operational) Risk Management en/of Compliance?

- ☐ Indien bovengenoemde afdelingen niet (allemaal) voorkomen in uw organisatie heeft u ten aanzien van monitoring dan specifieke afspraken gemaakt met uw externe accountant?

- ☐ Wordt de effectiviteit van het risicomanagementsysteem gemonitored door bestuurders en commissarissen en welke rol speelt de Internal Auditfunctie hierin?

Rapportage

- ☐ Omvat de managementinformatie alle stuurvariabelen en 'control'-issues, op basis waarvan tijdig (bij)gestuurd kan worden?

- ☐ Kan het management van uw organisatie een bevestiging geven van de effectiviteit van het totale risicomanagementsysteem? Indien de verplichting bestaat om een' In Control-verklaring' af te geven, kan een grondige analyse worden uitgevoerd op de inhoud en reikwijdte ervan.

- ☐ Wordt de risicomanagementinformatie besproken binnen het bestuur en met de commissarissen? En worden daarbij tijdig corrigerende maatregelen vastgesteld?

De verschillende rollen

Commissarissen

Betrokken en daadkrachtig
Commissarissen zijn verantwoordelijk voor het toezicht op het door het bestuur gevoerde risicobeleid (inclusief de risicobereidheid) en adviseren het bestuur waar nodig. Als onderdeel van dat toezicht zijn zij extra alert op mogelijke signalen van zogenaamd zonnekoninggedrag van bestuurders. Daarnaast stelt de Raad van Commissarissen de hoogte en de structuur van de bezoldiging van bestuurders vast met inachtneming van de risico's die variabele beloning met zich meebrengen.

Commissarissen vormen zich een zelfstandig oordeel over de aanwezige risico's en beoordelen periodiek op strategisch niveau of de activiteiten passen binnen het risicobeleid van de organisatie. Belangrijk is dat ze afwijkingen van het verwachte risicoprofiel aan de orde stellen en gemotiveerd evalueren. De voor deze beoordeling relevante informatie wordt niet alleen verstrekt door de bestuurders, maar ook door functionarissen van het tweede echelon zoals de risk manager, het hoofd Internal Audit en de compliance officer.

De commissarissen beoordelen de door het bestuur opgestelde risicoanalyse en de wijze waarop risico's worden afgedekt en beheerst, en treden hierover in overleg met de bestuurders. Hierin worden zowel de organisatiedoelstellingen op korte termijn als op de lange termijn betrokken.

Vaak vormt een deel van de commissarissen een Audit Committee dat in detail toeziet op alle in figuur 3 genoemde elementen. Indien aanwezig maakt het Audit Committee een grondige analyse van het risicomanagementsysteem ten behoeve van de discussie in de Raad van Commissarissen.

De raad van commissarissen bespreekt in ieder geval éénmaal per jaar de strategie en de voornaamste risico's verbonden aan de onderneming, de uitkomsten van de beoordeling door het bestuur van de opzet en werking van de interne risicobeheersings- en controlesystemen, alsmede eventuele significante wijzigingen hierin. Van het houden van de besprekingen wordt melding gemaakt in het verslag van de raad van commissarissen. [6]

Bestuurders

Verantwoordelijk, rolmodel en richtinggevend
De bestuurders zijn verantwoordelijk voor het vaststellen, uitvoeren en monitoren van het risicobeleid (inclusief risicobereidheid) en het brede risicomanagementsysteem, en doen hierover verslag aan commissarissen, aandeelhouders, externe toezichthouders (en andere stakeholders).

Het is van groot belang dat het bestuur bij de inrichting van het risicobouwwerk de intrinsieke noodzaak uitdraagt dat de risico's daadwerkelijk beheerst dienen te worden. Ze zorgen voor een cultuur waarin risicobeheersing optimaal tot z'n recht kan komen en bepalen door middel van hun gedrag de *tone at the top*.

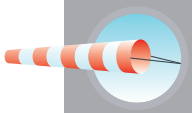
De bestuurders zorgen ervoor dat de risicobeheersing dusdanig is ingericht dat zij tijdig op de hoogte zijn van materiële risico's zodat zij hier de gewenste sturing aan kunnen geven in het licht van de (strategische) doelstellingen en risicobereidheid. Beslissingen die een materiële impact hebben op het risicoprofiel, worden genomen door het bestuur.

Het bestuur richt systematische monitoring op de risicobeheersing in. De resultaten hiervan dienen periodiek binnen het bestuur besproken te worden. Zonodig dienen corrigerende maatregelen te worden geïmplementeerd.

Voorts zorgen de bestuurders voor goede informatieverstrekking en risicorapportage richting commissarissen zodat deze hun rol goed kunnen uitoefenen.

Indien de bestuurders verplicht zijn om een 'In Control-verklaring' af te geven richting het maatschappelijk verkeer en/of externe toezichthouders, dient in overleg met de commissarissen en de externe accountant te worden bepaald wat de inhoud en reikwijdte van die verklaring dient te zijn.

[6] De Nederlandse Corporate Governance Code, III.1.8



(Senior) management

Verantwoordelijk ,praktisch en betrokken
Het senior management is verantwoordelijk voor de feitelijke inrichting van processen (design) waarbij de risicoanalyse en risicobereidheid moet worden omgezet in het feitelijk beheersen van de risico's. Ook hier dienen de lange termijn doelstellingen niet uit het oog verloren te worden. In samenspraak met het bestuur zal risicobereidheid vertaald worden naar risicotoleranties (inclusief zerotolerantie) en stuurvariabelen. Het senior management zal interne beheersingsmaatregelen in de processen en interne controleprocedures inrichten.

Het senior management werkt samen met de bestuurder aan de periodieke actualisering van de risicoanalyse, draagt bij aan een risicobewuste cultuur en werkt mee aan de monitoring van de effectiviteit van de interne beheersing. Eventuele afwijkingen dienen door het senior management aan de bestuurders te worden verklaard en zonodig nemen zij correctieve maatregelen.

In de managementrapportage verantwoorden zij zich niet alleen over de directe bedrijfsresultaten, maar ook over de beheersing van risico's en het risico-management.

De risicomanager

Door effectieve ondersteuning naar zelflerend vermogen
De risicomanager is verantwoordelijk voor het faciliteren van de inrichting van een adequaat risicomanagementsysteem ten behoeve van het bestuur, het senior management en de medewerkers, bijvoorbeeld bij het ondersteunen van risicobeleid, risicoanalyses en risicobereidheid, alsook bij het zorgen voor de noodzakelijke informatie ten behoeve van besluitvorming, monitoring etc.

De risicomanager faciliteert het management bij het monitoren en identificeren van de belangrijkste risico's, het creëren van risicobewustzijn binnen de onderneming en het bewaken van de adequaatheid van de genomen interne beheersingsmaatregelen. Hij draagt bij en neemt deel aan de monitoring van de effectieve werking ervan en legt periodiek verantwoording af aan de bestuurders (en in veel organisaties ook aan de commissarissen). Een onafhankelijke positie en houding van de risicomanager in de organisatie dragen in belangrijke mate bij aan het rendement van risicomanagement, waarbij een cultuur en een omgeving die ze in staat stelt optimaal te functioneren onmisbaar is. Daartoe daagt hij bijvoorbeeld de bestuurders blijvend uit om ook – en misschien wel juist – de meest succesvolle bedrijfsonderdelen kritisch te blijven volgen.

Monitoring-functies

Kritisch en toetsend
De bestuurders en het senior management zijn in eerste lijn verantwoordelijk voor de monitoring van zowel de effectiviteit van de interne beheersingsmaatregelen alsmede van het risicomanagementsysteem *(1st Line of defense)*.

Ook functies als Risicomanagement en Compliance worden daar actief bij betrokken door het uitvoeren van specifieke interne controlprocedures *(2nd Line of defense)*.

In veel ondernemingen wordt daarnaast aanvullende zekerheid verkregen door een onafhankelijke Internal Audit-functie *(3rd Line of defense)*. De Internal Auditfunctie voert – gebaseerd op een risicoanalyse en een meerjaren-auditplan – onafhankelijke onderzoeken uit die met bestuurders en het senior management worden besproken en waarvan de uitkomsten worden gerapporteerd aan de bestuurders. Op geaggregeerd niveau worden ook de commissarissen over de belangrijkste bevindingen geïnformeerd. Deze bevindingen worden dan besproken in het Audit Committee, indien aanwezig.

Externe accountant

Onafhankelijk en kritisch
Buiten de onderneming, in een assurancefunctie, bevindt zich de externe accountant. Hij heeft vanuit zijn activiteiten uit hoofde van de jaarrekeningcontrole veelal aandacht voor het effectief functioneren van (onderdelen van) het risicomanagementsysteem, aangezien dat systeem een belangrijke randvoorwaarde is voor de totstandkoming van betrouwbare managementinformatie en -rapportages. Bovendien voert de externe accountant een marginale beoordeling uit van het jaarverslag van de bestuurders, waartoe ook de risicoparagraaf behoort. Vanuit zijn natuurlijke adviesfunctie zal de externe accountant zijn bevindingen met betrekking tot het risicomanagementsysteem rapporteren aan de bestuurders en de commissarissen.

Externe toezichthouders

Maatschappelijke toetsing
Ondernemingen die externe toezichthouders hebben, zullen zich ook naar deze stakeholders toe verantwoorden over het gevoerde risicomanagement. Veelal hebben toezichthouders normen en standaarden ontwikkeld waaraan in dit verband voldaan dient te worden. Deze normen en standaarden dienen in het risicomanagementsysteem te worden opgenomen en een minimumniveau te vormen bij het inrichten van interne beheersing. De rapportages dienen

ingericht te zijn om verantwoording te kunnen afleggen over de door toezichthouders opgelegde normen en standaarden.

3.4 Gedragscomponenten van risicomanagement

Ondernemen is gecalculeerd risico's nemen. Risicomanagement is daarom geen tabel, systeem of toolbox. Het is het gestructureerde vermogen van organisaties om keuzes te maken over hoe met risico's en kansen wordt omgegaan en hoe daarover wordt gerapporteerd. Uiteindelijk spreken organisaties over het "in de genen hebben van" of "in de bloedvaten hebben" als ultieme doelstelling van risicomanagement. Tabellen, systemen en toolboxen zijn slechts dienstbaar aan die doelstelling.

Effectief risicomanagement is onlosmakelijk verbonden met cultuur en gedrag. Het bestuur van een organisatie bepaalt dit bijvoorbeeld door haar eigen gedrag, haar beloningsbeleid en het wel of niet aanspreken van haar medewerkers. In het beïnvloeden van het gedrag van medewerkers zijn twee uitersten te onderscheiden: afdwingen en inspireren. Voor de laatste stijl geldt dat deze effectiever is dan de eerste aangezien deze eerder zal leiden tot een blijvende gedragsverandering, ook nadat het actief inspireren is gestopt.

Om effectief risicomanagement te bewerkstelligen, is een inspirerende *tone at the top* een absolute must. Alleen afdwingen van het afvinken van checklijsten kan wel schijnzekerheid bieden, maar biedt geen garantie dat de organisatie werkelijk 'in control' is. Uiteindelijk zal de balans tussen harde en zachte factoren bepalend zijn voor de effectiviteit van het risicomanagement (zie ook figuur 2 in paragraaf 3.2).

Bestuurders en senior management dienen zich ervan bewust te zijn dat beloningen invloed hebben op het gedrag van medewerkers. Veelal is dit aspect echter nog onderbelicht in risicomanagementsystemen. Beloningen kunnen zowel een risico vormen voor de organisatie als een effectieve beheersingsmaatregel zijn om risico's te beheersen.

Bij de vaststelling van de hoogte en de structuur van de bezoldiging van bestuurders neemt de raad van commissarissen onder meer de resultaatontwikkeling, de ontwikkeling van de beurskoers van de aandelen en niet-financiële indicatoren die relevant zijn voor de lange termijn doelstellingen van de vennootschap in overweging, een en ander met inachtneming van de risico's die variabele bezoldiging voor de onderneming kan meebrengen.[7]

Risicobewustzijn en risicobereidheid zijn belangrijke pijlers onder risicomanagement. Het bestuur kan voor een 'gezonde' invulling van beide peilers zorgdragen door te voorkomen dat de beloningsstructuur aanleiding geeft tot gedrag met een focus op de korte termijndoelstellingen die mogelijk afleiden van – of zelfs in strijd zijn met – de strategie en lange termijndoelstellingen ('perverse prikkels') . Aan de andere kant kan juist de koppeling van bonussen aan de effectiviteit van het risicomanagement ervoor zorgen dat de organisatie 'in control' is om binnen de grenzen van haar risicobereidheid te blijven, en daarmee de lange termijnresultaten te borgen.

Commissarissen hebben een duidelijke toezichthoudende rol om het gedrag van bestuurders en senior management te evalueren. Tijdige en relevante informatie – zowel richting bestuurders als commissarissen – en heldere besluitvorming spelen hierbij een cruciale rol.

3.5 Maturity model m.b.t. risicomanagement

De "Breakfast groep Risk Management" [8] heeft aan de hand van praktijkervaringen een handzame benchmark opgesteld, waarin de belangrijkste stappen en elementen zijn uitgewerkt in drie niveaus van volwassenheid. Deze is hieronder weergegeven. In de praktijk blijkt veelal dat het hoogste *maturity level* een *top-down approach* vraagt, terwijl de meeste organisaties *bottom-up* beginnen.

[7] Nederlandse corporate governance Code , II.2.3

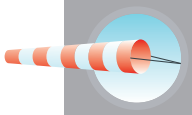
[8] Voor deelnemers van de "Breakfast groep Risk Management" verwijzen wij naar pagina 4.

	Vroege fase **(Belang RM wordt erkend, maar aanpak is gefragmenteerd).**	Groeifase **(Gestructureerde aanpak.)**	Duurzame fase **(Risico-management onderdeel dagelijks bedrijfsvoering).**
Governance			
• Stakeholders	Stakeholders zijn bekend, maar risicomanagement geschiedt puur op compliancebasis.	Interne en externe stakeholders worden gepriori-teerd en gekoppeld aan risico's.	Bedrijf richt zich op behoeften van stakeholders.
• Ownership en leiderschap ('Bestuurders')	Ownership van risicomanagement is gefragmenteerd en onzichtbaar in lijnmanagement. Ook op bestuurs-niveau is geen duidelijke ownership.	Ownership van risicomanagement is formeel vastgelegd op bestuursniveau. In de praktijk is het echter niet altijd zichtbaar binnen het bestuur en de managementni-veaus daaronder.	Ownership van risicomanagement is zeer duidelijk vastgelegd en zichtbaar binnen het bestuur en de hogere manage-ment.
• Framework	Initiële strategie, beleid, processen en risicoterminologie zijn vastgesteld. Uitvoering en rapportage zijn echter gefragmen-teerd en worden getrokken door de holding/centrale stafafdeling	Strategie, beleid, processen, terminologie, rapportage en verantwoordelijkhe-den zijn duidelijk gedefinieerd, gecommuniceerd en geïmplemen-teerd. De processen worden getrokken door de holding/ centrale stafafdeling en de divisies.	Volledige integratie in strategiebepaling en besluitvorming (op alle niveaus). Gebaseerd op behoeften van stakeholders en gefaciliteerd door doorslaggevende *risk-* en *performance-indicatoren.*

	Vroege fase **(Belang RM wordt erkend, maar aanpak is gefragmenteerd).**	Groeifase **(Gestructureerde aanpak.)**	Duurzame fase **(Risico-management onderdeel dagelijks bedrijfsvoering).**
Organisatiestrategie en doelstellingen			
• Risicobereidheid en strategie	Risico's worden niet formeel gedefinieerd in relatie tot de strategie.	Risico's worden gedefinieerd op basis van geselecteerde bedrijfsdoel-stellingen. (Risicobereidheid wordt later in het proces behandeld, bijvoorbeeld in de risk response- en monitoringfase.)	Strategie en risicobereidheid worden gezien als twee zijden van dezelfde medaille en worden vertaald naar de risico-tolerantie niveaus en volledig geïntegreerd in de management-systemen.
• Communicatie	Zeer beperkte communicatie richting organisatie over strategie en doelstellingen.	Formele communicatie.	Proactieve communicatie door de relevante leden van het manage-ment gebaseerd op hun *awareness* en handelen op het gebied van risico-management.
• Cultuur/houding	'Afvinkmentaliteit'	Frequent bewijs dat er op basis van risicomanagement strategie wordt gehandeld.	Risicomanagement is onderdeel van de belonings-structuur en beloningsrisico's worden beheerst. Handelen op basis van risicomanagement is zichtbaar in besluitvormings-processen.

	Vroege fase **(Belang RM wordt erkend, maar aanpak is gefragmenteerd).**	Groeifase **(Gestructureerde aanpak.)**	Duurzame fase **(Risico-management onderdeel dagelijks bedrijfsvoering).**
Risico-identificatie			
• Reikwijdte van risico-management	Financiële rapportage.	Operationele risico's en compliance.	Alle organisatie en strategische doelstellingen.
• Inbedding	Eenmalige en losstaande exercities.	Periodiek, geïntegreerd, onderdeel van de planning- en control cyclus.	Frequentie wordt gebaseerd op de snelheid van veranderingen bovenop de planningcycli.
• Mate van implementatie in de organisatie	Bestuur en management-niveaus daaronder.	Bestuur, management-niveaus daaronder, strategische business units (SBU's) en Corporate stafafdelingen.	Bestuur, hoger management, strategic business units (SBU's), Corporate Functions en situationeel bij afdelingen, projecten en functies.
• Ownership	Risicobeoordeling uitgevoerd door stafmedewerkers.	Risicobeoordeling uitgevoerd door lijnmanagement (bijgestaan door stafmedewerkers).	Risicobeoordeling in continuïteit uitgevoerd door lijnmanagement.
• Analyse (kwalitatief/ kwantitatief)	Van tevoren vastgestelde risico's worden beoordeeld.	Risicoscenario's worden vast-gesteld door lijnmanagement met focus op de toekomst.	Risicoscenario's worden vast-gesteld door lijnmanagement met focus op de toekomst, analyses van dieperliggende oorzaken geprioriteerd en gekwantificeerd (waar mogelijk).

	Vroege fase **(Belang RM wordt erkend, maar aanpak is gefragmenteerd).**	Groeifase **(Gestructureerde aanpak.)**	Duurzame fase **(Risico-management onderdeel dagelijks bedrijfsvoering).**
Risicorespons			
• Besluitvorming	Geen formeel besluitvormings-proces.	Risico's worden deels meegenomen in de besluitvor-ming. Besluiten worden genomen voor de meest relevante risico's .	Besluiten worden genomen voor de meest relevante risico's en risico's zijn de achter-liggende drijfveren voor het alledaagse management-proces.
• Acties	Geen aanvullende acties ondernomen n.a.v. van geïdentificeerde risico's.	Specifieke acties ondernomen n.a.v. de meeste relevante risico's.	Acties zijn geïntegreerd in management-systemen.
• Interne beheersing	Alleen proces-beschrijvingen.	Verzuilde benadering van interne beheersing, management controls, process controls en handleidingen.	Geïntegreerd risk en management framework. (geïntegreerde beheersing en monitoring).



	Vroege fase **(Belang RM wordt erkend, maar aanpak is gefragmenteerd).**	Groeifase **(Gestructureerde aanpak.)**	Duurzame fase **(Risico-management onderdeel dagelijks bedrijfsvoering).**
Monitoring			
• Monitoren van de risicobeheersing	Vindt niet plaats.	Uitgevoerd door (naast) hoger management, ondersteund door de afdelingen risicomanagement, compliance en eventueel Internal Audit voor aanvullende zekerheid.	Als in groeifase; volledig geïntegreerd in management-systeem. Internal Audit zorgt voor voor aanvullende zekerheid.
• Monitoren van de governance	Vindt niet plaats.	Door (naast) hoger management, ondersteund door de afdelingen risicomanagement, compliance en Internal Audit voor aanvullende zekerheid.	Als in groeifase; volledig geïntegreerd in management-systeem. Internal Audit zorgt voor aanvullende zekerheid.

	Vroege fase **(Belang RM wordt erkend, maar aanpak is gefragmenteerd).**	Groeifase **(Gestructureerde aanpak.)**	Duurzame fase **(Risico-management onderdeel dagelijks bedrijfsvoering).**
Rappportage			
• Interne risico-rapportage	Alleen omwille van externe compliance.	Geïntegreerd in organisatie rapportagestructuur.	Trendanalyses, risico-thema's, voornaamste risk en performance indicators worden (tijdig) intern gerapporteerd en dienen als basis voor besluit-vorming.
• Externe risico-rapportage	Niet gebaseerd op resultaat van risicomanagement-proces.	Voornaamste risico's worden gerapporteerd, maar zijn niet noodzakelijk geprioriteerd en/of volledig transparant.	Geprioriteerd en geactualiseerd. Transparantie ter ondersteuning van waardecreatie.
• 'In control'-statement	Niet gebaseerd op risicomanagement-proces.	Gebaseerd op risicomanagement-proces en financiële rapportage.	Gebaseerd op geborgde kwaliteit van het brede risicomanagement-proces.