

Herziene uitgave. Januari 2006.

# Risicomanagement

De praktijk in Nederland.



# Voorwoord

Door Prof. dr. J.G.M. Frijs,  
Voorzitter Monitoring Commissie Corporate Governance Code

Het op gestructureerde wijze identificeren, analyseren en managen van risico's wordt steeds meer gemeengoed binnen Nederlandse organisaties. Dat is één van de conclusies die getrokken mag worden uit het onderzoek waarvan in dit rapport de resultaten worden gepubliceerd.

PricewaterhouseCoopers en de Rijksuniversiteit Groningen hebben onderzoek gedaan naar de wijze waarop in organisaties in Nederland risicomanagement wordt bedreven. Een naar mijn mening zeer actueel en relevant onderwerp. Ik ben dan ook verheugd dat risicomanagement meer en meer zijn ingang lijkt te vinden, zowel in het Nederlandse bedrijfsleven als de overheid en non-profit sector. We weten allen wat de gevolgen kunnen zijn van ontoereikende risicobeheersing; daar zijn we in de afgelopen jaren immers meerdere keren mee geconfronteerd. Daarom is het mijns inziens goed dat ook op het niveau van bestuurders het onderwerp risicomanagement steeds meer begint te leven.

Niet in de laatste plaats hebben de ontwikkelingen op het gebied van corporate governance bijgedragen aan de groeiende belangstelling voor risicomanagement. Adequate risicobeheersing is één van de pijlers van goed ondernemings-bestuur. In mijn rol als voorzitter van de Monitoring Commissie Corporate Governance Code heb ik de taak om de opvolging van de aanbevelingen van de Commissie Tabaksblat te bewaken. De principes en 'best practices' aangaande interne beheersing en risicomanagement hebben in dit kader nadrukkelijk de aandacht van de Commissie. Met belangstelling volg ik de discussies die hierover plaatsvinden. Wat uit deze discussies duidelijk blijkt is dat er nog geen eenduidige interpretatie is van het begrip 'in-control'. Er zal in de loop van de tijd meer duidelijkheid moeten ontstaan bij de materiële invulling van dit begrip.

Een ander opvallend punt uit het onderzoek is wat mij betreft de tevredenheid die bestaat over de effectiviteit van in de organisaties aanwezige beheerssystemen. Er bestaat een redelijke mate van vertrouwen dat de aanwezige beheerssystemen de organisatie voor grote schade zullen behoeden. De grote bedragen die organisaties uitgeven aan risicomanagement – met name bij beursgenoteerde ondernemingen loopt dit al gauw in de miljoenen – lijken aldus in de ogen van de respondenten op het onderzoek hun doel te bereiken. Dit moet een geruststellende gedachte zijn voor controllers en financieel managers onder u die de budgetten die voor risicomanagement worden uitgetrokken de afgelopen jaren alleen maar hebben zien groeien.

Als er iets is dat dit rapport duidelijk maakt is het wel dat risicomanagement geen hype is: 'risicomanagement is here to stay'. Welke kant het precies op zal gaan en met welke vaart is echter nog niet geheel voorspelbaar. U wordt als lezer van dit rapport in ieder geval de gelegenheid geboden om het risicomanagement in uw eigen organisatie te spiegelen aan wat andere organisaties doen. Dit zal u helpen bij het uitstippelen van de juiste koers voor uw organisatie. Daar wens ik u veel succes bij!

Amsterdam, januari 2006

# Inhoudsopgave

Toelichting onderzoek en hoofdbevindingen	6
---	---

## Deel I

Inleiding	9
-----------	---

<b>1.1 Toenemende aandacht voor risicomanagement</b>	<b>10</b>
1.1.1 Corporate governance als katalysator voor risicomanagement	10
1.1.2 Code Tabaksblad brengt wettelijke verankering van eisen aan risicomanagement	10
1.1.3 Grote diversiteit in 'in-control rapportages' in jaarverslagen 2004	11
1.1.4 Ontwikkelingen in Europees perspectief	11
1.1.5 Branchespecifieke ontwikkelingen	12
1.1.6 Enterprise Risk Management als 'Business Enabler'	12
1.1.7 Acht COSO-componenten van Enterprise Risk Management	13
<b>1.2 Enterprise Risk Management</b>	<b>14</b>
1.2.1 Balanceren tussen risico en opbrengst	14
1.2.2 Interne beheersing beheersbaar gemaakt	14
1.2.3 De toegevoegde waarde van Enterprise Risk Management	15
1.2.4 Valkuilen bij de toepassing van Enterprise Risk Management	16

## Deel II

Het onderzoek en de resultaten	19
--------------------------------	----

<b>2.1 Onderzoeksopzet</b>	<b>20</b>
2.1.1 Doelstelling van het onderzoek	20
2.1.2 Aanpak van het onderzoek	20
2.1.3 Profiel van de respondenten	20
<b>2.2 Risicomanagement strategie</b>	<b>21</b>
2.2.1 Risicomanagement strategie bepalend voor inrichting risicomanagement systeem	21
2.2.2 Risicomanagement beleid vaak niet expliciet geformuleerd	22
2.2.3 Generieke risicomanagement standaarden door veel organisaties gebruikt	23

<b>2.3</b>	<b>Identificeren en analyseren van risico's</b>	<b>24</b>
2.3.1	Vijf generieke stappen te herkennen in elk risicomanagement proces	24
2.3.2	Integrale risicoanalyse voor de meeste organisaties nieuw fenomeen	24
2.3.3	Jaarlijkse risicoanalyse meest gebruikelijk	25
2.3.4	Risicoanalyse veelal met behulp van combinatie van technieken	26
2.3.5	Vooraf grotere organisaties maken gebruik van elektronische hulpmiddelen	27
<b>2.4</b>	<b>Beheersen van risico's</b>	<b>29</b>
2.4.1	Vier manieren om op risico te reageren	29
2.4.2	Aanwezige beheerssystematieken worden doorgaans als effectief ervaren	29
2.4.3	De bedragen die organisaties aan risicomanagement uitgeven zijn aanzienlijk	30
2.4.4	Er bestaat een redelijk vertrouwen in de huidige kwaliteit van de beheersing	30
<b>2.5</b>	<b>Rapporteren van risico's</b>	<b>31</b>
2.5.1	Risicorapportage veelal ingebouwd in planning & controlcyclus	31
2.5.2	In-control verklaringen vooral in gebruik bij beursgenoteerde ondernemingen	33
2.5.3	Externe rapportage over risicomanagement nog niet in lijn met code Tabaksblad	34
<b>2.6</b>	<b>Taken en verantwoordelijkheden</b>	<b>36</b>
2.6.1	Taken en verantwoordelijkheden op verschillende wijzen vastgelegd	36
2.6.2	Risicomanagement functie vaak belegd bij finance & control	36
2.6.3	De controller speelt een belangrijke rol in de uitvoering van risicomanagement	37
2.6.4	In veel organisatie worden managers getraind in risicomanagement	38

## Deel III

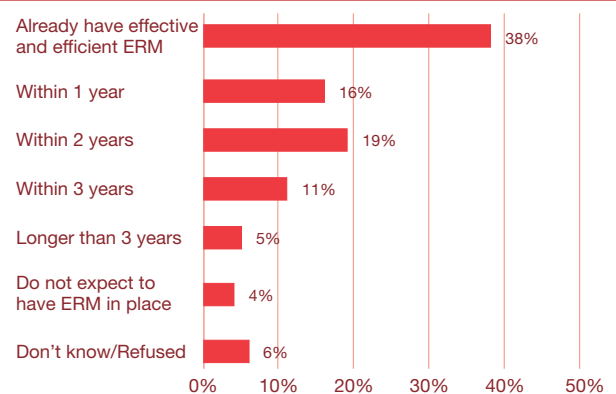
	<b>De visie van bestuurders op risicomanagement</b>	<b>41</b>
3.1	Robert-Jan van de Kraats, Chief Financial Officer, Randstad Holding	42
3.2	Chris Spanjaard, Hoofddirecteur, Informatie Beheer Groep	44
3.3	Frank Sonnemans, Chief Financial Officer, Provimi	46
3.4	Hans Leenaars, lid Raad van Bestuur, Bank Nederlandse Gemeenten	48

# Toelichting onderzoek en hoofdbevindingen

Het onderwerp risicomanagement staat meer dan ooit in de belangstelling. Onder meer als gevolg van toenemende druk vanuit de omgeving zijn veel organisaties bezig met het vormgeven van een gestructureerd proces van identificeren, analyseren, managen en rapporteren van risico's op alle niveaus in de organisatie. Dit is een mondiale ontwikkeling, zo blijkt ook uit een wereldwijde CEO survey die PricewaterhouseCoopers in 2004 heeft uitgevoerd naar het onderwerp risicomanagement. Zoals onderstaand kader laat zien zegt 38% van de CEO's dat zij reeds een effectief Enterprise Risk Management (ERM) systeem hebben en nog eens 46% zegt dat in de komende drie jaren te zullen realiseren.



PricewaterhouseCoopers Global CEO survey 2004



Nederland loopt in de pas met deze mondiale ontwikkeling. Ook hier is een groot aantal organisaties al enige jaren geleden begonnen met de invoering van gestructureerd risicomanagement en zijn nog meer organisaties daar recentelijk mee begonnen. Elke organisatie kiest hierbij zijn eigen specifieke invulling, gebaseerd op de eisen die er worden gesteld en de wensen van het management. Toch, en misschien wel juist daarom, bestaat er een grote behoefte bij organisaties naar inzicht in hoe andere organisaties met het onderwerp omgaan. Dit helpt immers bij het maken van de vele keuzes op weg naar volwassen risicomanagement. Aan deze behoefte naar spiegeling van de eigen organisatie met andere organisaties proberen PricewaterhouseCoopers en de Rijksuniversiteit Groningen tegemoet te komen door de publicatie van onderhavig rapport.

Eind 2004 heeft PricewaterhouseCoopers in samenwerking met de Postdoctorale Controllersopleiding van de Rijksuniversiteit Groningen het initiatief genomen tot het uitvoeren van een onderzoek naar de praktijk van risicomanagement in Nederland. Door middel van een enquête onder leden van het Controllers Instituut<sup>1</sup> is een groot aantal organisaties ondervraagd naar de wijze waarop zij invulling geven aan risicomanagement. Het gaat daarbij om concrete keuzes als de frequentie van risicoanalyses, het gebruik van methodieken en hulpmiddelen en de betrokkenheid van diverse functionarissen.

<sup>1</sup> Wij danken het Controllers Instituut voor de bereidheid aan dit onderzoek mee te werken.

De resultaten van het onderzoek worden in dit rapport getoond. Daarbij wordt op vele plekken onderscheid gemaakt naar branche, omzet en andere onderscheidende factoren. Hieronder volgt een samenvatting van de belangrijkste onderzoeksresultaten.

- Slechts 39% van de organisaties beschikt over een formeel risicomanagement beleid. Van alleen de beursgenoteerde ondernemingen is dat 56%. Bij een uitsplitsing naar branche valt op dat de financiële dienstverlening (61%) en de energie & utilities bedrijven (53%) beduidend vaker een formeel risicomanagement beleid hebben dan andere branches en in het bijzonder de overheid en non-profit sector (11%) (pagina 22, 2.2.2).
- 63% van de organisaties maakt gebruik van een openbaar beschikbare standaard voor risicomanagement bij het vormgeven van het eigen risicomanagement. In de overheid & non-profit sector is dit zelfs 79%. COSO is verreweg de meest gebruikte openbare standaard. Ruim driekwart van de organisaties die een standaard gebruiken noemt COSO (pagina 23, 2.2.3).
- In 66% van de organisaties worden reeds integrale risico-identificaties en –analyses uitgevoerd. 47% daarvan is daar in de afgelopen drie jaren mee begonnen terwijl 19% er al wat langer mee bezig is. 34% van de organisaties heeft nog nooit een integrale risico-identificatie en –analyse uitgevoerd. 26% daarvan is dat wel van plan (pagina 25, 2.3.2).

- De meest voorkomende frequentie waarmee risicoanalyses worden uitgevoerd is eens per jaar (34%), gevolgd door eens per kwartaal (26%). Eens per half jaar komt beduidend minder voor (7%). Bij grote investeringsbeslissingen (19%) en bij grote projecten (26%) worden nog slechts in beperkte mate risicoanalyses uitgevoerd (pagina 25-26, 2.3.3).
- De meeste gebruikte technieken voor risico-identificatie en –analyse zijn questionnaires/checklists (52%), Interviews (47%) en documentstudie (40%). De meeste organisaties gebruiken meerdere technieken (pagina 26, 2.3.4).
- Aanwezige beheerssystemen worden doorgaans als effectief ervaren. Het meest effectief zijn de planning & controlsystematiek en de administratieve organisatie / interne controle. Maar ook bijvoorbeeld het werken met KPI'en, het uitvoeren van risicoanalyses en het hebben van een gedragscode worden positief beoordeeld (pagina 29, 2.4.2).
- De onderzochte organisaties hebben er gemiddeld genomen 65% vertrouwen in dat de aanwezige beheersmaatregelen de organisatie voor aanzienlijke financiële schade zullen behoeden. De verschillende branches variëren hierin nauwelijks (pagina 30, 2.4.4).
- Risicomanagement wordt vaak geïntegreerd in de planning & controlcyclus. Bij 77% van de organisaties is dit geheel (25%) of gedeeltelijk (52%) het geval. Bij de grote organisaties (> 1 miljard omzet) is in 89% van de gevallen risicomanagement geheel of gedeeltelijk geïntegreerd in de planning & controlcyclus (pagina 31, 2.5.1).
- Binnen beursgenoteerde ondernemingen wordt veel gewerkt met interne in-control verklaringen. Bij 71% van de beursgenoteerde bedrijven geeft de Raad van Bestuur een dergelijke verklaring af. Bij 60% daarvan wordt dit ook van de tweede managementlaag verlangd. In 52% van de beursgenoteerde ondernemingen geven ook de managers op het derde echelon een verklaring af en bij 22% ook het vierde echelon. In 10% van de beursgenoteerde ondernemingen worden in-control verklaringen afgegeven door meer dan de eerste vier managementlagen. In niet-beursgenoteerde ondernemingen en in de overheid & non-profit sector is het werken met interne in-control verklaringen veel minder gemeengoed (pagina 33, 2.5.2).
- De risicomanagement functie is in de meeste organisaties expliciet belegd. Bij grote ondernemingen (> 1 miljard omzet) is dit zelfs bij 97% het geval. Bij het grootste deel daarvan (40%) is de risicomanagement functie belegd bij de finance & control afdeling. 26% van de grote ondernemingen hebben een zelfstandige risicomanagement afdeling ingericht. Bij 16% wordt deze rol vervuld door de internal audit afdeling. Bij kleine en middelgrote organisaties is de risicomanagement functie, voorzover aanwezig, in verreweg de meeste gevallen bij de finance & control afdeling belegd (pagina 36-37, 2.6.2).

Het onderzoek is namens PricewaterhouseCoopers uitgevoerd door Leen Paape en Dennis Freriksen en namens de Rijksuniversiteit Groningen door Dirk Swagerman.

Voor meer informatie kunt u contact opnemen met:



Leen Paape  
020 568 43 00  
leen.paape@nl.pwc.com

Leen is binnen de Advisorypraktijk van PricewaterhouseCoopers verantwoordelijk voor dienstverlening op het gebied van corporate governance, risicomanagement en compliance.



Dirk Swagerman  
06 260 18 513  
d.swagerman@worldonline.nl

Dirk is deeltijd hoogleraar controlling aan de economische faculteit van de RuG. Hij verricht zelfstandig advieswerk op het terrein van de organisatie en inrichting van de financiële functie.



# Deel I

## Inleiding

De aandacht voor risicomanagement bestaat geruime tijd. Echter nog nooit is de aandacht zo sterk geweest als in de afgelopen jaren. Debacles bij beursgenoteerde ondernemingen en de daarop volgende corporate governance codes in diverse landen hebben een katalyserend effect gehad. Daarnaast zien ondernemingen ook steeds meer de toegevoegde waarde van bewust en expliciet risicomanagement. In dit deel van het rapport worden actuele ontwikkelingen op het gebied van corporate governance en risicomanagement geschetst. Tevens wordt ingegaan op de voordelen van het op gestructureerde wijze identificeren, analyseren en managen van risico's.

# 1.1 Toenemende aandacht voor risicomanagement

## 1.1.1 Corporate governance als katalysator voor risicomanagement

Zelden heeft het onderwerp risicomanagement zo veel aandacht gehad in bestuurskamers als in de afgelopen drie jaren. Na de boekhoudschandalen waar we enkele jaren geleden zowel op internationaal als nationaal niveau mee geconfronteerd werden is er een grote druk ontstaan op ondernemingen om het managen van risico's serieus te nemen en een adequaat stelsel van beheersingsmaatregelen in te richten en te onderhouden. Het geschonden vertrouwen van de maatschappij - en in het bijzonder de financiële wereld - diende te worden herwonnen. De weg naar hernieuwd vertrouwen werd in diverse landen uiteengezet in nieuwe of aangepaste wet- en regelgeving op het gebied van corporate governance. Hiermee verdween de vrijblijvendheid en kwam de noodzaak voor beursgenoteerde ondernemingen om de veelal binnen de organisatie al lopende initiatieven op het gebied van risicomanagement - het nut daarvan werd namelijk wel ingezien - in een stroomversnelling te brengen en aan te passen aan de specifieke eisen vanuit de wet- en regelgeving. Als afgeleide van deze ontwikkelingen heeft risicomanagement ook binnen grotere, niet-beursgenoteerde ondernemingen en binnen de publieke sector steeds nadrukkelijker de aandacht gekregen.

Een pregnant voorbeeld van de toegenomen aandacht voor risicomanagement zijn de grote inspanningen die door aan de Amerikaanse beurs genoteerde ondernemingen worden ondernomen om te voldoen aan de eisen die vanuit de 'Sarbanes-Oxley Act of 2002' worden gesteld. Met name sectie 404 'Management assessment of internal controls' vergt aanzienlijke inspanningen en raakt de gehele organisatie. En dan te bedenken dat het hier nog slechts gaat om het waarborgen van een getrouwe externe financiële verslaggeving. Risico's voor bijvoorbeeld het behalen van de strategische doelstellingen of de effectiviteit van processen worden niet in beschouwing genomen.

## 1.1.2 Code Tabaksblat brengt wettelijke verankering van eisen aan risicomanagement

De eind 2003 verschenen Nederlandse corporate governance code ('code Tabaksblat') gaat wat betreft reikwijdte verder dan Sarbanes-Oxley. In de code wordt gesteld dat als onderdeel van het 'interne risicobeheersings- en controlesysteem' een vennootschap onder meer risicoanalyses uit dient te voeren van de 'operationele en financiële doelstellingen'. In tegenstelling tot Sarbanes-Oxley - waar de 'Public Company Accounting Oversight Board'(PCAOB) gedetailleerde uitwerking geeft van de wijze waarop dient

te worden voldaan aan de in de wet gestelde eisen - geeft de code Tabaksblat geen nadere richtlijnen ten aanzien van de inrichting van het interne risicobeheersings- en controlesysteem. Evenzo worden ondernemingen grotendeels vrijgelaten in de wijze waarop zij in hun jaarverslag rapporteren over het interne risicobeheersings- en controlesysteem.

De code Tabaksblat vervangt het rapport "Corporate Governance in Nederland; De Veertig Aanbevelingen" uit 1997 van de commissie Peters. In tegenstelling tot de 40 aanbevelingen van Peters kent de code Tabaksblat wel een wettelijke basis. Ondernemingen gezeteld en beursgenoteerd in Nederland zijn verplicht elk jaar in hun jaarverslag gemotiveerd uit te leggen of en zo ja waarom en in hoeverre zij afwijken van de best practice bepalingen van de code. De wettelijke verankering heeft plaatsgevonden door opname van deze regel van 'pas toe of leg uit' in boek 2 van het Burgerlijk Wetboek.

Er is een Monitoring Commissie ingesteld die tot taak heeft om de actualiteit en bruikbaarheid van de code te bevorderen en naleving te bewaken. De Commissie zal deze taak uitvoeren door ten minste jaarlijks te inventariseren op welke wijze en in welke mate de codevoorschriften door de Nederlandse beursgenoteerde vennootschappen worden nageleefd, door zich op de hoogte te stellen van de internationale ontwikkelingen en gebruiken op het terrein van corporate governance en door het signaleren van leemtes of onduidelijkheden in de code. De Commissie heeft geen bevoegdheid om de code zelfstandig te wijzigen. Er zal te zijner tijd een ad-hoc commissie worden ingesteld die de code integraal zal evalueren (naar verwachting drie jaar na inwerkingtreding van de code) en zonodig de regering over eventuele wijzingen zal adviseren.

Een vraag die bij velen momenteel leeft is of wettelijke verankering van eisen ten aanzien van risicomanagement wel de oplossing is. Een gevaar dat hier namelijk in schuilt is dat ondernemingen het onderwerp gaan benaderen als iets dat nou eenmaal moet; iets dat je moet doen om toezichhouders tevreden te stellen. Dit kan een 'afvinkmentaliteit' veroorzaken. In dat geval wordt daadwerkelijke toegevoegde waarde niet gerealiseerd en misschien ook niet eens nagestreefd. En dat zou zonde zijn, want adequate risicobeheersing is immers wel degelijk iets dat van invloed is op de waarde van een onderneming. U investeert uw geld bij voorkeur toch ook in een organisatie die weet welke risico's het loopt en die daar bewust mee omgaat? In dat kader is het vreemd dat het onderwerp risicomanagement in de 'beleggingswereld' relatief weinig de aandacht heeft. Beleggers tonen tot op heden maar zeer beperkt interesse

in het onderwerp, terwijl zij juist degenen zijn die er direct van profiteren. Indien ook de (institutionele) belegger zijn interesse in het onderwerp uitdraagt zal dit een belangrijke impuls betekenen voor de ontwikkeling van risicomanagement in het bedrijfsleven. Pas zodra ondernemingen zich in de ogen van beleggers en analisten kunnen differentiëren door aantoonbaar te maken dat zij zorgvuldig en bewust omgaan met risico's, zal risicomanagement daadwerkelijk worden omarmd door bestuurders van ondernemingen; en dan niet meer alleen omdat het moet, maar simpelweg omdat het wat oplevert.

Bovenstaande gedachte vindt steeds breder ingang bij de verschillende betrokken partijen. Er worden diverse initiatieven ontplooid om de beleggingswereld meer bewust te maken van de waarde van adequaat risicomanagement. Ook de Monitoring Commissie Corporate Governance Code zal hier een rol in vervullen.

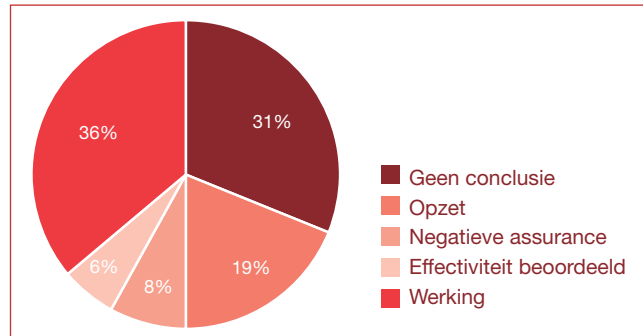
### 1.1.3 Grote diversiteit in 'in-control rapportages' in jaarverslagen 2004

De code Tabaksblat laat ondernemingen grotendeels vrij in de wijze waarop zij in hun jaarverslag rapporteren over het interne risicobeheersings- en controlesysteem. Dit heeft er toe geleid dat in de jaarverslagen over 2004 van aan de Amsterdamse beurs genoteerde ondernemingen een diversiteit aan 'in-control rapportages' te vinden is, zo blijkt uit een door PricewaterhouseCoopers uitgevoerde studie naar 80 jaarverslagen van Nederlandse beursgenoteerde ondernemingen (24 AEX, 23 Midkap en 24 lokale fondsen). De in-control rapportages in de jaarverslagen verschillen ten aanzien van reikwijdte, inhoud en bewoordingen. Verschillen betreffen met name het onderscheid tussen een beoordeling van de opzet en de werking van het interne risicobeheersings- en controlesysteem en het wel of niet verbinden van conclusies aan die beoordeling. Philips bijvoorbeeld spreekt zich enkel uit over de opzet en het bestaan van het interne risicobeheersings- en controlesysteem, terwijl bijvoorbeeld Akzo Nobel stelt dat het interne risicobeheersings- en controlesysteem adequaat is en effectief heeft gewerkt. Daarbij merkt Akzo Nobel overigens wel op dat deze conclusie niet inhoudt dat de effectiviteit van het systeem van interne beheersmaatregelen ten behoeve van een betrouwbare financiële verslaggeving is beoordeeld op de wijze als bedoeld in sectie 404 van de Sarbanes-Oxley Act. Aan de Sarbanes-Oxley Act hoefde Akzo Nobel – als 'Foreign Private Issuer' – immers ook nog niet te voldoen.

De bestudeerde in-control rapportages (of risicomanagement rapportages) zijn grofweg in te delen in vijf categorieën:

- a. Alleen een beschrijving, geen conclusie;
- b. Beschrijving en geen conclusie, maar wel een verklaring dat de werking is beoordeeld;
- c. Conclusie ten aanzien van de opzet;
- d. 'Negative assurance' ten aanzien van de opzet en/of werking;
- e. Conclusie over de werking.

Figuur 1.1 In-control rapportages in jaarverslagen 2004



Figuur 1.1 laat de verdeling naar deze categorieën zien. Maar liefst 36% van de onderzochte ondernemingen doet een uitspraak over de werking van het interne risicobeheersings- en controlesysteem. Dat is opvallend omdat dit een vrij vergaande uitspraak is. De code Tabaksblat beperkt zich immers niet, zoals de Sarbanes-Oxley Act, tot 'controls over financial reporting'. Ook de beheersmaatregelen bedoeld om bijvoorbeeld de operationele en strategische doelen veilig te stellen maken onderdeel uit van het interne risicobeheersings- en controlesysteem zoals bedoeld in de code Tabaksblat. Gelet op de inspanningen die aan de Amerikaanse beurs genoteerde ondernemingen momenteel moeten leveren om, in het kader van de Sarbanes-Oxley Act, de werking van de 'controls over financial reporting' vast te stellen, moet de inspanning van deze 36% van de onderzochte ondernemingen dus zeer fors zijn geweest. Het moge duidelijk zijn dat daar vraagtekens bij kunnen worden gezet. Het lijkt er meer op dat er hier sprake is van verschillende normstelling ten aanzien van de vraag wat 'in-control' zijn nu eigenlijk inhoudt. Er zal in de loop van de tijd dan ook meer duidelijkheid moeten ontstaan bij de materiële invulling van dit begrip.

Aan de andere kant van het spectrum kiest 31% van de ondernemingen ervoor om geen conclusie af te geven, maar slechts een beschrijving te geven van het interne risicobeheersings- en controlesysteem van de onderneming. Een begrijpelijke keuze gezien het werk dat in de meeste ondernemingen nog verzet moet worden om tot een gefundeerde conclusie ten aanzien van de adequate opzet en effectieve werking te kunnen komen. Nog eens 6% doet hetzelfde, maar merkt daarbij op dat de werking wel beoordeeld is. Het resultaat van die beoordeling wordt niet prijs gegeven. 19% geeft een conclusie die zich beperkt tot de opzet en 6% doet een uitspraak over de werking in de vorm van 'negative assurance' over de opzet en/of de werking ('ons is niet gebleken dat de werking niet goed is geweest').

### 1.1.4 Ontwikkelingen in Europees perspectief

In andere Europese landen bestaan al langer corporate governance codes met een wettelijke basis. Sinds 1998 bestaat in Duitsland de 'Gesetz zur Kontrolle und Transparenz im Unternehmensbereich' (KonTraG). Één van de belangrijkste verplichtingen uit KonTraG is dat de ondernemingsleiding een risicomanagement systeem dient op te

zetten, waarmee risico's voor de onderneming vroegtijdig gesignaleerd kunnen worden. Het management dient hierover periodiek te rapporteren aan de Raad van Commissarissen. In aanvulling op KonTraG is de 'Deutsche Corporate Governance Kodex'<sup>2</sup> ingesteld welke in 2002 eveneens via een regel van 'pas toe of leg uit' wettelijk is verankerd.

In het Verenigd Koninkrijk verscheen in 1999 het 'Turnbull-report'. Dit rapport is een uitwerking van de bepalingen over internal control die zijn opgenomen in de 'Combined Code of the Committee on Corporate Governance' uit 1998 van de commissie Hampel. In die code staat dat de ondernemingsleiding een adequaat interne beheersingssysteem moet onderhouden en dat dit jaarlijks dient te worden geëvalueerd. In 2003 is een hernieuwde Combined Code<sup>3</sup> verschenen waarin nieuwe ontwikkelingen en inzichten op het gebied van corporate governance zijn verwerkt. In de hernieuwde Combined Code wordt opnieuw naar het Turnbull rapport verwezen voor mogelijke invulling van de principes inzake interne beheersing en risicomanagement.

In Frankrijk is in 2003 de 'Loi sur la Sécurité Financière' (LSF) verschenen. Ten aanzien van het onderwerp risicomanagement is de belangrijkste implicatie van de LSF dat aan de Franse beurs genoteerde ondernemingen in hun jaarverslag een verklaring op moeten nemen over hun systeem van risicobeheersing. Deze dient vergezeld te gaan van een accountantsverklaring.

Sinds het verschijnen van KonTraG en Turnbull in respectievelijk Duitsland en het Verenigd Koninkrijk heeft de toepassing van risicomanagement in organisaties zich sterk ontwikkeld in beide landen. De verwachting is dat Nederland een vergelijkbare ontwikkeling door zal maken. Natuurlijk is risicomanagement niet nieuw in Nederland. Eisen vanuit wet- en regelgeving zijn immers niet de enige drijfveren voor het inrichten van een gestructureerd risicomanagement systeem. Bovendien opereren Nederlandse bedrijven in een internationale context waarin het bewust en expliciet identificeren en managen van risico's meer en meer 'bon usance' is geworden. De wettelijke verankering van de code Tabaksblat zorgt ervoor dat de ingezette ontwikkeling wordt gecontinueerd en geïntensiveerd. Tevens is onder grotere, niet-beursgenoteerde ondernemingen en publieke organisaties een duidelijke beweging in dezelfde richting waarneembaar.

### 1.1.5 Branchespecifieke ontwikkelingen

Naast de algemene corporate governance codes zijn er binnen specifieke sectoren ook ontwikkelingen die katalyserend werken op de ontwikkeling van risicomanagement binnen de betreffende sector. Koploper op dit terrein is de financiële dienstverlening met in Nederland de door De Nederlandsche Bank uitgevaardigde 'Regeling Organisatie en Beheer' (ROB) en in internationaal verband het tweede

Bazelse Kapitaalakkkoord (Bazel II). Bazel II biedt banken de gelegenheid om een lager kapitaalbeslag aan te houden. Voorwaarde is dat het risicomanagement van de bank aan bepaalde eisen voldoet. Eenzelfde situatie gaat gelden voor verzekeraars onder de nog in ontwikkeling zijnde Solvency II regelgeving. Ook heeft De Nederlandsche bank aangekondigd dat er een ROB voor verzekeraars zal gaan verschijnen.

Binnen de rijksoverheid heeft risicomanagement nadrukkelijk zijn intrede gedaan als uitvloeisel van de in 1999 ingevoerde nieuwe wijze van begroten en verantwoorden onder de noemer 'Van Beleidsbegroting tot Beleidsverantwoording' (VBTB). Risicoanalyses en risicomanagement zijn tot norm verheven voor het besturen en laten functioneren van overheidsinstellingen.

De rijksbrede eisen betreffen o.a. een periodieke (jaarlijkse) risicoanalyse, periodieke op- en bijstelling van het bedrijfsvoeringbeleid en bedrijfsvoeringplannen, een adequate inbedding van risicomanagement in de planning- en controlcyclus, het laten aansluiten van een auditjaarplan op de risicoanalyse, en het onderbrengen van kwaliteitsborging binnen het management control systeem. Denk hierbij aan zaken als de borging van deskundigheid, toetsing van beheerskaders en -maatregelen en borging van de oplevering van betrouwbare (deel)mededelingen over de bedrijfsvoering.

Ook op het niveau van de lokale overheid, de provincies en gemeenten, zijn de principes van risicomanagement geïntroduceerd. Zo wordt bijvoorbeeld in de nieuwe gemeentewet (2004) het managen van risico's behandeld en verwachten gemeenteraden van haar colleges dat zij zich verantwoorden over de wijze waarop zij de risico's gemanaged hebben. Hierbij wordt aangestuurd op een bewuste afweging van risico's en de wijze waarop deze kunnen worden weggenomen of verkleind door het nemen van beheersmaatregelen.

### 1.1.6 Enterprise Risk Management als 'Business Enabler'

In 1992 verscheen van het 'Committee of Sponsoring Organizations of the Treadway Commission'<sup>4</sup> het rapport 'Internal Control – Integrated Framework'. In het rapport wordt een raamwerk gepresenteerd aan de hand waarvan organisaties hun eigen interne beheersingssysteem kunnen inrichten en beoordelen. Het COSO-rapport is sindsdien uitgegroeid tot het wereldwijde standaardwerk op het gebied van interne beheersing. In de Sarbanes-Oxley Act en ook in de code Tabaksblat wordt COSO als enige genoemd als mogelijk te hanteren raamwerk bij het uitwerken van de bepalingen in de code ten aanzien van interne beheersing en risicomanagement.

In september 2004 is van hetzelfde COSO het 'Enterprise Risk Management – Integrated Framework' (ERMF) verschenen.

<sup>2</sup> Ook wel de 'Cromme code' genoemd, naar de voorzitter van de commissie, Gerhard Cromme.

<sup>3</sup> Ook wel 'the Higgs report' genoemd, naar de voorzitter van de commissie, Derek Higgs

Het ERMF bouwt voort op het Internal Control Framework uit 1992 en is een reactie van COSO op de waargenomen trend binnen organisaties van het in toenemende mate uitvoeren van risicoanalyses als basis voor de inrichting van de organisatie en het systeem van interne beheersmaatregelen.

Een belangrijk onderscheid tussen het internal control framework en het ERMF is dat in het ERMF nog meer duidelijk wordt dat risicomanagement niet iets is dat je alleen doet om risico's te beperken, maar dat risicomanagement een 'tool of management' is waarmee ook 'business-wise' daadwerkelijk resultaten kunnen worden geboekt. In die zin is het verschijnen van het ERMF een welkome ontwikkeling. Als gevolg van met name Sarbanes-Oxley benaderen veel organisaties risicomanagement momenteel met een sterk compliance-gedreven insteek. De inspanningen die moeten worden gedaan – in tijd en geld – zijn enorm en vele betrokkenen twijfelen aan de meerwaarde. Enterprise Risk Management biedt een ideale mogelijkheid om die meerwaarde te verhogen. Door voort te bouwen op hetgeen in de afgelopen jaren reeds gerealiseerd is en de reikwijdte daarvan uit te breiden naar andere, meer toekomstgerichte aspecten van de organisatie (strategische en operationele doelstellingen) zal het management van de organisatie risicomanagement leren waarderen als zinvol instrument in het besturen en beheersen van de organisatie op weg naar het creëren van waarde voor de aandeelhouders en andere belanghebbenden.

### 1.1.7 Acht COSO-componenten van Enterprise Risk Management

Het COSO Enterprise Risk Management Framework bestaat uit acht hoofdcomponenten die gericht zijn op het bereiken van doelstellingen in vier categorieën op alle niveaus in een organisatie. Dit wordt geïllustreerd in de COSO ERM kubus (figuur 1.2).

Figuur 1.2 De COSO ERM kubus



- **Internal Environment** – met 'internal environment' wordt de houding en het gedrag van de interne organisatie bedoeld. Het bepaald de wijze waarop risico wordt gepercipieerd en hoe er mee wordt omgegaan door de mensen in de organisatie. Onder meer de risicomanagement filosofie, de risicobereidheid en de integriteit en ethische waarden van de organisatie maken deel uit van de 'internal environment'.
- **Objective Setting** – Doelstellingen moeten aanwezig zijn voordat potentiële gebeurtenissen kunnen worden geïdentificeerd die het behalen ervan kunnen beïnvloeden. Als onderdeel van enterprise risk management is een 'objective setting' proces aanwezig en wordt ervoor zorg gedragen dat de geformuleerde doelstellingen zijn afgestemd op de missie van de organisatie en passen binnen de risicobereidheid van de organisatie.
- **Event Identification** – interne en externe gebeurtenissen die van invloed zijn op het behalen van de doelstellingen dienen te worden geïdentificeerd. Daarbij dient onderscheid te worden gemaakt tussen risico's en kansen.
- **Risk Assessment** – risico's worden geanalyseerd in termen van kans en impact. Op basis daarvan kan een passende reactie worden geformuleerd. Risico's kunnen worden beoordeeld voor en na de effecten van de risicoreactie.
- **Risk Response** – per risico wordt de meest geschikte reactie geselecteerd – vermijden, accepteren, beheersen of overdragen – en uitgewerkt in concrete acties om de omvang van de risico's in lijn te brengen met de risicobereidheid van de organisatie.
- **Control Activities** – beleid en procedures worden opgesteld en geïmplementeerd teneinde de gekozen risicoreactie daadwerkelijk in de organisatie te verankeren.
- **Information and Communication** – relevante informatie wordt geïdentificeerd, opgeslagen en gecommuniceerd op een wijze die betrokkenen in staat stelt om hun werkzaamheden uit te voeren. Effectieve communicatie vindt plaats in de gehele organisatie, van boven naar beneden, van beneden naar boven en horizontaal.
- **Monitoring** – de effectiviteit van enterprise risk management wordt bewaakt en wijzigingen worden aangebracht ter verbetering. Monitoring vindt op continue wijze plaats binnen alle bedrijfsprocessen, maar ook in de vorm van separate evaluaties.

Enterprise Risk Management is niet een volgtijdelijk proces, waarbij een component slechts de volgende component beïnvloedt. Het is een iteratief proces dat tegelijkertijd in meerdere richtingen werkt. Elke component beïnvloedt elke andere component.

In het volgende hoofdstuk wordt nader ingegaan op wat Enterprise Risk Management is en de voordelen die ermee kunnen worden behaald.

<sup>4</sup> COSO is een samenwerkingsverband van The American Institute of Certified Public Accountants, The Institute of Internal Auditors, Financial Executives International, The Institute of Management Accountants en The American Accounting Association.

# 1.2 Enterprise Risk Management

## 1.2.1 Balanceren tussen risico en opbrengst

Elke organisatie bestaat om waarde te creëren voor haar 'stakeholders'<sup>5</sup>. De enige manier om waarde te creëren is het nemen van risico. Ondernemen is in enge vorm niets anders dan het zo goed mogelijk balanceren tussen risico en opbrengst. Goede organisaties onderscheiden zich van slechte organisaties doordat zij beter in staat zijn om de 'risk/reward trade-off' (figuur 1.3) naar hun voordeel te keren. Zij slagen er in om met gelijke inzet van middelen een beter resultaat neer te zetten. Veelal ligt het verschil erin dat succesvolle ondernemingen zich beter bewust zijn van de risico's die zij nemen, en daardoor in staat zijn om eerder dan de concurrentie op adequate wijze met deze risico's om te gaan. Zij slagen erin om het risico, de onzekere factor, om te buigen naar een kans om waarde te creëren. Tegelijkertijd neemt hetzelfde risico voor de concurrentie de vorm van een bedreiging aan.

Figuur 1.3 Risk/reward trade-off in voordeel van de organisatie keren



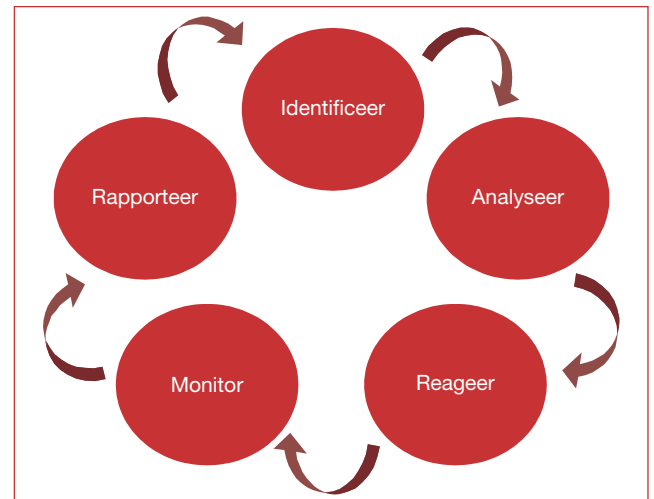
De capaciteit van een organisatie om risico's vroegtijdig te signaleren en om te buigen in kansen is sterk afhankelijk van de individuele kwaliteiten van de ondernemer, bestuurder of manager. Dit geldt zeker voor kleinere organisaties.

In grotere organisaties is dit echter niet genoeg. De omvang van de organisatie, de complexiteit, regionale spreiding en diversiteit in producten en markten vragen om een systematisch, organisatiebreed proces van identificeren en managen van risico's. Tevens bestaat de noodzaak om richting de 'stakeholders' verantwoording af te leggen over de omvang van de risico's die de organisatie neemt en de wijze waarop deze gemanaged worden.

Enterprise Risk Management biedt een organisatie de mogelijkheid om proactief te reageren op veranderende omstandigheden. Door het vroegtijdig signaleren van mogelijke gebeurtenissen en daaruit voortvloeiende risico's is de organisatie in staat om tijdig actie te nemen en het systeem van interne beheersmaatregelen op adequate wijze

aan te passen. De kern van Enterprise Risk Management bestaat uit een organisatiebreed, uniform en gestructureerd proces van identificeren en analyseren van, reageren op en monitoren en rapporteren van mogelijke toekomstige gebeurtenissen die van invloed kunnen zijn op het behalen van de organisatiedoelstellingen (zie figuur 1.4).

Figuur 1.4 Enterprise risk management proces



## 1.2.2 Interne beheersing beheersbaar gemaakt

Het managen van risico's is voor geen enkele organisatie nieuw. Overal in de organisatie zijn maatregelen, procedures, richtlijnen e.d. aanwezig die tot doel hebben het beheersen van één of meerdere specifieke risico's. Enkele bekende voorbeelden van beheerssystemen zijn de planning & controlsystematiek, administratieve organisatie en interne controle, kwaliteitsmanagement (bijv. ISO 9000) en personeelsbeleid en -procedures. Gesteld kan worden dat elke organisatie reeds aan risicomanagement doet. Tegelijkertijd kan de vraag worden gesteld of wel de juiste risico's worden gemanaged. Het kan zijn dat de organisatie belangrijke risico's over het hoofd ziet of risico's verkeerd inschat, waardoor zij niet de juiste prioriteit aanbrengt in haar stelsel van beheersmaatregelen. Met andere woorden: het interne beheersingssysteem van de organisatie is mogelijk niet goed afgestemd op het risicoprofiel van de organisatie.

Het nieuwe van Enterprise Risk Management ten opzichte van traditioneel risicomanagement is dat overal in de organisatie een expliciete risicoanalyse de basis vormt voor de managementagenda en voor het inrichten van het interne beheersingssysteem. Door bovendien veranderingen in het risicoprofiel van de organisatie te monitoren kan het interne beheersingssysteem in continuïteit worden aangepast aan veranderende omstandigheden. De organisatie is blijvend 'in-control'.

<sup>5</sup> Alle belanghebbenden in een organisatie, bijvoorbeeld aandeelhouders, werknemers, cliënten, toezichthouders of de maatschappij als geheel.

Door het risicoprofiel als basis te nemen voor het vormgeven en verbeteren van het interne beheersysteem ontstaat tevens een overkoepelend kader dat alle in de organisatie aanwezige activiteiten op het gebied van risicobeheersing tot een coherent geheel maakt. Het interne beheersingssysteem is beheersbaar gemaakt. Geheel in lijn met de code Tabaksblat kan nu op zinvolle wijze verantwoording worden afgelegd aan de buitenwereld over het risicomanagement van de organisatie.

Figuur 1.5 laat zien dat verschillende traditionele vormen van risicomanagement binnen het concept van Enterprise Risk Management als één samenhangend geheel van activiteiten wordt beschouwd en aangestuurd. De traditionele aanpak van risicomanagement verschilt op vier essentiële punten van Enterprise Risk Management:

- Enterprise Risk Management brengt de aard en omvang van risico's **expliciet** in beeld, waar traditionele vormen van risicomanagement vaak vorm hebben gekregen op basis van een impliciete risico-inschatting.
- Waar traditionele vormen van risicomanagement veelal op organische wijze tot stand zijn gekomen zonder bewust een optimale aanpak te ontwikkelen, biedt Enterprise Risk Management een weloverwogen en **gestructureerd** proces voor het identificeren, analyseren, managen, monitoren en rapporteren van risico's.
- Enterprise Risk Management kiest een **integrale** benadering van alle typen risico's. Dit terwijl risico's voorheen afzonderlijk in beschouwing werden genomen in de verschillende silo's van traditioneel risicomanagement.
- Waar de aanpak van risico's en risicomanagement voorheen veelal verschilde per organisatieonderdeel kiest Enterprise Risk Management voor een **uniforme** benadering voor de gehele organisatie. Dit maakt de communicatie over risico's eenduidiger en vereenvoudigt vergelijking en consolidatie van risicoprofielen van verschillende organisatieonderdelen.

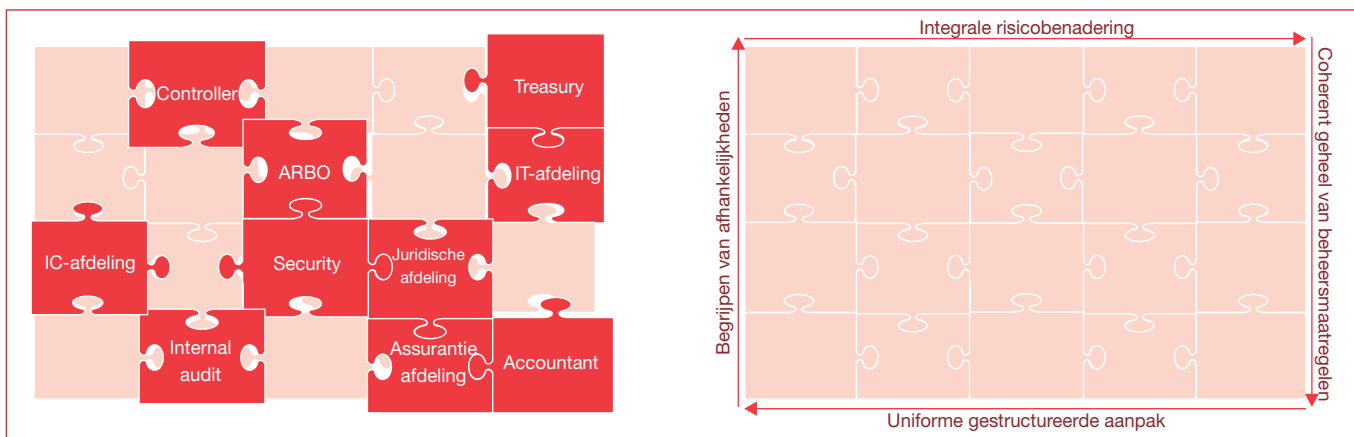
Zoals uit figuur 1.5 blijkt betekent de opkomst van Enterprise Risk Management niet dat traditionele vormen van risicomanagement het veld zullen ruimen. Treasury risico's blijven gemanaged worden vanuit de treasury afdeling en juridische risico's blijven gemanaged worden door de juridische afdeling. Wel zullen wellicht bestaande afspraken en werkwijzen worden aangepast om de aansluiting te kunnen maken op de uniforme, bedrijfsbrede aanpak van Enterprise Risk Management. Dit zal er echter enkel toe leiden dat de diverse afdelingen beter in staat worden gesteld hun risico's te managen in het licht van de doelstellingen en het risicobeleid van de algehele organisatie.

### 1.2.3 De toegevoegde waarde van Enterprise Risk Management

Afhankelijk van de redenen die een organisatie heeft om volgens de principes van Enterprise Risk Management te werken zullen de voordelen die de organisatie daarvan ervaart verschillen. Hierdoor zullen accentverschillen ontstaan in de aard en de omvang van de gerealiseerde voordelen. In het algemeen kan echter worden gesteld dat organisaties die Enterprise Risk Management goed hebben geborgd in de gehele organisatie beter dan andere organisaties in staat zijn om:

- **Opbrengsten te verhogen** – indien risico's goed beheerst worden kan de organisatie meer risico's nemen, hetgeen doorgaans ook hogere opbrengsten met zich meebrengt. Concreet voorbeeld is de mogelijkheid voor het aanhouden van een lager solvabiliteitsbeslag onder de Basel II regelgeving voor banken.
- **Kansen te benutten** – toekomstige ontwikkelingen worden eerder gesignaleerd, er wordt eerder op gereageerd en zo worden concurrentievoordelen behaald.
- **De inzet van middelen te rationaliseren** – er ontstaat beter inzicht in wat de belangrijkste risico's zijn en waar dus de beschikbare middelen (bijv. geld, tijd) het beste aan kunnen worden besteed. Managementkeuzes worden op deze wijze bewuster en explicieter gemaakt.

Figuur 1.5 Van een onsamenhangende naar een geïntegreerde benadering



- **Operationele verliezen en verrassingen te voorkomen** – knelpunten en zwakke plekken in de operationele processen worden eerder gedetecteerd.
- **Aan eisen van wet- en regelgeving te voldoen** – de organisatie voldoet aan de eisen inzake risicomanagement als onderdeel van corporate governance wet- en regelgeving.

Uiteindelijk zullen de genoemde voordelen er toe leiden dat de organisatie beter in staat is om haar doelstellingen te behalen en zodoende waarde te creëren voor haar 'stakeholders'.

## 1.2.4 Valkuilen bij de toepassing van Enterprise Risk Management

De mate waarin een organisatie erin slaagt om voordelen te behalen met Enterprise Risk Management – zoals in voorgaande paragraaf uiteengezet – is uiteraard afhankelijk van de kwaliteit van de uitvoering. In onze adviespraktijk zien wij meer dan eens organisaties die worstelen met de effectieve toepassing van Enterprise Risk Management. De in opzet goed doordachte systematiek blijkt in de praktijk toch niet zo goed te werken, met als gevolg dat de beoogde effecten niet worden gerealiseerd. De oorzaken van die worsteling zijn vaak terug te voeren op enkele veel voorkomende misvattingen of valkuilen. In deze paragraaf worden enkele van deze valkuilen behandeld.

### Valkuil 1: Enterprise Risk Management is vooral iets voor de controller

Doordat risico's altijd een financiële consequentie hebben en veelal als zodanig worden uitgedrukt, wordt al gauw gesproken over financiële risico's. Op grond daarvan wordt vervolgens de verantwoordelijkheid al gauw neergelegd bij de financiële functie. Echter risico's dienen niet te worden geclassificeerd naar gevolg, maar naar ontstaansgrond. Dat is zuiverder, nauwkeuriger en gemakkelijker als het gaat om mogelijke maatregelen te bepalen en verantwoordelijkheden toe te wijzen. Doorgaans zal dan ook blijken dat de verantwoordelijkheid voor een risico veel eerder bij het lijnmanagement ligt dan bij de financiële functie.

Eigenaarschap is cruciaal in risico's onderkennen en managen. Daarom speelt de ontstaansgrond van een risico (risk driver) een zeer belangrijke rol bij het managen van risico's. Die ontstaansgrond ligt heel dikwijls bij die processen, systemen en organisatiedelen waarvoor de lijnmanager verantwoordelijk is. Indien de ontstaansgrond buiten de organisatie ligt dan is de lijnmanager minimaal verantwoordelijk voor het waarnemen ervan. Enterprise Risk Management is dan ook niet iets typisch van de controller of auditor, maar van de lijnmanager. Het gaat immers over management. Draagvlak voor het concept dient dan ook breed en zeker ook hoog in de organisatie gedragen te worden met nadrukkelijke betrokkenheid van lijn- en topmanagement.

Mogelijkheden om betrokkenheid van het lijnmanagement te vergroten zijn:

- Benoem risico's naar hun ontstaansgrond en niet het gevolg;
- Betrek lijnmanagers actief in risico-inventarisatie en -evaluatie; Maak hen hier zo mogelijk voor verantwoordelijk; zij staan het dichtst op het primaire proces en zijn omgeving en hebben daardoor de beste kennis voorhanden.
- Maak individuele lijnmanagers expliciet verantwoordelijk voor het managen van één of meerdere risico's; bijvoorbeeld door hen te benoemen in risicorapportages die worden besproken met het hogere management.

### Valkuil 2: De kenmerken van een risico zijn voor alle direct betrokkenen gelijk

Het is sterk afhankelijk van de positie in het bedrijf, zowel horizontaal (functioneel) als verticaal (hiërarchisch), hoe men tegen een bepaald risico aankijkt. Het strategisch management is vooral gericht op de trade-off tussen risico en opbrengsten en heeft daarbij een sterke externe oriëntatie. Het operationeel management daarentegen heeft juist een interne oriëntatie en denkt vooral in termen van trade-off tussen risico's en beheersmaatregelen.

Daarnaast spelen het referentiekader (bijvoorbeeld kennis van omgeving, organisatie en eerdere ervaringen) en de risicobereidheid een belangrijke rol bij het inschatten van risico's. Indien een organisatie zich niet bewust is van deze factoren en een beperkte functionele dan wel hiërarchische benadering kiest, loopt men het gevaar van een eenzijdige benadering en een risico foutief in te schatten.

Handreikingen om dit probleem zo goed mogelijk te benaderen zijn:

- Gebruik een groot aantal verschillende bronnen, zowel in de breedte als in de diepte van de organisatie, bijvoorbeeld door questionnaires te hanteren en reeds aanwezige rapportages;
- Breng zoveel mogelijk verschillende disciplines bij elkaar als risico's worden geanalyseerd en geëvalueerd, b.v. een MT overleg of management bijeenkomst;
- Zorg voor groepsdiscussies (workshops) over de beschrijving van risico's en de omvang van risico's;
- Stel de risicobereidheid ('risk appetite') van een organisatie vast door duidelijke algemene richtlijnen en normen wat wel en niet acceptabel wordt geacht en eenduidige risicobeoordelingscriteria voor waarschijnlijkheid en impact, beide vastgesteld door de directie.

### Valkuil 3: Risico's managen is een eenmalig of jaarlijks uit te voeren exercitie om tot een lijstje van risico's te komen

Veel organisaties worden óf door incidenten óf door externe of interne (bijvoorbeeld via de moederorganisatie) regelgeving geconfronteerd met Enterprise Risk Management als ogenschijnlijk nieuw bedrijfsvoeringconcept. Vanuit die beleving wordt vervolgens gehandeld en gedacht. Dit uit

zich in één of meer van de volgende verschijningsvormen:

- Enterprise Risk Management en de bijbehorende modellen worden gezien als weer een managementconcept naast de vele andere managementconcepten, zoals bijvoorbeeld INK en de Business Balanced Scorecard.
- Enterprise Risk Management wordt vooral gezien als een trucje: van achter het bureau volgens een vast stappenplan, éénmaal per jaar op een vast moment. Het levert een overzicht met risico's dat vooral andere belanghebbenden, niet zijnde het management, tevredenstelt.
- Enterprise Risk Management moet vooral door andere partijen, niet zijnde het reguliere lijnmanagement, worden uitgevoerd, bijvoorbeeld door stafmedewerkers van audit, control, assurantie of door externen.

Het voorgaande heeft ernstige consequenties voor de kwaliteit van Enterprise Risk Management. Enterprise Risk Management moet men juist zien als het bindende element tussen al die managementconcepten, gericht op integrale sturing en beheersing en de organisatiedoelstellingen. Periodiciteit en verantwoordelijkheid spelen hierin een sleutelrol. Enterprise Risk Management moet bij voorkeur in continuïteit plaatsvinden. Het management heeft immers zelf het meeste belang bij inzicht in en het adequaat managen van risico's. Voldoen aan de wensen van toezichhouders dient slechts een nevendoelelstelling te zijn.

Fundamenteel in het voorgaande is het ontbreken van voldoende risicobewustzijn bij het lijnmanagement. Dit is de kritieke succesfactor en vormt de voedingsbodem om daadwerkelijk aan Enterprise Risk Management invulling te geven. Wanneer deze houding en het bijbehorende gedrag ontbreken, wordt elke handeling met betrekking tot Enterprise Risk Management als aanvullend en belastend gezien, terwijl het juist een onderdeel van de dagelijkse managementactiviteiten dient te zijn.

De volgende activiteiten kunnen helpen bij het versterken van het risicobewustzijn:

- Zorg voor natuurlijke betrokkenheid en voorbeeldgedrag van het topmanagement;
- Maak lijnmanagement expliciet eigenaar van risico's en spreek het hierop aan;
- Betrek lijnmanagement bij het vormgeven van Enterprise Risk Management in de organisatie;
- Praat en discussieer over risico's en het managen ervan in groepsverband, bijvoorbeeld managementbijeenkomsten, werkoverleg, interne conferenties;
- Verzorg opleiding en training;
- Maak Enterprise Risk Management onderdeel van reguliere managementactiviteiten, bijvoorbeeld door een risicoparagraaf op te nemen in jaarplannen en managementrapportages, standaard onderwerp te laten zijn op de agenda van vergaderingen en managementbijeenkomsten, doelstellingen op het

gebied van Enterprise Risk Management op te nemen in persoonlijke jaarplannen, medewerkers te beoordelen op hun bijdrage aan Enterprise Risk Management en onderdeel van de bedrijfsinstructie te laten zijn.

#### Valkuil 4: Een risico houdt in: een doelstelling niet halen of een niet functionerende beheersmaatregel

Bij een pensioenverzekeraar wordt tijdens een vrije brainstorm in een risk self-assessment workshop een groot aantal risico's ingebracht, waaronder:

- Het niet halen van een 6% rendement op de beleggingsportefeuille in 2003;
- De training van portefeuillemanagers voor gebruik van het nieuwe MIS is ineffectief.

Valide risico's op het eerste gezicht. Toch is dat maar zeer ten dele waar. Men redeneert in cirkels. Een doelstelling niet halen is dan misschien wel een risico, het ultieme risico van een organisatie, maar het zegt erg weinig en is onvoldoende specifiek. Het is veel belangrijker en relevanter voor het managen ervan het risico uit te drukken in de oorzaak – gebeurtenis, omstandigheid, activiteit – die doelrealisatie bedreigt. Hetzelfde geldt voor het tweede genoemde risico. Het betreft hier een risico dat een beheersmaatregel niet functioneert. Het is belangrijk dit probleem als oorzaak van een gebeurtenis te onderkennen om adequate (vervolg)stappen in de vorm van bijvoorbeeld nieuwe beheersmaatregelen te kunnen nemen. Het probleem weer als een risico te benoemen, is minder relevant omdat dit eveneens leidt tot cirkelredenering. Immers de nieuwe beheersmaatregelen kunnen eveneens het risico lopen van inadequaet functioneren en zo kan men door blijven gaan.

Wederom een aantal adviezen om niet in deze valkuil te belanden zijn:

- Hanteer duidelijke en relatief gedetailleerde beschrijvingen van risico's;
- Stel vast of het risico werkelijk voldoende specifiek is en iets zegt over de organisatie dan wel haar omgeving;
- Probeer daarbij zoveel mogelijk zowel oorzaak als gevolg te benoemen van een risico;
- Probeer indien relevant een relatie te leggen met andere reeds benoemde risico's en stel vast of dit risico werkelijk wat toevoegt en geen verkapt disfunctionerende beheersmaatregel is;
- Laat een relatieve buitenstaander met kennis van risicomangement de lijst van risico's beoordelen of gebruik een risicomangement specialist om het proces van risico-inventarisatie te ondersteunen en door te vragen.

In deze paragraaf zijn enkele veel voorkomende valkuilen bij het vormgeven van Enterprise Risk Management beschreven. Herkenbare voorbeelden met praktische tips om dit te voorkomen of zoveel mogelijk tegen te gaan. Wellicht zelfs direct toepasbaar in uw eigen organisatie teneinde de voordelen van Enterprise Risk Management ten optimale te benutten.



# Deel II

## Het onderzoek en de resultaten

PricewaterhouseCoopers heeft samen met de Rijksuniversiteit Groningen onderzoek gedaan naar de toepassing van risicomanagement in Nederland. Het onderzoek is uitgevoerd door middel van een enquête. In dit deel van het rapport worden de aanpak en de resultaten van het onderzoek gepresenteerd.

# 2.1 Onderzoekopzet

## 2.1.1 Doelstelling van het onderzoek

Over het onderwerp risicomanagement wordt veel geschreven. In diverse artikelen en openbaar beschikbare standaarden wordt beschreven hoe een organisatie aan risicomanagement zou kunnen doen. Waar het echter veelal aan ontbreekt is een inzicht in hoe in de praktijk werkelijk met risicomanagement om wordt gegaan. De theorie reikt de keuzes aan die gemaakt dienen te worden, maar welke keuzes worden daadwerkelijk gemaakt? Hoe ziet het risicomanagement in een organisatie er in de werkelijkheid uit?

In de adviespraktijk van PricewaterhouseCoopers zijn wij bij het risicomanagement van veel van onze cliënten betrokken. Sommige cliënten maken voor het eerst kennis met risicomanagement, anderen zijn al een paar stappen verder. Ongeacht de fase waarin een cliënt zich bevindt wordt ons met enige regelmaat de vraag gesteld hoe andere organisaties met bepaalde keuzes omgaan. Er bestaat duidelijk een behoefte bij veel organisaties om het eigen risicomanagement te vergelijken met dat van andere organisaties. In deze behoefte probeert dit onderzoek te voorzien. Het onderzoek beoogt inzicht te verschaffen in de wijze waarop risicomanagement in organisaties in Nederland is ingericht en wordt toegepast. De resultaten bieden geïnteresseerden de mogelijkheid om het risicomanagement in de eigen organisatie te vergelijken met de gangbare werkwijzen in andere organisaties.

Tevens kan het rapport worden gebruikt om basiskennis op te doen over de toepassing van risicomanagement in organisaties. Niet in de laatste plaats door studenten van (postdoctorale) opleidingen op het gebied van control en auditing. Voor de postdoctorale controllersopleiding van de Rijksuniversiteit Groningen was dit nadrukkelijk een aanleiding om het onderzoek mede uit te voeren.

## 2.1.2 Aanpak van het onderzoek

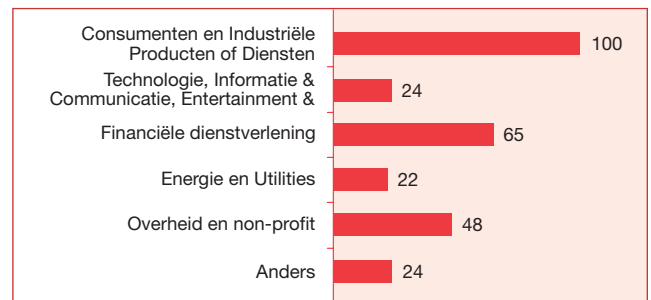
Het onderzoek is uitgevoerd in de vorm van een enquête. De enquête is eind 2004 uitgestuurd naar alle leden van het Controllers Instituut. In de enquête zijn vragen opgenomen over de wijze waarop de organisatie waar de geënquêteerde werkzaam is invulling geeft aan risicomanagement. De leden van het Controllers Instituut hebben enkele weken de tijd gehad om de vragenlijst op een speciaal daarvoor ingerichte internetpagina in te vullen. Dit heeft uiteindelijk geleid tot 283 bruikbare ingevulde vragenlijsten.

De verzamelde respons is verwerkt tot tabellen, waarin ook analyses naar branche, omvang van de organisatie en andere variabelen zijn meegenomen. Deze tabellen worden weergegeven in de volgende hoofdstukken van dit rapport.

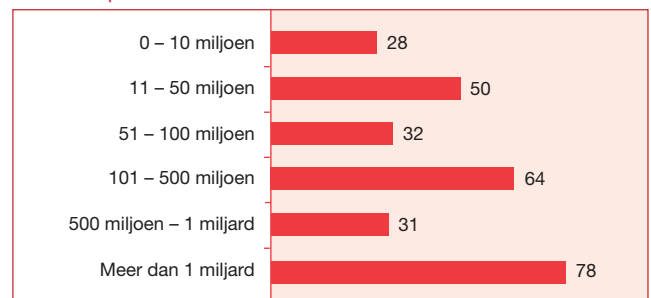
## 2.1.3 Profiel van de respondenten

In totaal zijn 283 bruikbare ingevulde vragenlijsten verzameld en verwerkt. De hieronder opgenomen tabellen geven inzicht in de samenstelling van het respondentenbestand.

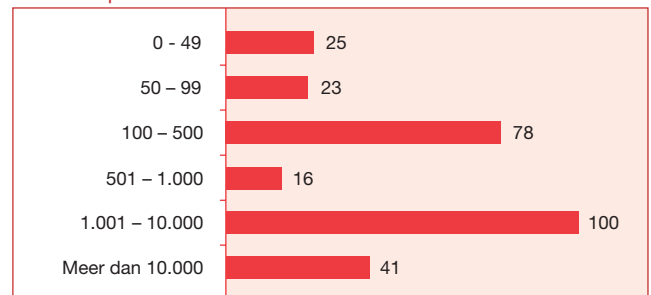
Aantal respondenten naar branche



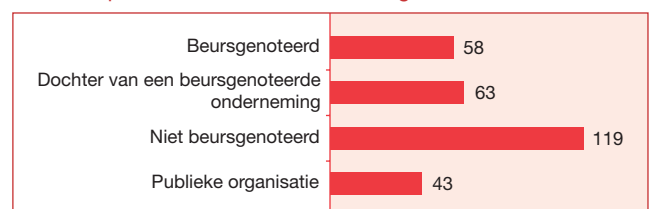
Aantal respondenten naar omzet



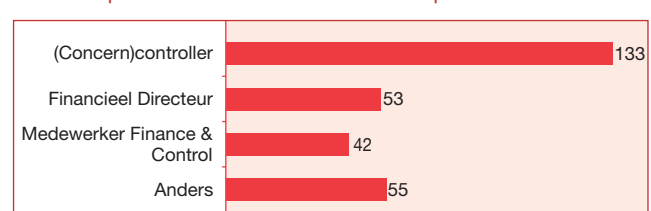
Aantal respondenten naar aantallen medewerkers



Aantal respondenten naar wel/niet beursgenoteerd



Aantal respondenten naar functie van de respondent



## 2.2 Risicomanagement strategie

### 2.2.1 Risicomanagement strategie bepalend voor inrichting risicomanagement systeem

Verskillende organisaties kunnen verschillende zaken nastreven met risicomanagement. Hetgeen een organisatie met risicomanagement na wil streven komt tot uiting in de risicomanagement strategie. Het is van belang om eerst over de strategie na te denken voordat begonnen wordt met de invoering van risicomanagement. Het dient helder te zijn waarom de organisatie aan risicomanagement doet – de risicomanagement visie - en hoe men het risicomanagement vorm wil geven om de gestelde doelen te bereiken – het risicomanagement beleid. De risicomanagement strategie (visie en beleid) is namelijk bepalend voor de inrichting van het risicomanagement systeem.

De risicomanagement strategie van een organisatie is sterk afhankelijk van de aanleidingen die een organisatie heeft om aan risicomanagement te gaan doen. En die aanleidingen kunnen sterk verschillen. Onderstaand kader 2.1 bevat een overzicht van veel voorkomende 'triggers' voor risicomanagement. Overigens is het doorgaans een combinatie van redenen die een organisatie beweegt om bewust aan de slag te gaan met risicomanagement.

#### Kader 2.1

##### 'Triggers' voor risicomanagement

- De onderneming is beursgenoteerd. In dat geval is vaak een corporate governance code van toepassing die eisen stelt aan het risicomanagement van aan de beurs genoteerde ondernemingen (Bijv. code Tabaksblat, Sarbanes-Oxley, Turnbull of KonTraG).
- De toezichthouder stelt eisen aan de interne beheersing (bijv. ROB, Bazel II, Solvency II, VBTB).
- De onderneming is actief in een sterk gereguleerde markt (bijv. Farmaceutische sector).
- Stakeholders hebben onvoldoende comfort en vragen om transparantie.
- Er hebben zich in het recente verleden één of meerdere incidenten voorgedaan.
- De organisatie is snel gegroeid (autonoom of door overnames) waardoor het management moeite heeft grip te houden.
- De onderneming heeft een beursgang gepland.
- De organisatie ondergaat ingrijpende interne veranderingen (bijv. reorganisatie, grote investeringen).
- De organisatie heeft te maken met belangrijke externe veranderingen (bijv. veranderende politieke besluitvorming, sterke concentratiegolf in de branche).

In kader 2.2 staat een voorbeeld weergegeven van een risicomanagement visie. Gegeven de aard van deze risicomanagement visie zal het risicomanagement in deze organisatie waarschijnlijk vooral worden toegepast op strategisch niveau in de organisatie. Ook komt uit deze visie duidelijk naar voren dat het gaat om een afweging tussen risico en opbrengst. De 'upside' van risico dient hier nadrukkelijk en expliciet te worden meegenomen in besluitvormingsprocessen, hetgeen vertaald zal moeten worden naar het proces van identificeren en analyseren van risico's.

#### Kader 2.2 Voorbeeld risicomanagement visie (I)

“Ontwikkelen van een competentie in risicomanagement, met als doel het creëren van een instinctieve en consistente afweging van risico en opbrengst bij het maken van strategische keuzes en het uitvoeren van de strategie opdat de strategische doelstellingen worden bereikt”

Een ander voorbeeld staat weergegeven in kader 2.3. De betreffende organisatie geeft in deze visie aan dat zij risicomanagement vooral toepast als instrument om risico's te beheersen. Hier gaat het dus niet zozeer om het maken van de juiste afweging bij het nemen van strategische beslissingen, de nadruk ligt hier veel meer op het beheersen van mogelijke negatieve gebeurtenissen. Het daadwerkelijke risicomanagement proces zal in deze organisatie dan ook verschillen van de organisatie uit het andere voorbeeld.

#### Kader 2.3 Voorbeeld risicomanagement visie (II)

“Risicomanagement moet de organisatie in staat stellen om op elk niveau weloverwogen keuzes te maken ten aanzien van het samenstellen van een uitgebalanceerd geheel van beheersmaatregelen. Die beheersmaatregelen moeten uiteindelijk leiden tot het 'in control' zijn van de gehele organisatie.”

## 2.2.2 Risicomanagement beleid vaak niet expliciet geformuleerd

De risicomanagement visie kan verder worden uitgewerkt in een risicomanagement beleid. Het risicomanagement beleid beschrijft de wijze waarop de organisatie aan risicomanagement wil doen. Typische elementen die in een risicomanagement beleid worden opgenomen zijn de visie en doelstellingen, rollen & verantwoordelijkheden en een korte beschrijving van de hoofdelementen van het risicomanagement systeem. Ook een uitspraak over de risicobereidheid ('risk appetite') van de organisatie maakt vaak deel uit van het risicomanagement beleid.

In de risicomanagement enquête (zie grafiek 2.2.2.1) is respondenten gevraagd aan te geven of hun organisatie een formeel risicomanagement beleid kent. In slechts 39% van de organisaties blijkt dit het geval te zijn. Het zijn vooral de beursgenoteerde ondernemingen die over een formeel risicomanagement beleid beschikken (56%), in tegenstelling tot niet-beursgenoteerde (29%) en publieke organisaties (18%).

### Kader 2.4

"Heeft het topmanagement van uw organisatie een risicomanagementbeleid geformuleerd en gecommuniceerd?"

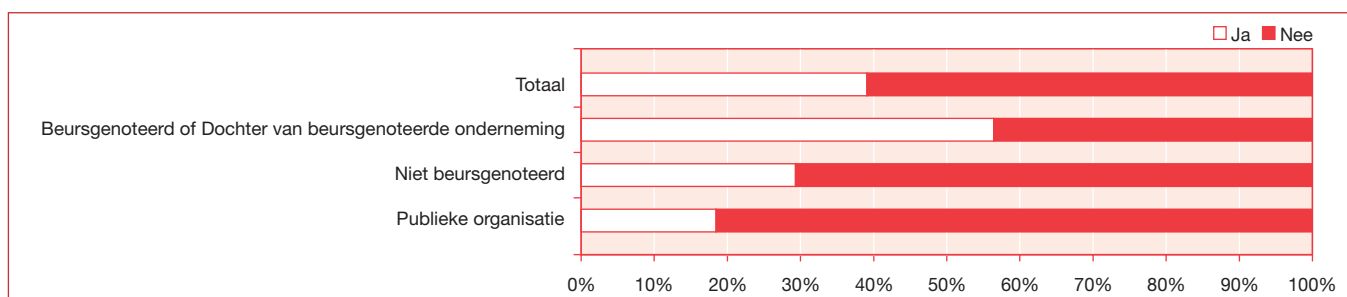
Bij een uitsplitsing naar branche (zie grafiek 2.2.2.2) valt op dat de financiële sector er met 61% uitspringt, gevolgd door de energie en utilities bedrijven met 53%. De overheid en non-profit blijft duidelijk achter met 11%. Voor alle branches geldt dat dit in meer of mindere mate tegenvallende percentages zijn die aangeven dat de formele inbedding van risicomanagement op het hoogste niveau in een organisatie vaak nog onvoldoende is geregeld.

Figuur 1.6 Voorbeeld inhoudsopgave risicomanagement handboek

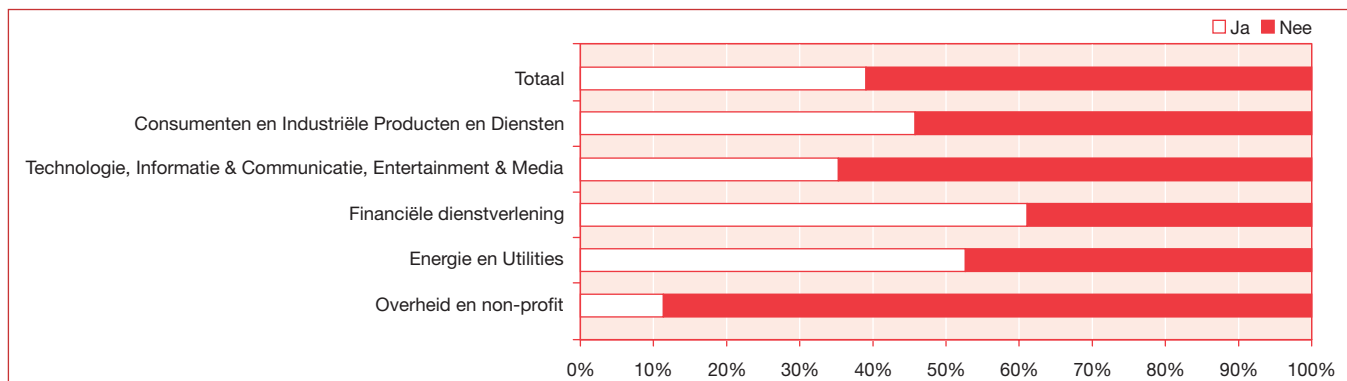
Risk Management Manual	
<b>Contents</b>	
1. Approach to risk management	7. Corporate planning
1.1 Introduction	7.1 Alignment of risk management with planning, execution and measurement
1.2 What is risk	7.2 Corporate planning
1.3 What is risk management	7.3 Change management process
2. Risk management policy	7.4 Projects
2.1 Risk management policy	
2.2 Principles	
2.3 Likelihood and impact	
3. Risk Management structure	8. Project risk management
3.1 Structure	
3.2 Roles and responsibilities	
3.3 Risk Management Committees	9. Compliance
4. Risk assessment process	10. Insurance
4.1 Description of risk assessment process	
4.2 Self assessment process	
4.3 Risk prioritisation	
4.4 Cost/benefit assessment	
4.5 Dependency modelling	
5. Risk reporting and discretions	<b>Appendices:</b>
5.1 Documentation requirements	1 Glossary of risk management terms
5.2 Risk and Board reporting	2 Operating risk guide
5.3 Financial delegated authority	3 Project risk guide
5.4 Meeting agendas	4 Qualitative risk measures
	5 Operating plan risk assessment template
	6 Project risk assessment template
	7 Register of projects
	8 Risk treatment template
	9 Business initiative sign off
	10 Reporting formats - Audit Committee, Management reports, Board submissions
	11 Compliance certificate
6. Risk categories	

Een beleidsdocument heeft een kaderstellende en richtinggevende functie voor de organisatie. Het geeft voor de mensen in de organisatie aan binnen welke grenzen uitvoering moet worden gegeven aan risicomanagement en biedt daarvoor aanknopingspunten. Sommige organisaties werken het risicomanagement beleid verder uit in risicomanagement procedures of een risicomanagement handboek. In het risicomanagement handboek wordt het risicomanagement systeem van de organisatie in detail beschreven. Doel van een dergelijk risicomanagement handboek is het bevorderen van consistentie in de wijze waarop binnen diverse onderdelen van de organisatie uitvoering wordt gegeven aan het risicomanagement beleid. Figuur 1.6 geeft een voorbeeld van een inhoudsopgave van een risicomanagement handboek.

Grafiek 2.2.2.1 Heeft het topmanagement van uw organisatie een risicomanagementbeleid geformuleerd en gecommuniceerd?



Grafiek 2.2.2.2 Heeft het topmanagement van uw organisatie een risicomanagementbeleid geformuleerd en gecommuniceerd?



### 2.2.3 Generieke risicomanagement standaarden door veel organisaties gebruikt

Er zijn wereldwijd door verschillende instanties standaarden ontwikkeld ten aanzien van de wijze waarop risicomanagement vorm zou kunnen worden gegeven. De meest recente en meteen ook de meest bekende is het COSO Enterprise Risk Management – Integrated Framework dat in 2004 is verschenen en voortborduurde op het COSO Internal Control – Integrated Framework uit 1992. De verwachting is dat het Enterprise Risk Management Framework evenals het Internal Control Framework zal uitgroeien tot wereldwijd geaccepteerde standaard.

Andere bekende risicomanagement standaarden vinden vaak hun oorsprong binnen een bepaalde branche of binnen een bepaald land. Een aardig voorbeeld van het laatste is de Australian/New Zealand Risk Management Standard 4360 waarvan reeds in 1995 de eerste versie werd uitgegeven door de ‘Council of Standards’ van beide landen. Omdat het de eerste generieke standaard voor risicomanagement was en bovendien een kwalitatief goed document heeft de Australische / Nieuw Zeelandse standaard ook bij ondernemingen elders in de wereld zijn ingang gevonden. In 1999 en in 2004 is een geactualiseerde versie van de standaard verschenen.

In het Verenigd Koninkrijk hebben in 2002 drie grote beroepsverenigingen<sup>6</sup> tezamen een risicomanagement standaard gepubliceerd. Dit initiatief is vooral gedreven door en gericht op de verbreding van de verzekeringsfunctie in een organisatie naar een bredere risicomanagement benadering. Voorbeelden van branchespecifieke risicomanagement standaarden zijn Bazel II voor het bankwezen en Solvency II voor de verzekeringsbranche.

Ook de Internationale Organisatie voor Standaardisatie (ISO) heeft inmiddels van zich laten horen op het terrein van risicomanagement. In 2002 verscheen van ISO een richtlijn voor het gebruik van risicomanagement termen in standaarden (ISO/IEC Guide 73). In de richtlijn worden 29 risicomanagement termen van een definitie voorzien, met als doel meer consistentie in het gebruik van risicomanagement terminologie.

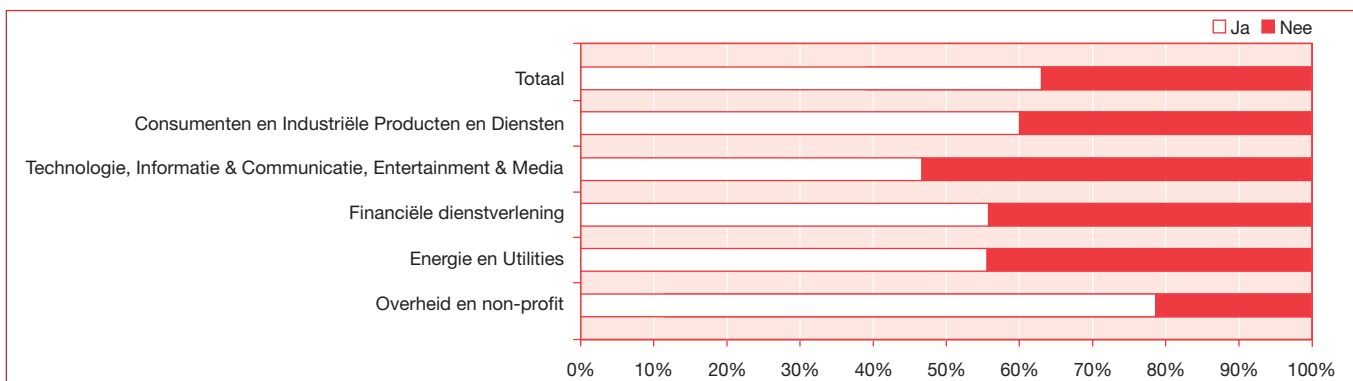
Uit ons onderzoek blijkt (zie grafiek 2.2.3.1) dat het merendeel van de organisaties in Nederland (63%) bij het vormgeven van het risicomanagement in de organisatie een openbare risicomanagement standaard als uitgangspunt heeft genomen. Opvallend daarbij is dat de Overheid en non-profit sector hier een uitschieter naar boven is met 79%.

#### Kader 2.5

“Is het risicomanagement in uw organisatie ingericht volgens een bepaalde risicomanagement standaard?”

Door bijna driekwart van de respondenten die aangeven gebruik te maken van een standaard wordt COSO genoemd als gehanteerde standaard. Veelal is onduidelijk of zij daarmee verwijzen naar het COSO ERM Framework of het COSO Internal Control Framework. Andere genoemde standaarden zijn ABIB, Bazel II, Solvency II en de Australian / New Zealand Standard. Ook worden enkele minder expliciet aan risicomanagement gekoppelde concepten en theorieën als het INK-model, CobiT, Six Sigma en de typologie van Starreveld genoemd als basis waarop het risicomanagement in de organisatie (mede) gestoeld is. Veel respondenten geven aan dat bij het vormgeven van het risicomanagement systeem van de organisatie uit meerdere bronnen geput is en daar vervolgens een organisatiespecifieke draai aan is gegeven.

Grafiek 2.2.3.1 Is het risicomanagement in uw organisatie ingericht volgens een bepaalde risicomanagement standaard?



<sup>6</sup> The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) en The National Forum for Risk Management in the Public Sector (ALARM)

## 2.3 Identificeren en analyseren van risico's

### 2.3.1 Vijf generieke stappen te herkennen in elk risicomanagement proces

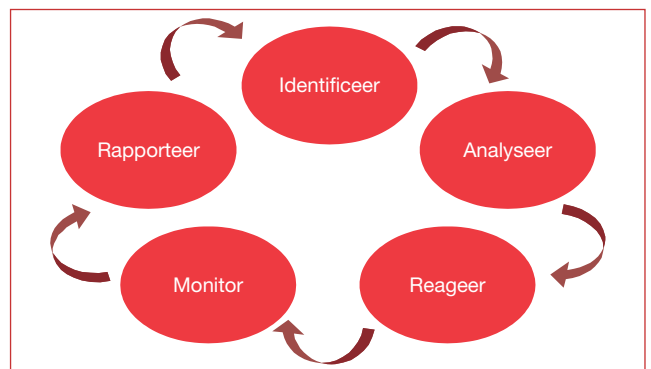
Op verschillende plekken in een organisatie worden op verschillende wijzen vormen van risicomanagement bedreven. Ook tussen organisaties bestaan verschillen ten aanzien van de inrichting van het risicomanagement proces. Kortom, geen risicomanagement proces is hetzelfde. Er zijn echter een vijf basisstappen te benoemen die onderdeel uitmaken van elk risicomanagement proces:

- **Identificatie;** Het op gestructureerde wijze identificeren van mogelijke toekomstige gebeurtenissen, het adequaat formuleren van deze gebeurtenissen in de vorm van risico's en het vaststellen van de oorzaken van deze risico's.
- **Analyse;** Het beoordelen van de waarschijnlijkheid en de impact van risico's vóór en na beheersing. Voor het beoordelen van de risico's na beheersing dient de effectiviteit van de beheersmaatregelen te worden beoordeeld. Deze beoordeling van de beheersmaatregelen vormt aldus een onlosmakelijk onderdeel van de risicoanalyse.
- **Reactie;** Selecteren en implementeren van gewenste reactie op geïdentificeerde risico's. Er zijn een viertal generieke reacties mogelijk: vermijden, overdragen, beheersen of accepteren.
- **Monitoring;** Het in continuïteit bewaken van de risico's en de achterliggende oorzaken en het observeren van mogelijke veranderingen daarin, met inbegrip van de werking van de beheersmaatregelen.
- **Rapportage;** Het rapporteren over de oorzaak, aard en omvang van risico's, de effectiviteit van de beheersmaatregelen en veranderingen daarin. De rapportage gebeurt zowel binnen vaste vooraf bepaalde structuren (richting, tijd, format) als op ad-hoc basis op de wijze en in de vorm zoals op dat moment nodig geacht.

Hoewel niet altijd expliciet benoemd maken de genoemde vijf activiteiten onderdeel uit van elk risicomanagement proces. De stappen zullen in continuïteit en op iteratieve wijze worden doorlopen.

In dit hoofdstuk zullen de eerste twee stappen – identificeer en analyseer – aan bod komen. De volgende stappen komen in hoofdstuk 2.4 en 2.5 aan bod.

Figuur 1.7 Generiek risicomanagement proces



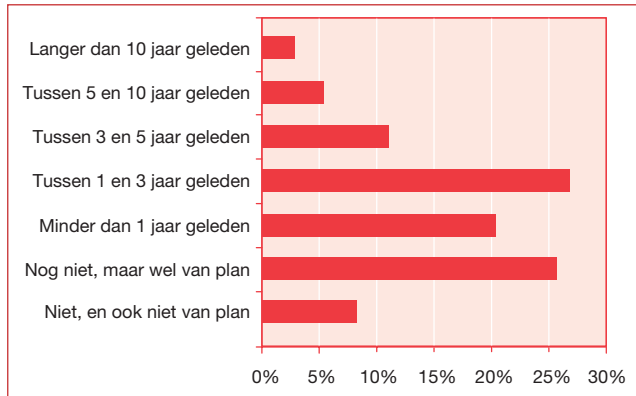
### 2.3.2 Integrale risicoanalyse voor de meeste organisaties nieuw fenomeen

Een belangrijk element van modern risicomanagement is een integrale benadering van risico's. Dat wil zeggen dat alle typen risico's van een organisatie (of business unit, proces etc.) tegelijkertijd in ogenschouw worden genomen. Dit in tegenstelling tot meer traditionele vormen van risicomanagement die veelal zijn gericht op specifieke risicogebieden (bijv. verzekeringsrisico's, treasury, ARBO). Er zijn vele bronnen van risico, zowel binnen de organisatie als extern, die elkaar bovendien beïnvloeden. Het is daarom verstandig om op integrale wijze de interne en externe omgeving te blijven monitoren op mogelijke gebeurtenissen die van invloed kunnen zijn op het behalen van de doelstellingen van de organisatie. Figuur 1.8 toont een overzicht van enkele typische bronnen van risico.

Figuur 1.8 Veel voorkomende bronnen van risico

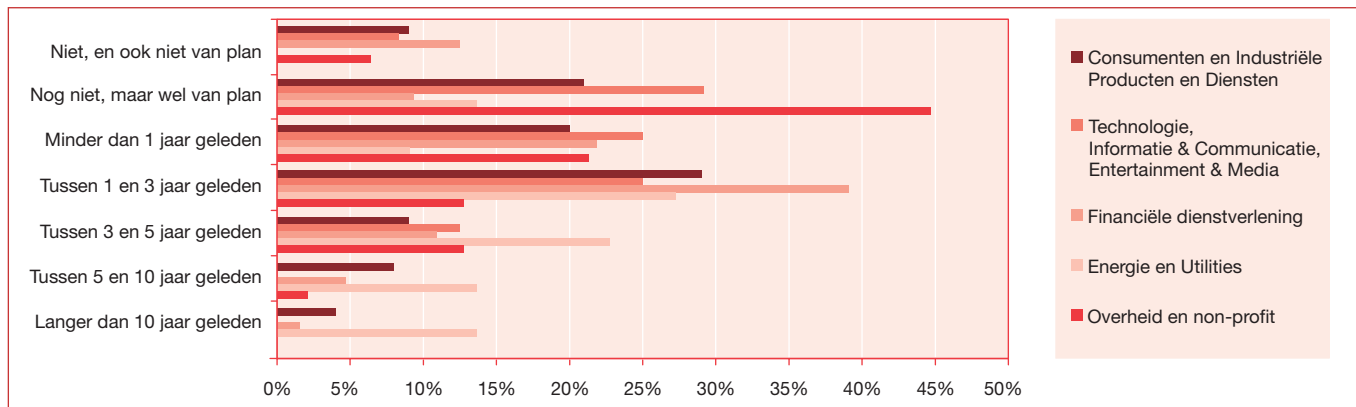


Grafiek 2.3.2.1 Wanneer is uw organisatie begonnen met het uitvoeren van integrale risico-inventarisaties en –analyses?

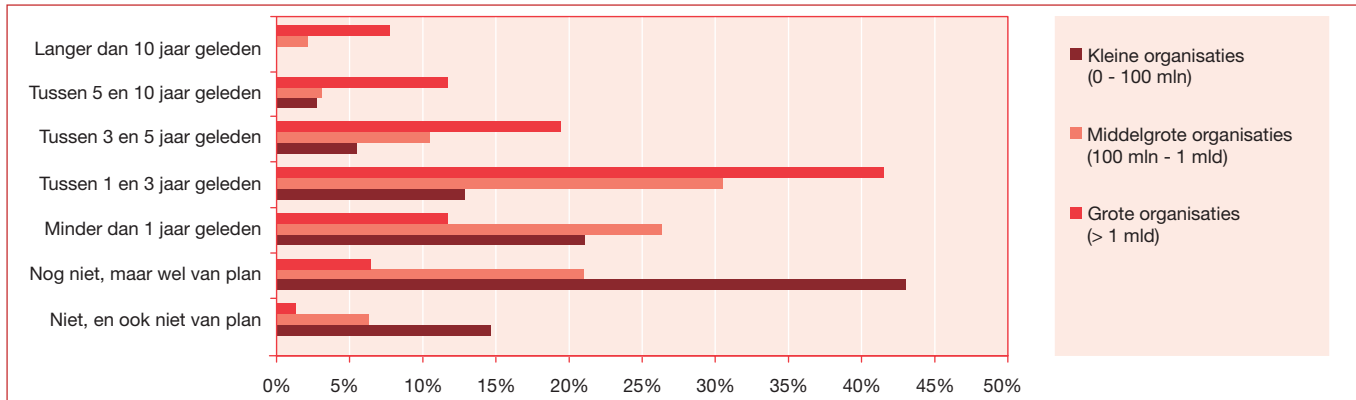


Een uitsplitsing naar grootte van de organisatie (naar omzet gemeten) laat het te verwachten beeld zien (zie grafiek 2.3.2.3). Grote organisaties zijn al wat langer geleden begonnen met integrale risico-identificatie en –analyse, middelgrote organisaties hebben dat doorgaans vrij recentelijk gedaan en de meeste kleinere organisaties hebben nog slechts plannen daartoe.

Grafiek 2.3.2.2 Wanneer is uw organisatie begonnen met het uitvoeren van integrale risico-inventarisaties en –analyses?



Grafiek 2.3.2.3 Wanneer is uw organisatie begonnen met het uitvoeren van integrale risico-inventarisaties en –analyses?



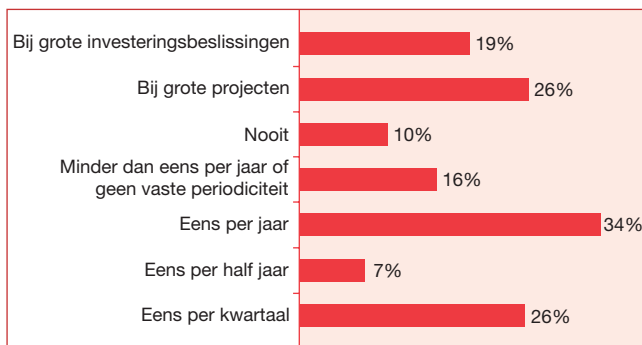
In ons onderzoek (zie grafiek 2.3.2.1) hebben wij respondenten gevraagd aan te geven wanneer hun organisatie is gestart met het uitvoeren van integrale risico-identificaties en –analyses. Voor bijna de helft (47%) van alle organisaties blijkt dit in de afgelopen drie jaren te zijn geweest. Voor 19% is dat al wat langer geleden. 34% van de organisaties heeft nog nooit een integrale risico-identificatie en –analyse uitgevoerd. Echter 26% daarvan geeft aan dat wel van plan te zijn.

Een uitsplitsing naar branche (zie grafiek 2.3.2.2) laat zien dat het met name de overheid en non-profit sector is waar men voornemens is te gaan starten met het uitvoeren van integrale risico-identificaties en –analyses (45%). Ander opvallend punt is dat 51% van de Energie & Utilities bedrijven reeds langer dan drie jaar geleden is aangevangen met het integraal identificeren en analyseren van risico's.

### 2.3.3 Jaarlijkse risicoanalyse meest gebruikelijk

Risicomanagement wordt gedefinieerd als een proces. Het uitvoeren van een risico-identificatie en –analyse is dus niet iets dat je slechts eenmalig uitvoert, maar met een zekere periodiciteit herhaalt. In ons onderzoek (zie grafiek 2.3.3) hebben wij de respondenten gevraagd aan te geven hoe vaak het management in hun organisatie een risico-identificatie en –analyse uit dient te voeren. Het meest voorkomend blijkt 'eens per jaar' (34%) en 'eens per kwartaal' (26%). Halfjaarlijks blijkt minder gangbaar (7%). In 16% van de organisaties is de periodiciteit minder dan een jaar of kent men geen vaste periodiciteit.

Grafiek 2.3.3 Hoe vaak dient het management in uw organisatie een risico-inventarisatie en -analyse uit te (laten) voeren en hierover te rapporteren?



Uit bovenstaande grafiek is niet af te lezen dat in de praktijk de diepgang van de risicoanalyses op verschillende momenten in het jaar kan verschillen. Een in de praktijk veel voorkomende en in onze ogen goed werkbaar vorm is een jaarlijkse diepgaande risicoanalyse, gekoppeld aan het opstellen van het jaarplan en budget. Gedurende het jaar, meestal per kwartaal, wordt vervolgens het risicoprofiel nog eens tegen het licht gehouden om te kijken of er significante wijzigingen zijn opgetreden. Deze minder diepgaande analyse wordt vaak gekoppeld aan het opstellen en bespreken van de kwartaalrapportage.

Naast de reguliere cyclus zijn er ook andere momenten die een natuurlijke aanleiding geven voor het uitvoeren van een risicoanalyse. Bijvoorbeeld indien een onderneming overweegt een grote investering te doen kan het zinvol zijn om de risico's die die investering met zich mee brengt expliciet in kaart te brengen. Uit het onderzoek blijkt echter dat bij slechts 19% van de respondenten grote investeringsbeslissingen in hun organisatie een reden vormen voor het uitvoeren van een risicoanalyse.

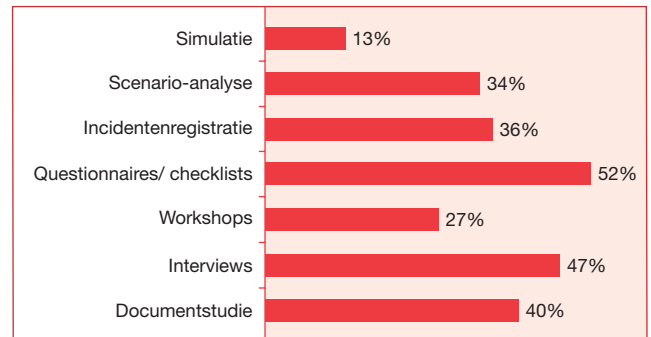
Ook grote projecten vormen een natuurlijke aanleiding om risico's gestructureerd in kaart te brengen en te analyseren. Risicomanagement is een kernonderdeel van goed projectmanagement. Binnen Nederlandse organisaties is dit echter, blijkens de enquête, doorgaans niet het geval. Slechts 26% van de organisaties voert een expliciete risicoanalyse uit voor grote projecten.

### 2.3.4 Risicoanalyse veelal met behulp van combinatie van technieken

Er zijn meerdere technieken toepasbaar voor het identificeren en analyseren van risico's. De technieken zijn in sterke mate gelijk aan gangbare onderzoekstechnieken. In het onderzoek (zie grafiek 2.3.4) is aan respondenten gevraagd aan te geven welke technieken in hun organisatie gehanteerd worden. Checklists, al dan niet in de vorm van een questionnaire, worden in 52% van de organisaties gebruikt en zijn daarmee het meest populaire instrument. In 47% van de organisaties wordt gebruik gemaakt van interviews bij het identificeren en/of analyseren van risico's. Ook documentstudie wordt veelvuldig toegepast (40%).

Opvallend is dat 36% van de organisaties aangeeft gebruik te maken van incidentenregistratie en 34% aan scenarioanalyse doet. Dit is opvallend omdat deze technieken als meer verfijnde technieken voor risico-identificatie worden gezien.

Grafiek 2.3.4 Welke technieken worden in uw organisatie gebruikt voor het identificeren en analyseren van risico's?



Risicomanagement workshops worden in 27% van de organisaties gehouden. Dit instrument wordt vooral toegepast in grotere organisaties. Simulatietechnieken worden slechts op beperkte schaal in organisaties toegepast voor het analyseren van risico's (13%). De meeste respondenten geven aan meerdere technieken te gebruiken voor het identificeren en analyseren van risico's.

Een relatief eenvoudig hulpmiddel voor het identificeren van risico's is een risicomodel. Een risicomodel is een standaardclassificatie en van alle typen risico's waar een organisatie mee te maken kan hebben. De generieke risico's of risicogebieden waaruit het risicomodel is opgebouwd dekken tezamen op een relatief hoog abstractieniveau het gehele risico-universum van de organisatie af. Figuur 1.9 toont het standaard Business Risk Model van PricewaterhouseCoopers. Uiteraard zal voor elke organisatie een op de organisatie toegesneden risicomodel gemaakt moeten worden. Dit model biedt wellicht een goed startpunt. De bijbehorende risico-omschrijvingen zijn hier niet opgenomen.

Het werken met een risicomodel heeft een aantal voordelen. Ten eerste biedt het een goede kapstok voor het identificeren van risico's. De generieke risico's kunnen als het ware worden ontleed in specifieke voor de organisatie herkenbare risico's. Ten tweede kan het risicomodel worden gebruikt voor een volledigheidstoets aan het einde van een risico-identificatieproces (hebben we wel overal aan gedacht?). Een derde voordeel is dat door uniform gebruik van het risicomodel en de bijbehorende risico-omschrijvingen in de gehele organisatie de communicatie over risico's en risicomanagement wordt vereenvoudigd. Dit is vaak een eerste belangrijke stap naar organisatiebreed risicomanagement. Een vierde voordeel van het werken met een risicomodel is dat indien alle organisatieonderdelen met hetzelfde risicomodel werken ook langs deze lijnen een consolidatie plaats kan vinden van risicoprofielen tot een risicoprofiel op een hoger niveau in de organisatie. Bovendien maakt het vergelijking tussen verschillende organisatieonderdelen mogelijk.

Figuur 1.9 PricewaterhouseCoopers Business Risk Model

<b>Environment risk</b>	Competitor Sovereign/political	Customer wants Legal	Technological innovation Regulatory	Sensitivity Industry	Shareholder relations Financial markets	Capital availability Catastrophic loss
<b>Process risk</b>	<b>Operations</b> Customer satisfaction Human resources Knowledge capital Product development Efficiency Capacity Performance gap Cycle time Sourcing Channel effectiveness Partnering Compliance Business interruption Product/service failure Environmental Health and safety Trademark/brand erosion	<b>Empowerment</b> Leadership Authority/limit Outsourcing Performance incentives Change readiness Communications	<b>Information processing/technology</b> Relevance Integrity Access Availability Infrastructure	<b>Integrity</b> Management fraud Employee/third party fraud Illegal acts Unauthorized use Reputation	<b>Financial</b> Price Interest rate Currency Equity Commodity Financial instrument	<b>Liquidity</b> Cash flow Opportunity cost Concentration
<b>Information for decision making risk</b>	<b>Process/operational</b> Product/service pricing Contract commitment Measurement (operations) Alignment	<b>Business reporting</b> Budget and planning Accounting information Financial reporting evaluation Taxation Pension fund Investment evaluation Regulatory reporting	<b>Environment/strategic</b> Environmental scan Business model Business portfolio Valuation Organization structure Measurement (strategy) Resource allocation Planning Life cycle			

### 2.3.5 Vooral grotere organisaties maken gebruik van elektronische hulpmiddelen

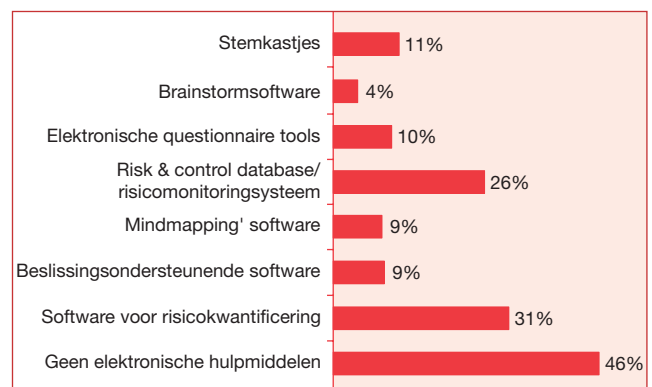
Er is een groot aantal elektronische hulpmiddelen ('tools') op de markt beschikbaar die ondersteuning kunnen bieden bij de uitvoering van risicomanagement activiteiten. Voordelen van dergelijke software zijn dat ze besluitvormingsprocessen ondersteunen en grote hoeveelheden data kunnen opslaan en bewerken. Er is de laatste jaren een duidelijke trend zichtbaar naar toenemend gebruik van risicomanagement software. In beginsel is dat een goede ontwikkeling, omdat het gebruik van software een belangrijke rol kan vervullen in het borgen van ontwikkelde risicomanagement processen. Het komt echter ook steeds meer voor dat organisaties al in een zeer vroeg stadium, nog voordat een passende risicomanagement benadering zich in de organisatie heeft ontwikkeld en bewezen, overgaan tot de aanschaf en implementatie van risicomanagement software. In onze optiek is dat niet de juiste volgorde. Het gevaar schuilt erin dat de software dwingt tot een bepaalde werkwijze terwijl dit in de specifieke situatie voor de specifieke organisatie niet de meest optimale werkwijze is. Beter is het om eerst ervaring op te doen met risicomanagement, mogelijke werkwijzen uit te proberen, en pas na verloop van tijd door middel van een gedegen softwareselectieproces de meest geschikte software bij de ontwikkelde methodiek te zoeken. De voordelen van ondersteunende software worden dan optimaal benut.

Uit het onderzoek blijkt dat 54% van de organisaties één of meerdere elektronische hulpmiddelen gebruikt. Het meest populair is software voor risicokwantificering (31%).

Veelal gaat het hier om zelfgebouwde spreadsheets waarin de omvang van een risico wordt berekend aan de hand van een aantal variabelen. Overigens geldt voor de meeste risico's dat ze moeilijk te kwantificeren zijn wegens gebrek aan historische data. Het zijn vooral typisch financiële risico's als het valutarisico of het kredietrisico die in detail gekwantificeerd worden.

Risicomonitoring-systemen worden blijkens het onderzoek (zie grafiek 2.3.5.1) eveneens veel gebruikt (26%). Deze systemen kunnen variëren van vrij eenvoudige Excel-sheets of MS Access-databases (risicoregister) tot omvangrijke, zeer verfijnde risk management workflow en risk intelligence systemen die real-time verbonden zijn aan andere informatiesystemen binnen de organisatie, zoals bijvoorbeeld het financiële systeem of het personeelsmanagementsysteem. De overige elektronische hulpmiddelen worden beduidend minder toegepast.

Grafiek 2.3.5.1 Worden er in uw organisatie elektronische hulpmiddelen (tools) gebruikt bij risicomanagement en zo ja, welke?



Bij een uitsplitsing naar omvang van de organisatie (gemeten in omzet) valt op dat met name in kleine organisaties weinig gebruik wordt gemaakt van elektronische hulpmiddelen bij risicomanagement (33%). Daarentegen maakt van de grote organisaties juist 82% gebruik van elektronische hulpmiddelen (zie grafiek 2.3.5.2).

Naast hierboven reeds genoemde risicomonitoring-systemen en software voor risicokwantificering wordt in grote organisaties ook relatief veel gebruik gemaakt van stemkastjes-systemen (23%). Deze stemkastjes worden gebruikt tijdens workshops waarin management teams bij elkaar zitten om onder meer de omvang van geïdentificeerde risico's in te schatten. Veelal gebeurt dit door de deelnemers aan de workshop een score te laten toekennen aan de kans dat een risico zich voordoet en de impact ingeval het risico zich voordoet. De vermenigvuldiging van de gemiddeld toegekende kans maal de gemiddeld toegekende impact bepaald dan de omvang van het risico. Door het inschatten van de omvang van een risico op deze wijze door middel van een groepsproces te laten verlopen wordt de kwaliteit van de risico-inschatting verhoogd. Er wordt immers gebruik gemaakt van de cumulatieve kennis van de aanwezigen. De subjectieve risico-inschatting wordt zo veel mogelijk geobjectiveerd. Het gehanteerde stemkastjessysteem maakt de resultaten van de risico-

inschatting direct zichtbaar, inclusief de stembreiding. Mogelijke verschillen van inzicht worden hiermee direct blootgelegd hetgeen gerichte discussie mogelijk maakt. Vaak zijn het juist deze discussies die door het aanwezige management als waardevol worden ervaren.

#### Kader 2.6

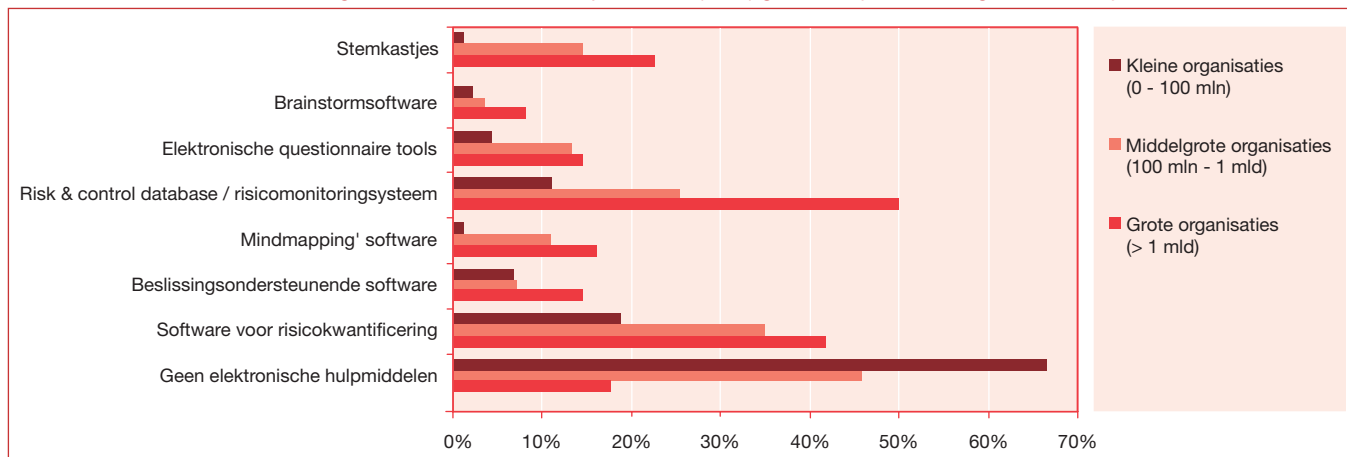
“Worden er in uw organisatie elektronische hulpmiddelen (tools) gebruikt bij risicomanagement en zo ja, welke?”

Bij het inschatten van de kans en de impact van een risico op de wijze als hierboven beschreven is het van belang dat er duidelijke afspraken zijn gemaakt over wanneer een risico als bijvoorbeeld hoog, midden of laag kan worden bestempeld. Indien twee deelnemers aan een workshop beide van mening zijn dat de mogelijke impact van een risico circa 10 miljoen euro is, kan het nog steeds zo zijn dat de één het risico als laag beoordeeld en de ander het een hoog risico vindt. Om dit te voorkomen is het zinvol om vooraf de schaal vast te leggen waarlangs gescoord wordt en de betekenis van de mogelijke scores op die schaal. Dit wordt veelal aangeduid met de term 'risk appetite matrix', omdat het een uiting is van de risicobereidheid van de organisatie. Onderstaande figuur bevat een voorbeeld van een 'risk appetite matrix' voor wat betreft de impact van de in te schatten risico's.

Figuur 1.10 Matrix voor het inschatten van de impact van een risico ingeval van optreden.

IMPACT	Score									
	1	2	3	4	5	6	7	8	9	10
	Laag			Midden				Hoog		
Marktpositie	Leidt niet tot verlies van top 3 positie.			Leidt tot daling naar nr. 4 positie.				Leidt tot daling naar nr. 5 positie of lager.		
Netto resultaat	Verlies van netto resultaat van <i>minder dan 1%</i> ten opzichte van begroot resultaat.			Verlies van netto resultaat van <i>meer dan 1% maar minder dan 10%</i> ten opzichte van begroot resultaat.				Verlies van netto resultaat van <i>meer dan 10%</i> ten opzichte van begroot resultaat.		
Groei	Verlies van <i>minder dan 1%</i> van de begrote groei.			Verlies van <i>meer dan 1% maar minder dan 3%</i> van de begrote groei.				Verlies van <i>meer dan 3%</i> van de begrote groei.		
Reputatie	Geen negatieve aandacht in media			Beperkte negatieve aandacht in media. Opmerking van toezichhouder				Ruime negatieve aandacht in media Sanctie van toezichhouder		

Grafiek 2.3.5.2 Worden er in uw organisatie elektronische hulpmiddelen (tools) gebruikt bij risicomanagement en zo ja, welke?



# 2.4 Beheersen van risico's

## 2.4.1 Vier manieren om op risico te reageren

De meest voor de hand liggende manier om met een risico om te gaan is het invoeren van beheersmaatregelen om het risico te beperken. Dit is echter maar één van de beschikbare mogelijkheden om op een risico te reageren. Risico's hoeven immers niet per definitie altijd beperkt te worden. Juist door het nemen van risico bereikt een organisatie immers haar doelen. Daarom kan ook het bewust accepteren van een risico een goede risicoreactie zijn. En ook als acceptatie van een risico niet gewenst is zijn er meerdere mogelijkheden om een risico te beperken dan alleen het invoeren van beheersmaatregelen. In beginsel zijn er vier basisstrategieën om met een risico om te gaan. Deze worden in onderstaande figuur weergegeven.

Figuur 1.11 Vier generieke risicoreactiestrategieën



Vooraf bij risico's op strategisch niveau zal er variatie zitten in de gekozen reactiestrategie per risico. Immers het maken van strategische keuzes impliceert het bewust nemen en dus accepteren van risico's. Bij risico's op operationeel procesniveau, dus bij het operationeel maken van de strategische keuzes, wordt doorgaans weinig risico geaccepteerd. De voor de hand liggende reactie is daar het beheersen van de risico's.

## 2.4.2 Aanwezige beheerssystematieken worden doorgaans als effectief ervaren

Een beheersmaatregel kan vele vormen aannemen. Elke activiteit, geautomatiseerd of door mensen verricht, die de kans en/of de impact van een risico verkleint kan worden bestempeld als een beheersmaatregel. Vanuit dit oogpunt kent een organisatie een ontelbare hoeveelheid beheersmaatregelen. Er hebben zich in de loop der jaren een aantal meer of minder gangbare beheersingssystematieken ontwikkeld waarin meerdere individuele beheersmaatregelen besloten liggen. In ons onderzoek hebben wij respondenten gevraagd aan te geven welke van deze beheerssystemen in hun organisatie aanwezig zijn. Tevens is hen gevraagd aan te geven in welke mate die beheerssystemen effectief worden geacht. Er blijken twee beheerssystemen te zijn die door het overgrote deel van de organisaties worden toegepast (99%) en bovendien als het meest effectief worden gezien. Dit zijn de planning & controlsystematiek en de administratieve organisatie / interne controle. Opvallend is verder dat alle genoemde beheerssystemen als effectief worden beschouwd. Het minst effectief, maar nog steeds meer wel dan niet effectief, is de klokkenluiderregeling. Deze komt bovendien met 48% het minst voor in de ondervraagde organisaties.

Uit tabel 2.4.2.1 blijkt dat de genoemde beheerssystemen in sterke mate aanwezig zijn binnen de ondervraagde organisaties. De percentages zijn zo hoog dat de vraag zich opdringt of de werkelijkheid er inderdaad zo uit ziet als hier voorgespiegeld. De ervaringen in onze adviespraktijk leren dat de werkelijkheid een stuk weerbarstiger is. Wij zien bijvoorbeeld nog niet zo veel organisaties die op gestructureerde wijze aan Business Continuity Planning doen. Veel organisaties hebben wel een herstel- en uitwijkplan voor de IT-systemen, maar daarmee is het bedrijf natuurlijk nog niet direct op de rails in geval van een ramp of crisissituatie. Ook het hoge percentage respondenten dat hier aangeeft aan risicoanalyse te doen moet wellicht met enige voorzichtigheid worden geïnterpreteerd. Eerder

Tabel 2.4.2.1 Welke beheersmaatregelen of beheerssystemen zijn in uw organisatie aanwezig en hoe beoordeelt u de effectiviteit?

	Aanwezig		Indien wel aanwezig		
	Ja	Nee	Niet effectief		Zeer effectief
Gedragcode	81%	19%			
Klokkenluiderregeling	48%	52%			
Planning & controlsystematiek	99%	1%			
Administratieve organisatie / Interne Controle	99%	1%			
Risk & control matrices / process control models	68%	32%			
Risicoanalyse	88%	12%			
Kwaliteitsmanagement (ISO, EFQM, INK)	72%	28%			
Performance management (KPI'en, BBSC)	85%	15%			
Business Continuity Planning	63%	37%			
Benchmarking	79%	21%			
Scenario planning	62%	38%			

in dit rapport, bij paragraaf 2.3.2, zagen we immers dat circa eenderde van de organisaties nog niet is begonnen met het uitvoeren van risico-inventarisaties en –analyses. Dit strookt niet met de 12% uit bovenstaande tabel. Ook de genoemde 66% van de organisaties dat aan scenario planning doet wekt enige verbazing. In paragraaf 2.3.4 was dat immers nog slechts 36%.

Onze inschatting is dat genoemde beheerssystemen in veel mindere mate aanwezig zijn binnen organisaties dan de resultaten op deze enquêtevraag willen doen geloven. De oorzaak ligt er waarschijnlijk in dat de genoemde beheerssystemen wel op de agenda staan in veel organisaties. Echter de praktijk leert dat dit niet betekent dat ze daadwerkelijk adequaat zijn en effectief werken.

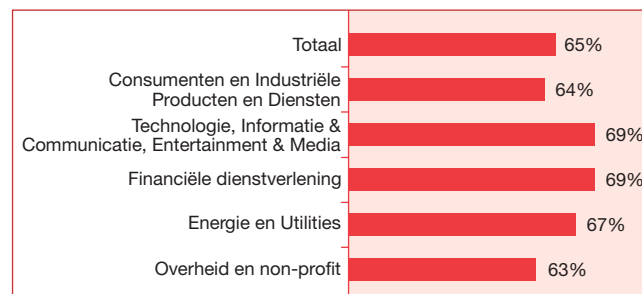
### 2.4.3 De bedragen die organisaties aan risicomanagement uitgeven zijn aanzienlijk

Het adequaat managen van risico's kost geld. Zeker als gevolg van wet- en regelgeving als bijvoorbeeld de Amerikaanse Sarbanes-Oxley Act zien beursgenoteerde ondernemingen steeds grotere delen van hun budget verdwijnen in aan risicomanagement gerelateerde projecten en activiteiten. In het onderzoek is aan de respondenten gevraagd aan te geven hoeveel geld hun organisatie jaarlijks uitgeeft aan risicomanagement. Hierbij is niet aangegeven welke uitgaven in deze categorie passen. Zo zal de ene respondent wellicht slechts projectbudgetten voor risicomanagement projecten hebben opgeteld, terwijl de andere respondent ook de kosten van de uitvoering van allerlei beheersmaatregelen in de organisatie in zijn berekening kan hebben meegenomen. Daarom moet het overzicht dat onderstaande tabel biedt met enige voorzichtigheid worden geïnterpreteerd. Desalniettemin geeft het wel een inzicht in de omvang van de bedragen die met risicomanagement gemoeid zijn. Zo laat de tabel zien dat circa de helft van de grote organisaties (49%) jaarlijks meer dan een miljoen euro's uitgeeft aan risicomanagement (zie grafiek 2.4.3).

### 2.4.4 Er bestaat een redelijk vertrouwen in de huidige kwaliteit van de beheersing

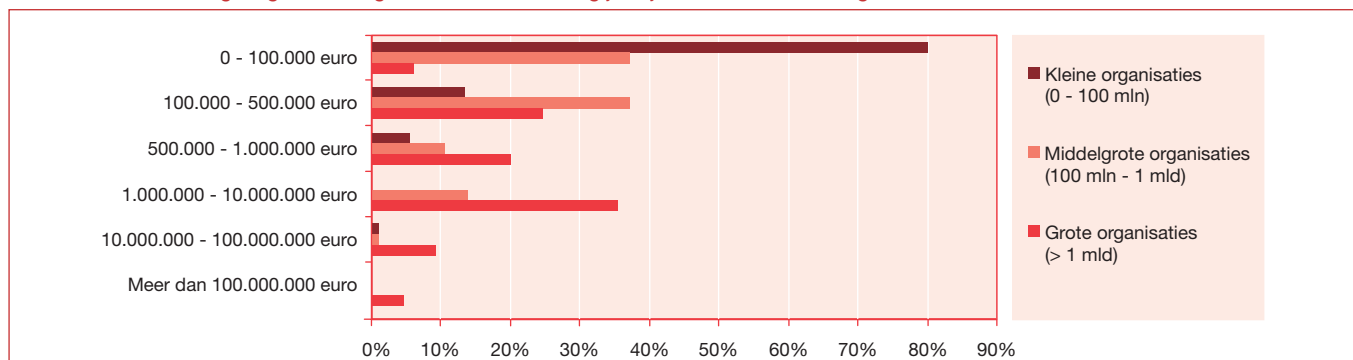
Uit de voorgaande paragrafen is gebleken dat de uitgaven aan risicomanagement hoog zijn, maar dat de beheersings-systematieken die men heeft ingericht ook wel degelijk als effectief worden ervaren. Deze conclusie wordt ondersteund door onderstaande tabel. Hier is de respondenten gevraagd hoeveel vertrouwen zij erin hebben dat de beheersmaatregelen in hun organisatie de organisatie voor aanzienlijke financiële schade zullen behoeden. In procenten uitgedrukt heeft men er gemiddeld genomen 65% vertrouwen in dat de beheersmaatregelen inderdaad aanzienlijke financiële schade voor de organisatie zullen voorkomen. De onderscheiden branches verschillen op dit punt weinig.

Grafiek 2.4.4.1 Hoeveel vertrouwen heeft u erin dat de beheersmaatregelen van uw organisatie aanzienlijke financiële schade zullen voorkomen?



Uit het bovenstaande kan afgeleid worden dat hoewel men tevreden is over de effectiviteit van beheersings-systematieken (zie paragraaf 2.4.3) dit de respondenten nog geen zekerheid geeft dat de organisatie niet iets zal overkomen dat een zware financiële impact heeft. Dit strookt met onze ervaring dat er bij de meeste organisaties nog ruimte is voor verbeterlagen als het gaat om de kwaliteit van risicobeheersing.

Grafiek 2.4.3 Hoeveel geld geeft uw organisatie naar schatting jaarlijks uit aan risicomanagement?



## 2.5 Rapporteren van risico's

### 2.5.1 Risicorapportage veelal ingebouwd in planning & controlcyclus

Een belangrijk element van risicomanagement is het intern rapporteren over risico's. Voor het hogere management van een organisatie is het zeer zinvol om een goed inzicht te hebben in de aard en de omvang van de risico's die in de diverse organisatieonderdelen (en daarmee door de organisatie als geheel) worden gelopen. Alleen als dat inzicht bestaat kunnen de financiële prestaties van een organisatieonderdeel ook op waarde worden geschat. Het geeft antwoord op de vraag hoeveel risico men loopt om de gerapporteerde financiële resultaten te realiseren. Tevens biedt het het hoger management inzicht in de issues die lager in de organisatie spelen en hoe het betreffende management daarmee om gaat.

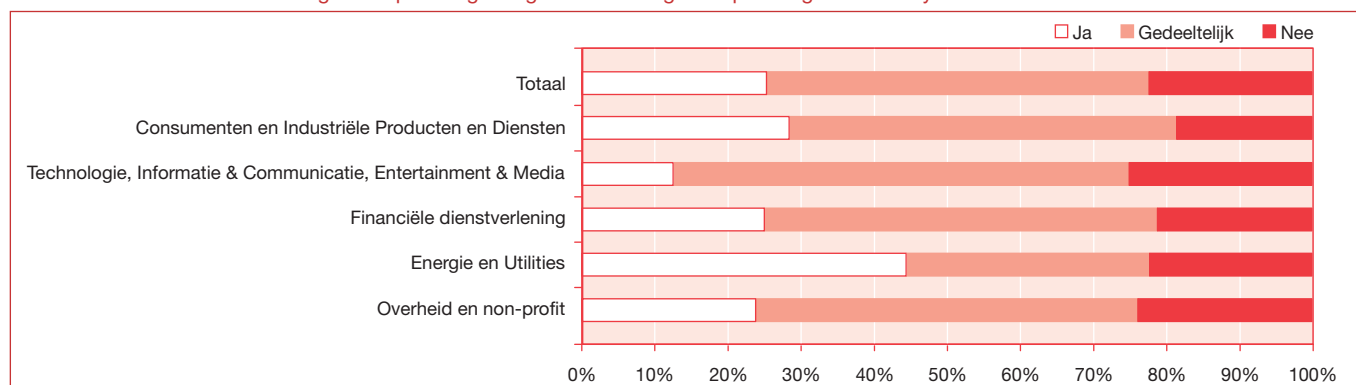
De meest eenvoudige weg om het rapporteren over risico's in de organisatie in te voeren is dit te koppelen aan de planning & controlcyclus die in de meeste organisaties reeds bestaat. Bijvoorbeeld het opstellen van een operationeel plan - in veel organisaties een jaarlijks terugkerend verschijnsel - biedt een uitstekend aanknopingspunt voor het betreffende management om haar risicoprofiel nog eens goed tegen het licht te houden. Het aldus opgebouwde of geactualiseerde risicoprofiel en de daarbij geformuleerde verbeteracties kunnen dan worden opgenomen in het operationele plan. Vervolgens rapporteert het verantwoordelijke management gedurende het jaar over de realisatie van het opgestelde plan. Ook in deze rapportages kan -

bijvoorbeeld per kwartaal - een extra paragraaf worden opgenomen waarin het hogere management inzicht wordt geboden in de voortgang van de afgesproken acties en van eventuele significante wijzigingen in het risicoprofiel. Van belang hierbij is dat bij de bespreking van de plannen en rapportages het onderwerp risicomanagement ook expliciet aan bod komt. Het sluitstuk van de cyclus kan bestaan uit een 'in-control verklaring' van het verantwoordelijk management richting het hogere management (zie ook paragraaf 2.5.2).

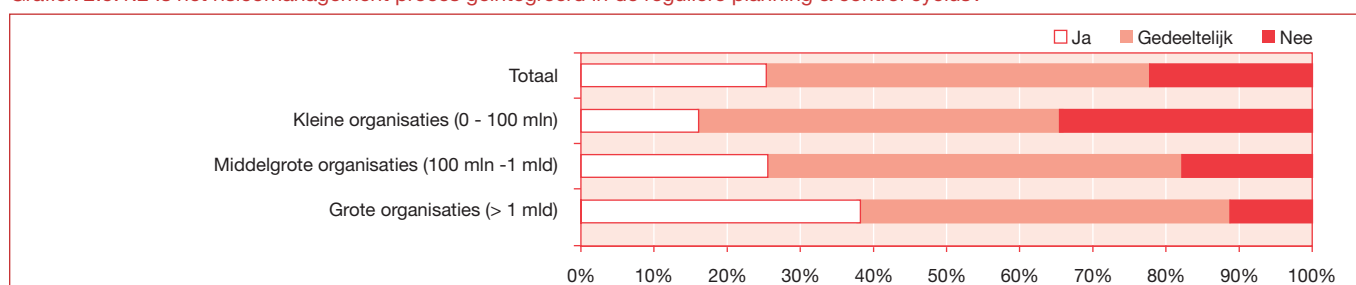
In het onderzoek is respondenten gevraagd of in hun organisatie het risicomanagement proces is geïntegreerd in de planning & controlcyclus. In 77% van de organisaties blijkt dit geheel (25%) of gedeeltelijk (52%) het geval te zijn. Het beeld dat in 23% van de organisaties er dus geen sprake is van integratie in de planning & controlcyclus komt overeen met het beeld in alle branches dat een uitsplitsing naar branche laat zien. Opvallend aan de uitsplitsing naar branche is dat vooral in de energie & utilities branche vaak (44%) sprake is van volledige integratie in de planning & controlcyclus. Met name de technologie-, communicatie- & entertainment bedrijven blijven hier achter (13%).

Een uitsplitsing naar grootte van de organisaties (gemeten naar omzet) laat het te verwachten beeld zien. In grotere organisaties is risicomanagement meer geïntegreerd in de planning & control dan in kleinere organisaties. In 89% van de grote organisaties (> 1 miljard omzet) is risicomanagement deels of geheel in de planning & control geïntegreerd.

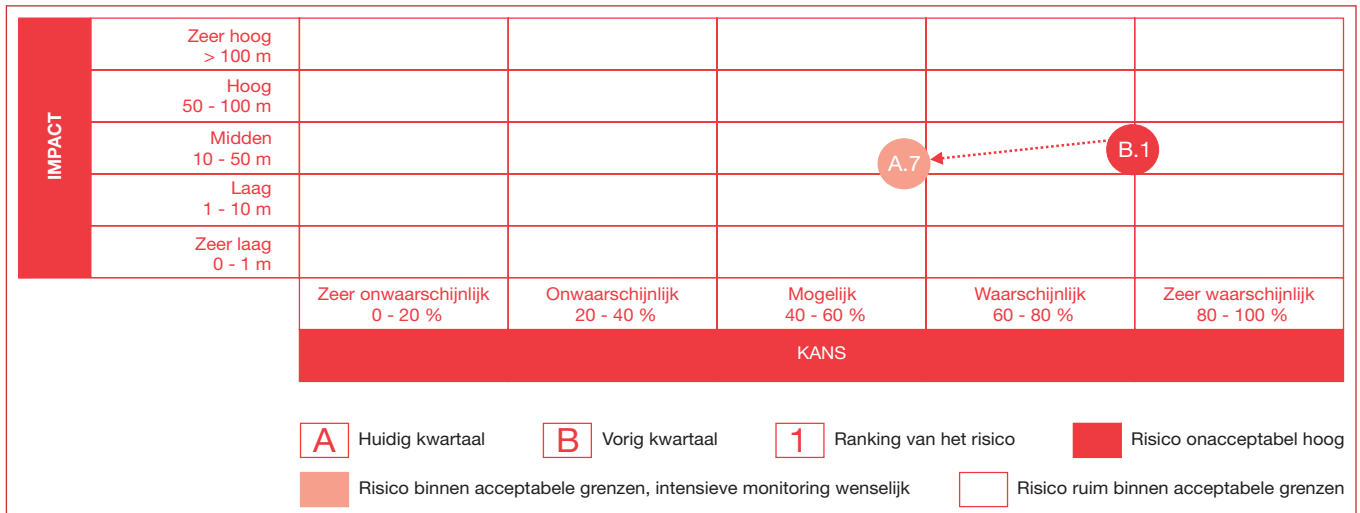
Grafiek 2.5.1.1 Is het risicomanagement proces geïntegreerd in de reguliere planning & control cyclus?



Grafiek 2.5.1.2 Is het risicomanagement proces geïntegreerd in de reguliere planning & control cyclus?



Figuur 1.12 Voorbeeld risicomatrix



Desalniettemin is het percentage grote bedrijven waar sprake is van volledige integratie in de planning & control-cyclus (38%) niet hoog te noemen, gezien het aantal jaren dat deze organisaties reeds actief zijn op het gebied van risicomanagement.

Als gezegd is het invoegen van een risicomanagement paragraaf in de reguliere maand- of kwartaalrapportage een vrij eenvoudige manier om op een gestructureerde manier te rapporteren over risico's. Een dergelijke paragraaf kan vrij beknopt zijn. Doorgaans vormen drie elementen de basis voor een risicomanagement paragraaf. Ten eerste is dat de risicomatrix. In een risicomatrix worden de belangrijkste risico's van een organisatie(onderdeel) geplot op een matrix met op de assen de kans van optreden en de impact ingeval van optreden. Figuur 1.12 laat een voorbeeld zien.

Omdat het een periodieke rapportage betreft is het zinvol om inzichtelijk te maken hoe het risicoprofiel van de organisatie zich heeft ontwikkeld ten opzicht van de vorige rapportageperiode. In bovenstaand voorbeeld is dit gedaan door van elk risico te laten zien waar het risico zich nu

bevindt en waar het zich het vorige kwartaal bevond. De verandering wordt inzichtelijk gemaakt door de pijl die het huidige kwartaal met het vorige kwartaal verbindt. Daarnaast geeft de kleur van het bolletje aan of de omvang van het risico wel of niet acceptabel is. In dit voorbeeld is verbetering aangebracht in de beheersing van het betreffende risico. De kleur is veranderd van rood in het vorige kwartaal naar geel in dit kwartaal.

Een dergelijke risicomatrix dient vergezeld te gaan van een toelichtend schrijven. In het bijzonder dient toelichting te worden gegeven op nieuw opgenomen risico's, verwijderde risico's en significante verschuivingen binnen de matrix.

Naast de omvang van de risico's en de verschuivingen daarin dient uiteraard ook een goed inzicht te bestaan in de inhoud van de risico's en genomen en geplande maatregelen om het risico te managen. Hiervoor wordt veelal een zogenaamd risicoregister opgenomen in risicorapportages. Figuur 1.13 bevat een voorbeeld. Aan de hand van de nummering van de risico's is een relatie te leggen tussen de risicomatrix en het risicoregister.

Figuur 1.13 Voorbeeld risicoregister

Rank	Rank vorig kwartaal	Risico	Omschrijving	Categorie	Kans	Impact	Risico-omvang	Bestaande maatregelen	Risico-eigenaar	Risico-reactie	Acties	Wie	Status	Eind-datum
1														
2														
3														
4														
5														
6														
7	1													
8														
9														
10														
11														
12														
13														
14														
15														

Het voorbeeld van een risicoregister in figuur 1.13 bevat reeds 15 kolommen met informatie voor elk risico. Het is zeer wel mogelijk dat de informatiebehoefte nog groter is. Denk bijvoorbeeld aan de doelstellingen of KSF'en waar het risico aan gekoppeld is, de kosten van de gekozen risicoreactie en de verwachte kans en impact na werking van de gekozen risicoreactie. Naarmate er meer verfijndheid komt in het risicomanagement van een organisatie en er meer en diepgaandere analyses worden uitgevoerd zal een eenvoudige tabel of spreadsheet als hierboven minder goed voldoen. Indien een organisatie een dergelijk stadium bereikt is het vaak een goed moment om over te gaan op meer professionele risicomanagement informatiesystemen waarin de diverse analysemethoden en rapportagevormen geïntegreerd zijn.

Een derde kernelement van periodieke risicorapportage is het rapporteren van incidenten die zich in de afgelopen periode binnen het organisatie(onderdeel) hebben voorgedaan. Hierbij moet gedacht worden aan incidenten in de breedste zin des woords, dus niet enkel in de sfeer van ARBO, veiligheid of milieu. Indien elk organisatieonderdeel periodiek al haar incidenten rapporteert kan vrij eenvoudig een organisatiebreed incidentenregister worden opgebouwd. Dit incidentenregister bevat na verloop van tijd zeer waardevolle historische gegevens met behulp waarvan kwantitatieve analyse van risico's mogelijk wordt gemaakt.

## 2.5.2 In-control verklaringen vooral in gebruik bij beursgenoteerde ondernemingen

In zowel de publieke als de private sector wordt steeds meer van organisaties verwacht dat zij ook extern communiceren over de kwaliteit van het risicomanagement in de organisatie. De gedachte hierbij is dat belanghebbenden in de organisatie (bijv. aandeelhouders) dan beter in staat zijn te beoordelen of de organisatie op de juiste wijze met hun belangen omgaat en niet te veel risico neemt of risico's onvoldoende beheerst. Deze externe communicatie over de risico's en het risicomanagement van de organisatie vindt vooral plaats in de vorm van een corporate governance paragraaf en/of risicomanagement paragraaf in het jaarverslag. Veelal is hier een verklaring opgenomen omtrent de kwaliteit van het risicomanagement in de organisatie.

Voor beursgenoteerde bedrijven is dit verplicht onder de code Tabaksblat en de meeste corporate governance codes in andere landen.

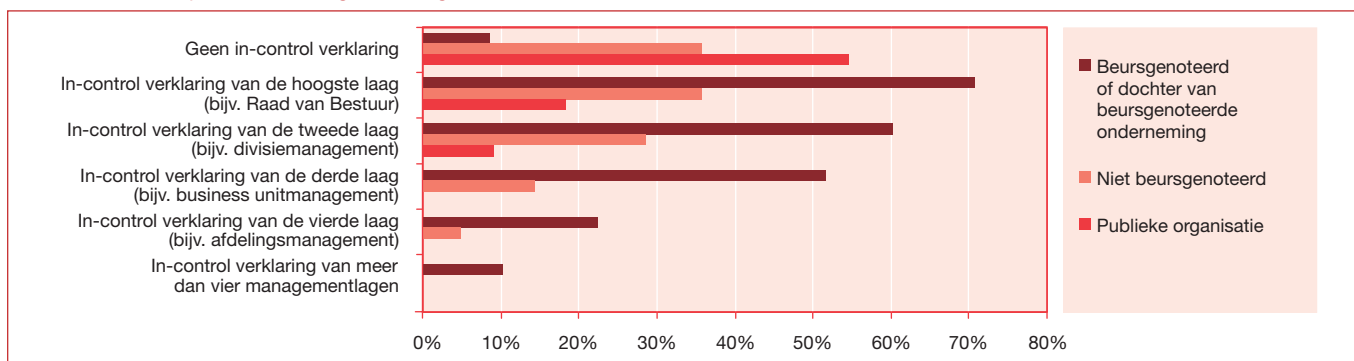
Om een externe verklaring over de kwaliteit van het risicomanagement te kunnen afgeven kiezen veel organisaties ervoor om binnen de organisatie van verantwoordelijk management op lagere niveaus ook een dergelijke verklaring te verlangen. Op deze wijze wordt van onderuit de organisatie de basis gecreëerd waarop extern over het onderwerp risicomanagement kan worden gerapporteerd.

In het onderzoek (zie grafiek 2.5.2.1) hebben wij gevraagd naar de aanwezigheid van dergelijke 'in-control verklaringen'. Daarbij is gevraagd naar het aantal managementlagen dat een dergelijke verklaring af dient te geven. Voor beursgenoteerde ondernemingen geldt dat bij 71% de Raad van Bestuur een dergelijke verklaring afgeeft. 11% daarvan laat het daarbij, terwijl de overige 60% ook van de tweede managementlaag (bijv. divisie management) een in-control verklaring verlangt. 52% daarvan doet dat ook bij de derde managementlaag en 22% bij de vierde managementlaag. Bij 10% van de beursgenoteerde bedrijven wordt een in-control verklaring afgegeven door meer dan de bovenste vier managementlagen.

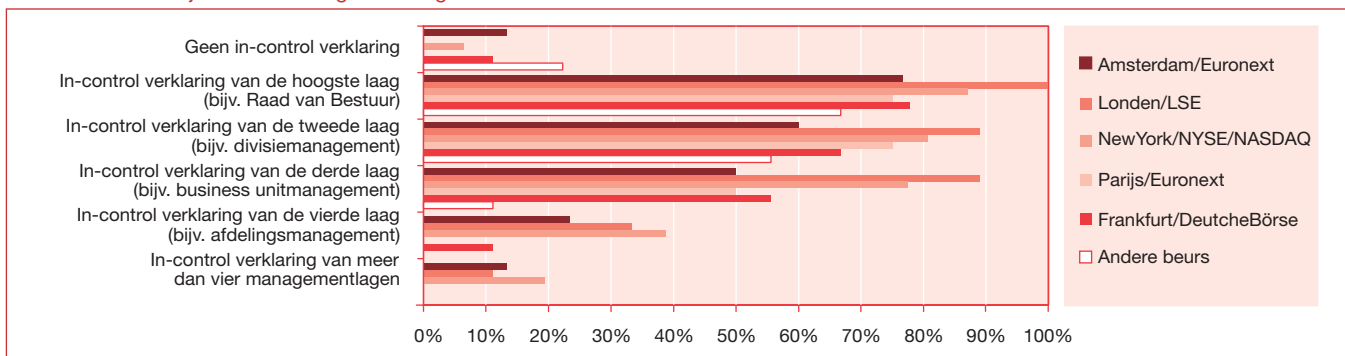
Uit grafiek 2.5.2.1 blijkt dat binnen niet-beursgenoteerde organisaties het gebruik van in-control verklaringen al veel minder gemeengoed is. En in de publieke sector komt het nog een stuk minder voor.

Het gebruik van interne in-control verklaringen komt doorgaans voort uit de behoefte die in de top van de organisatie leeft om een basis te creëren voor de externe verklaring die zij naar de buitenwereld af dienen te geven. Een tweede reden kan zijn dat door het laten tekenen van in-control verklaringen de persoonlijke verantwoordelijkheid van managers op alle niveaus in de organisatie voor adequate risicobeheersing expliciet wordt benadrukt. Het onderwerp komt hiermee ook meer op de agenda te staan bij operationeel management, hetgeen een goede ontwikkeling is. Het aantal managementlagen dat een in-control verklaring zou moeten tekenen hangt uiteraard af van de specifieke organisatie. Echter naar onze mening kan dit relatief diep in de organisatie worden ingevoerd. Het zou ons inziens goed

Grafiek 2.5.2.1 Wordt er binnen uw organisatie gewerkt met een verklaring van het verantwoordelijke management dat hun organisatieonderdeel 'in-control' is en zo ja voor welke organisatielagen?



Grafiek 2.5.2.2 Wordt er binnen uw organisatie gewerkt met een verklaring van het verantwoordelijke management dat hun organisatieonderdeel 'in-control' is en zo ja voor welke organisatieelagen?



zijn indien ook de procesverantwoordelijke manager op deze wijze verantwoording aflegt over de kwaliteit van de beheersing in de processen waar hij of zij direct voor verantwoordelijk is. Bedrijfsbrede beheersing begint immers bij de operationele processen.

Grafiek 2.5.2.2 laat een uitsplitsing zien van de beursgenoteerde bedrijven naar de beurs(en) waaraan zij genoteerd zijn. Hieruit blijkt dat er geen grote verschillen bestaan tussen de genoemde beurzen voor wat betreft het gebruik van in-control verklaringen. Londen lijkt net iets boven de rest uit te steken, terwijl de categorie 'andere beurs' iets achter blijft.

Andere veel gebruikte termen voor In-control verklaring zijn 'Statement on Business Controls' en 'Letter of Representation', waarbij deze laatste veelal een verbreding betreft van de traditionele Letter of Representation die door het management wordt afgegeven bij de jaar- of kwartaalcijfers. Onderstaand kader bevat een voorbeeld van een interne In-control verklaring.

### 2.5.3 Externe rapportage over risicomanagement nog niet in lijn met code Tabaksblad

Informatie over de risico's die een organisatie loopt en de wijze waarop die risico's beheerd worden is relevant voor belanghebbers in die organisatie. Een aandeelhouder zal graag willen

Figuur 1.14 Voorbeeld In-control verklaring

**In-control statement**

Dear Sirs,

This letter is provided for the purpose of expressing the results of our assessment of the presence and operation of business controls in [ABC] during the year ending 31 December 20.. and in connection with the financial statements of [ABC] as per the same date.

We hereby declare that:

- We assume full responsibility for the implementation and maintenance of effective business controls in conformity with the principles as laid down in the [ABC] Business Controls Manual.
- To the best of our knowledge and belief, within our area of responsibility no serious shortcomings currently exist or have existed during the year under review with regard to the above business controls, except for ..... (to be specified in Annex 1), which implies that we have set clear policies and directives, that an organisation structure is in place with clearly defined lines of responsibility and delegation of authority, that adequate supervision is carried out and corrective actions are taken when and where necessary, and that an adequate accounting system is in place, including effective internal controls;
- Our above statement is evidenced by appropriate self assessments carried out throughout our organisation except for ..... (shortcomings in the carrying out of self assessments to be specified in Annex 2).
- Proper action plans have been established for remedying serious shortcomings in business controls / in the carrying out of self assessments (where applicable).

We confirm, to the best of our knowledge and belief, the following representations:

- We acknowledge our responsibility for the preparation and the fair presentation of the financial statements in accordance with [ABC] accounting principles.
- All assets inclusive of assets previously sold subject to a repurchase obligation, as well as assets provided as collateral to secure debts to third parties or contractual commitments not to encumber assets, have been properly recorded or disclosed in the balance sheet or in the notes thereto.
- All obligations and liabilities, including those resulting from breach of laws or regulations, both conditional and unconditional, and all securities provided to third parties have been properly reflected or disclosed in the balance sheet or in the notes thereto.
- Adequate provisions have been made in the balance sheet for all risks known to us arising from transactions entered into before 31 Dec.20.. or from existing situations at that date.
- There are no decisions to discontinue (parts of) group companies for which the effects have not been recorded in the financial statements.
- We have made available to you:
  - all financial records, contracts and related data.
  - all minutes of meetings of stockholders, supervisory board and board of management or summaries of actions of recent meetings for which minutes have not yet been prepared.
- There are no formal or informal compensating balance arrangements with any of our cash and investment accounts. Except as disclosed in the notes to the financial statements, there are no other agreements with lenders.
- All transactions in connection with financial instruments executed during the year, as well as the receivables and (contingent) liabilities outstanding at the balance sheet date, have been adequately recorded or disclosed in the financial statements.
- We have properly recorded or disclosed in the financial statements the capital stock repurchase options and agreements, and capital stock reserved for options, warrants, conversions and other requirements.
- During the period after the balance sheet date there have been no occurrences or developments which materially affect the view provided by the accounts.
  - either by having an impact on the valuation of assets and liabilities
  - or by being significant to the evaluation of the development of equity and results of the company.

Yours faithfully,

Management (ABC)

weten welke risico's genomen worden met zijn investering om te kunnen bepalen of dat wel in lijn ligt met het risico dat de aandeelhouder wenst te lopen. Maar ook maatschappelijke organisaties hebben graag inzicht in de risico's die publieke en private organisaties aangaan die gevolgen kunnen hebben voor de belangen van de maatschappij die door de betreffende organisaties worden behartigd. Dit zijn twee voorbeelden die laten zien dat van organisaties verlangd wordt dat zij inzicht geven in hun risicoprofiel en de wijze van risicobeheersing.

Corporate governance codes in diverse landen, inclusief de Nederlandse Corporate Governance code ('code Tabaksblat'), bevatten bepalingen die eisen stellen aan het extern rapporteren over risico's en risicomanagement door beursgenoteerde organisaties. Hieronder is de betreffende passage uit de code Tabaksblat afgebeeld.

**Figuur 1.15 Passage uit de code Tabaksblat over extern rapporteren over risicomanagement**

II.1.4 In het jaarverslag verklaart het bestuur dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn en geeft hij een duidelijke onderbouwing hiervan. Het bestuur rapporteert in het jaarverslag over de werking van het interne risicobeheersings- en controlesysteem in het boekjaar. Het bestuur geeft daarbij tevens aan welke eventuele significante wijzigingen zijn aangebracht, welke eventuele belangrijke verbeteringen zijn gepland en dat één en ander met de auditcommissie en de raad van commissarissen is besproken.

II.1.5 Het bestuur rapporteert in het jaarverslag over de gevoeligheid van de resultaten van de vennootschap ten aanzien van externe omstandigheden en variabelen.

De externe communicatie over risico's en risicomanagement vindt doorgaans plaats via een daarvoor bestemde paragraaf in het jaarverslag. In het onderzoek is gevraagd naar wat organi-

saties in hun jaarverslag rapporteren over dit onderwerp. Onderstaande tabel laat de resultaten zien. 40% van de organisaties rapporteert in het geheel niet over risicomanagement in hun jaarverslag. 48% rapporteert de belangrijkste risico's van de organisatie. Aan een rapportage over de werking van het risicomanagement systeem waagt slechts 18% van de organisaties zich. Nog minder organisaties rapporteren over aangebrachte significante wijzigingen (8%) en geplande wijzigingen (5%) in het risicomanagement systeem.

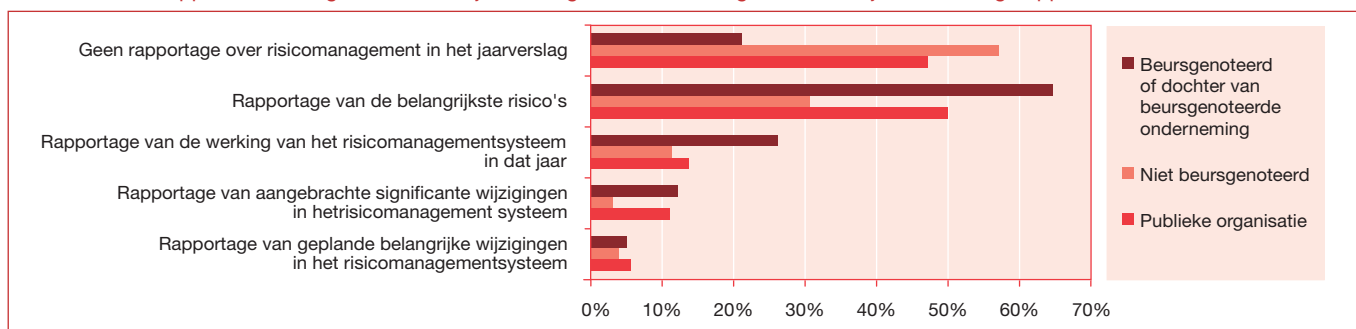
Een uitsplitsing naar wel of geen beursnotering of een publieke organisatie laat een iets ander beeld zien. Echter nog steeds 21% van de beursgenoteerde ondernemingen geeft aan niet in haar jaarverslag te rapporteren over risicomanagement. Reden hiervoor kan zijn dat ten tijde van het invullen van deze enquête het jaarverslag over 2004 nog niet uitgebracht was. Juist in dit jaarverslag zullen veel ondernemingen als gevolg van de code Tabaksblat voor het eerst hebben gerapporteerd over risicomanagement. Verder valt op dat publieke organisaties beduidend vaker (50%) in hun jaarverslag rapporteren over de risico's dan niet-beursgenoteerde ondernemingen (31%).

De code Tabaksblat vraagt tevens om een rapportage over het risicomanagement systeem ('interne risicobeheersings- en controlesysteem') en over aangebrachte en geplande wijzigingen daarin. Onderstaande tabel laat zien dat slechts een minderheid van de in Amsterdam aan de beurs genoteerde ondernemingen dit doen. Waarschijnlijk eveneens omdat het eerste jaarverslag van de onderneming sinds de komst van de code Tabaksblat nog moest verschijnen ten tijde van het invullen van deze enquête.

**Grafiek 2.5.3.1 Rapporteert uw organisatie in het jaarverslag over risicomanagement en zo ja wat wordt gerapporteerd?**



**Grafiek 2.5.3.2 Rapporteert uw organisatie in het jaarverslag over risicomanagement en zo ja wat wordt gerapporteerd?**



**Grafiek 2.5.3.3 Rapporteert uw organisatie in het jaarverslag over risicomanagement en zo ja wat wordt gerapporteerd? (alleen in Amsterdam aan de beurs genoteerde ondernemingen)**



# 2.6 Taken en verantwoordelijkheden

## 2.6.1 Taken en verantwoordelijkheden op verschillende wijzen vastgelegd

Voor de goede werking van een proces is het van belang dat de mensen die een rol spelen in het proces op de hoogte zijn van de activiteiten die zij dienen te verrichten en hoe deze passen binnen het grotere geheel. Dit geldt uiteraard ook voor het risicomanagement proces. Verschillende functionarissen binnen de organisatie hebben verschillende taken en verantwoordelijkheden binnen het risicomanagement proces.

Taken en verantwoordelijkheden worden binnen organisaties veelal vastgelegd. In het onderzoek is gevraagd of ook taken en verantwoordelijkheden ten aanzien van risicomanagement worden vastgelegd en op welke wijze. Onderstaande tabel laat zien dat binnen grote organisaties risicomanagement taken en verantwoordelijkheden doorgaans zijn vastgelegd (86%). Meestal zijn ze vastgelegd in risicomanagement beleid – en/of procedures (67%) of opgenomen in functiebeschrijvingen (55%). Uit de percentages is af te leiden dat de taken en verantwoordelijkheden in een deel van de organisaties op meerdere wijzen is vastgelegd.

Van de middelgrote organisaties heeft 62% op enigerlei wijze de risicomanagement taken en verantwoordelijkheden vastgelegd. Bij de kleinere organisaties is dat 43%.

Risicomanagement is zoals al eerder gesteld een continue proces. Om continue werking van het proces te waarborgen

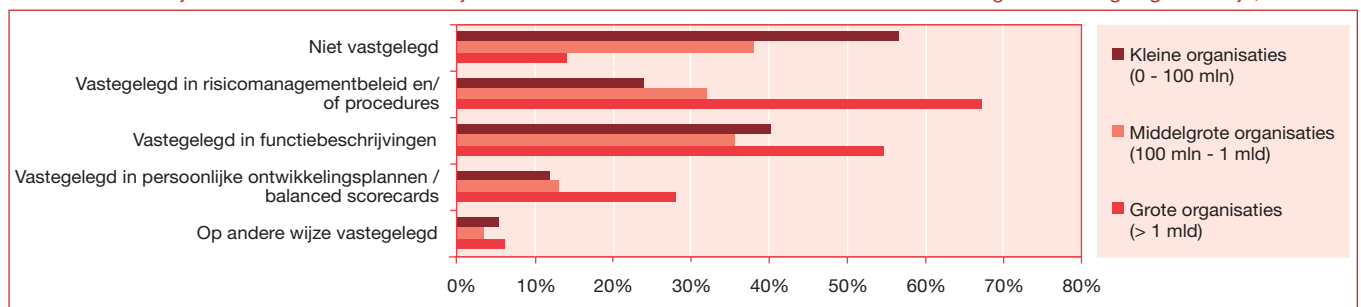
is het van belang dat betrokken functionarissen hun taken op structurele wijze blijven uitvoeren. Om dat te bereiken is het van belang dat zij daar ook op worden beoordeeld. Om deze beoordeling mogelijk te maken dienen de taken en verantwoordelijkheden te worden vastgelegd. Doorgaans zal vastlegging van taken en verantwoordelijkheden niet de eerste stap zijn bij de invoering van risicomanagement. Echter onze ervaring is dat, indien na verloop van tijd het risicomanagement project over dient te gaan een risicomanagement proces, het van belang is dat taken en verantwoordelijkheden worden vastgelegd en expliciet worden meegenomen bij de beoordeling van betrokken functionarissen.

## 2.6.2 Risicomanagement functie vaak belegd bij finance & control

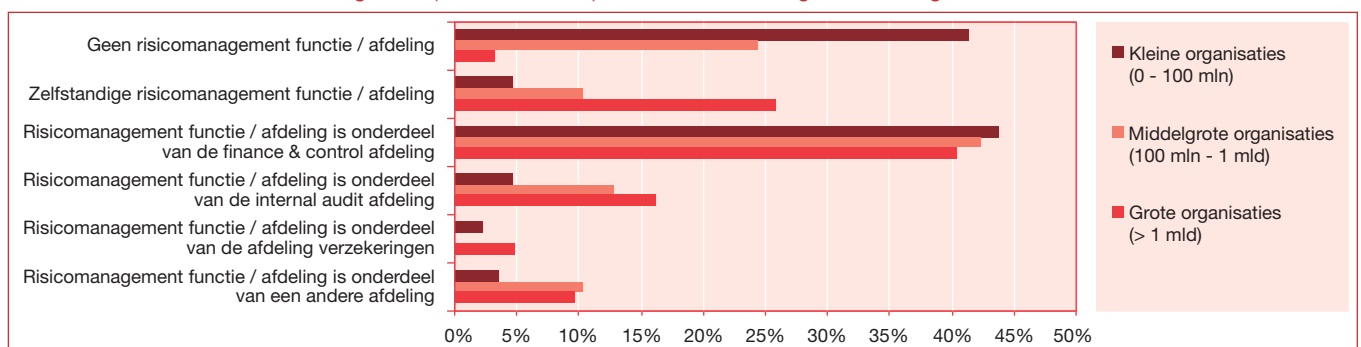
In organisaties waar bewust en expliciet risicomanagement wordt bedreven zullen de activiteiten die daarmee samenhangen door een bepaalde afdeling of functionaris moeten worden gecoördineerd. Die risicomanagement functie kan op verschillende plekken in een organisatie worden belegd. Ook kan er voor worden gekozen om een afzonderlijke risicomanagement afdeling in te richten.

Grafiek 2.6.2.1 laat zien hoe binnen de ondervraagde organisaties de risicomanagement functie is belegd. Van de grote organisaties geeft 97% aan op enigerlei wijze ergens in de organisatie een risicomanagement functie te hebben belegd. Bij middelgrote organisaties is dit 76% en bij kleine organisaties 59%.

Grafiek 2.6.1.1 “Zijn de taken en verantwoordelijkheden van functionarissen ten aanzien van risicomanagement vastgelegd en zo ja, hoe?”



Grafiek 2.6.2.1 Hoe is de risicomanagement (ondersteunende) functie binnen uw organisatie belegd?



## Kader 2.7

“Hoe is de risicomanagement (ondersteunende) functie binnen uw organisatie belegd?”

Bij kleine en middelgrote organisaties is de risicomanagement functie vooral belegd bij de finance & control afdeling (44% resp. 42%). Bij grote ondernemingen komt dit ook veel voor (40%), maar er zijn ook een flink aantal grote ondernemingen die een zelfstandige risicomanagement afdeling hebben ingericht (26%). Ook de internal audit afdeling blijkt in een aantal gevallen de risicomanagement functie op zich te nemen. Bij 16% van de grote ondernemingen is dit het geval.

Risicomanagement is een integrale verantwoordelijkheid van elke manager. In een ideaalsituatie zou dan ook geen risicomanagement ondersteunende functie nodig zijn. Deze ideaalsituatie zal echter niet snel worden bereikt, en daarom is het goed dat deze functie ergens in een organisatie expliciet wordt belegd. De meest geschikte plek hangt af van de specifieke organisatie. De omvang van het takenpakket zal afhangen van de grootte van de organisatie. De enquêteresultaten laten ook zien dat grote organisaties er soms voor kiezen een afdeling in te richten die zich alleen maar met risicomanagement bezig houdt. In kleinere organisaties zal dit veelal niet kostenefficiënt zijn en wordt deze functie gecombineerd met andere functies. In de tabel worden enkele veel voorkomende situaties genoemd, met elk zijn voor- en nadelen. Met name aan het beleggen van de risicomanagement functie bij de internal audit afdeling kleven belangrijke nadelen. Het is immers juist deze afdeling die de kwaliteit van het risicomanagement in de organisatie voortdurend tot object van onderzoek heeft. Indien de internal audit afdeling echter ook zelf een verantwoordelijkheid draagt voor de kwaliteit van het risicomanagement kan een belangenconflict ontstaan. Echter in voorkomende gevallen kan uit praktische overwegingen toch voor deze opzet worden gekozen. Daarbij is het dan zaak om het belangenconflict zo veel mogelijk voor te zijn door duidelijk aan te geven waar de verantwoordelijkheid van internal audit ophoudt en die van het management begint.

## 2.6.3 De controller speelt een belangrijke rol in de uitvoering van risicomanagement

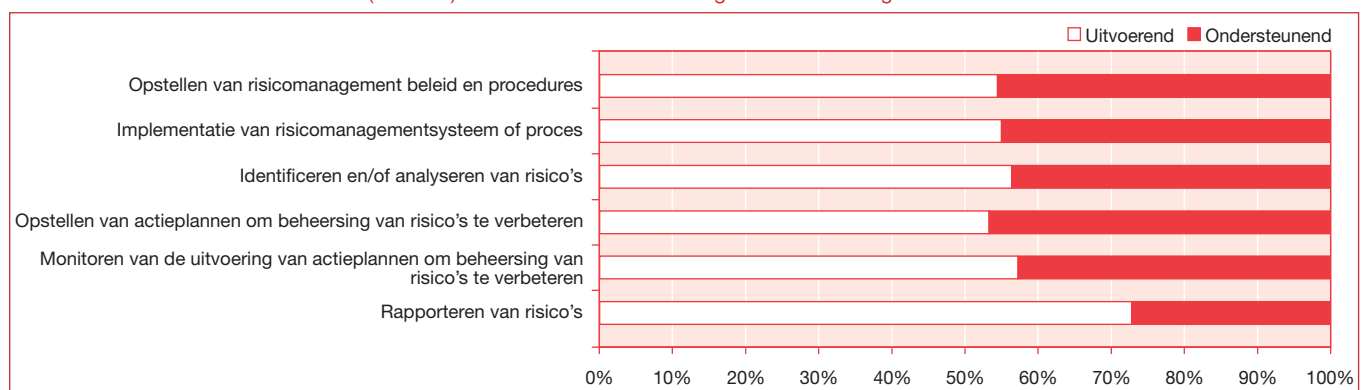
Het onderzoek is uitgevoerd onder leden van het Controllers Instituut. Het merendeel van de respondenten geeft dan ook aan werkzaam te zijn in de functie van (concern)controller. Onderstaande tabel laat zien welke rol deze (concern)controllers spelen in het risicomanagement van hun organisaties. Hieruit blijkt onder meer dat (concern)controllers vaak uitvoerend bezig zijn met risicomanagement. Dit strookt niet met de heersende opvatting dat risicomanagement een verantwoordelijkheid van het lijnmanagement is. Volgens deze gedachte zou de (concern)controller vooral een ondersteunende rol moeten vervullen. De praktijk laat hier echter zien dat het lijnmanagement doorgaans niet zelf het voortouw neemt als het om risicomanagement gaat.

## Kader 2.8

“Welke rol vervult u als (concern)controller in het risicomanagement van de organisatie?”

Het zal in de natuurlijke aard van veel controllers liggen om zelf risico's te benoemen, analyseren, kwantificeren en rapporteren. Des te groter zal de uitdaging zijn voor de controller om de komende jaren de uitvoering van risicomanagement activiteiten meer en meer naar de manager over te dragen. Toch moet het ons inziens die kant wel op. Om daadwerkelijk de voordelen van risicomanagement te kunnen benutten, zal het moeten worden gehanteerd als 'tool of management' en dus ook door het management moeten worden uitgevoerd als onderdeel van hun dagelijkse managementactiviteiten.

Grafiek 2.6.3.1 Welke rol vervult u als (concern)controller in het risicomanagement van de organisatie?



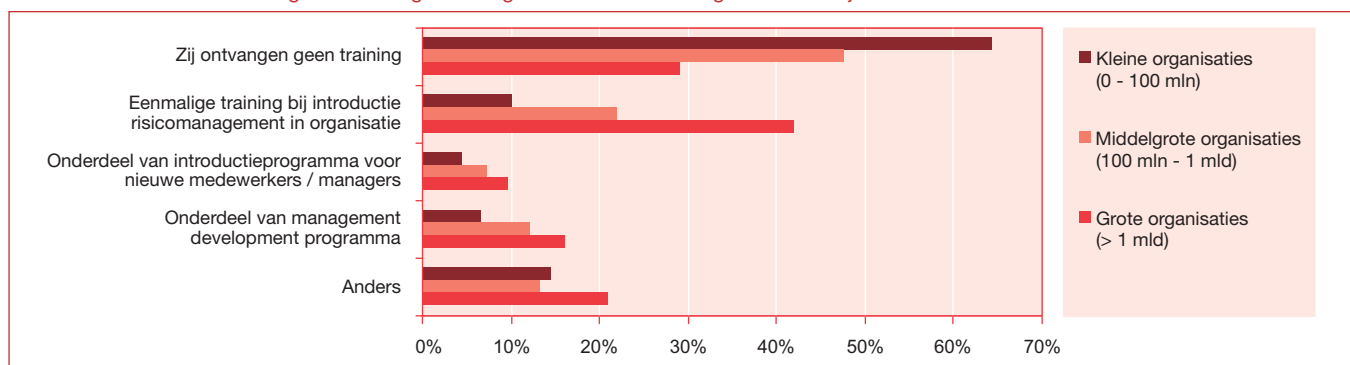
## 2.6.4 In veel organisatie worden managers getraind in risicomangement

Om effectief risicomangement te kunnen bedrijven zullen de managers die daar verantwoordelijk voor zijn over de benodigde kennis en competenties dienen te beschikken. Afhankelijk van de diepgang en verfijndheid van het risicomangement in de organisatie zal training nodig zijn voor het management. Onderstaande tabel laat zien dat slechts in een beperkt deel van de organisaties risicomangement training wordt gegeven. Bij grote organisaties is dat nog 71%, maar bij middelgrote (52%) en kleine organisaties (34%) is dat al een stuk minder.

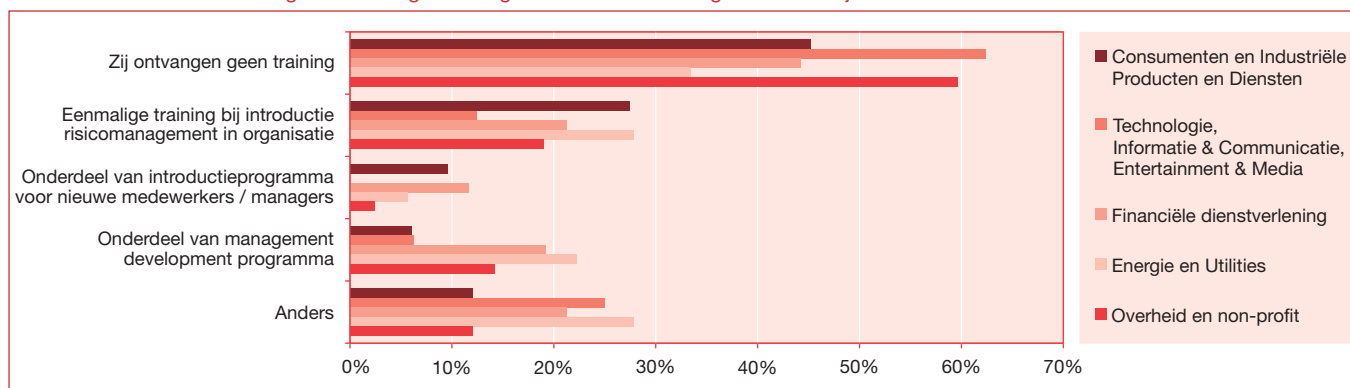
De meest voorkomende vorm van risicomangement training is een eenmalige training bij de introductie van risicomangement in de organisatie. Vooral binnen grote organisaties is dit het geval (42%). Bij een deel van de ondervraagde organisaties maakt risicomangement onderdeel uit van het introductieprogramma of van het management development programma.

Een uitsplitsing naar branche laat zien dat risicomangement training meer voorkomt in de financiële dienstverlening en de energie & utilities branche dan in andere branches. De overheid & non-profit en technologie, informatie & communicatie en entertainment branche blijven op dit punt enigszins achter.

Grafiek 2.6.4.1 Worden managers in uw organisatie getraind in risicomangement en zo ja hoe?



Grafiek 2.6.4.2 Worden managers in uw organisatie getraind in risicomangement en zo ja hoe?







# Deel III

## De visie van bestuurders op risicomanagement

In dit deel van het rapport volgt een weergave van vier gesprekken met bestuurders van vooraanstaande organisaties over het onderwerp risicomanagement. Zij geven hun mening over de ontwikkelingen op dit gebied en bieden inzicht in de wijze waarop er in hun organisaties mee wordt omgegaan. In tegenstelling tot deel II van dit rapport – waar het ging om het geaggregeerd weergeven van op gestructureerde wijze verzamelde inzichten en informatie – bieden de interviews met de bestuurders ruimte voor nuance en persoonlijke visies. Waardevolle informatie voor éénieder die zich met risicomanagement bezighoudt.

# 3.1 Robert-Jan van de Kraats

## Chief Financial Officer, Randstad Holding

Robert-Jan van de Kraats is Chief Financial Officer van Randstad Holding N.V. (Randstad). Randstad is één van de grootste uitzendondernemingen in de wereld en is marktleider in Nederland, België, Duitsland, Polen en het zuidoosten van de Verenigde Staten. Bijna tweederde van de omzet wordt buiten Nederland gerealiseerd. Naast Chief Financial Officer is de heer Van de Kraats binnen de Raad van Bestuur tevens verantwoordelijk voor Informatietechnologie, Investor Relations en de werkmaatschappij Yacht. Het risicomanagement binnen Randstad is onder zijn hoede vorm gegeven. De heer Van de Kraats volgt actief het publieke debat over corporate governance en risicomanagement en laat waar nodig zijn stem horen, zo ook hier.

**In recente corporate governance codes in diverse landen (o.m. Sarbanes-Oxley en de code Tabaksblat) worden eisen gesteld aan de wijze waarop beursgenoteerde ondernemingen hun interne risicobeheersings- en controle-systemen dienen in te richten. Wat is uw gevoel hierbij?**

‘Aandacht voor risicomanagement is in beginsel een goede zaak. Ik vraag mij echter sterk af of we de goede kant op gaan als we dit soort zaken in regels willen verankeren. Ik denk dat het veel beter zou zijn indien ondernemingen meer vrijheid hebben om op eigen wijze vorm te geven aan de wijze waarop zij hun risico’s willen beheersen. Het opbouwen van een goed werkend systeem voor risicobeheersing is iets wat tijd kost en sterk afhankelijk is van zachte factoren als cultuur en leiderschap. Het zou mijns inziens de kwaliteit ten goede komen indien de focus wat minder komt te liggen op het voldoen aan regels. Dat veroorzaakt slechts een check-the-box-mentaliteit. Ik ben kortom voor minder in plaats van meer regels. De druk om werk te maken van risicobeheersing zou uit een andere hoek moeten komen, namelijk van de belegger. Het verbaast mij telkens weer hoe weinig beleggers geïnteresseerd zijn in dit onderwerp. Terwijl adequaat risicomanagement mijns inziens zeer relevant is voor de waarde van een onderneming. De aandacht moet daarom veel meer uitgaan naar het opvoeden van de belegger. Bedrijven zouden zich ook door middel van hun risicomanagement strategie, implementatie en track record naar beleggers toe moeten kunnen differentiëren. Nu wordt dat nog nauwelijks geapprecieerd maar in de toekomst zou door middel van het bewust maken van de belegger er veel meer vanzelfsprekendheid kunnen ontstaan met betrekking tot adequaat risicomanagement. Een in risicomanagement geïnteresseerde belegger krijgt meer voor elkaar dan regels. Hier ligt nog een schone taak te wachten, waar wat mij betreft alle partijen in de corporate governance arena een rol in dienen te spelen.’

**Wat verwacht u in dat kader van uw accountant?**

‘Accountancy firma’s spinnen natuurlijk garen bij de toenemende check-the-box-mentaliteit. Echter vanuit hun verantwoordelijkheid zou het goed zijn als vanuit die hoek ook eens geluiden te horen zijn die twijfels zetten bij deze

ontwikkeling. Ook accountancy firma’s hebben een rol te spelen bij het opvoeden van de belegger. Ik denk ook niet dat accountants een oordeel zouden moeten vellen over de kwaliteit van het risicomanagement in een onderneming. Zij zijn daar denk ik ook niet goed toe in staat. Die rol zou ik eerder weggelegd zien voor rating agencies. Zij zijn gewend om met wat bredere blik naar een onderneming te kijken en daar kan ook het risicomanagement in mee worden genomen. De kwaliteit van het risicomanagement komt dan nadrukkelijk tot uiting in de afgegeven rating. Overigens vraag ik me wel af of rating agencies dan nog op dezelfde wijze te werk kunnen blijven gaan. Het is niet onvoorstelbaar dat zodra deze publieke druk op hun schouders komt te liggen ook zij de materie meer vanuit een juridische invalshoek zullen benaderen.’



**‘Niet meer, maar minder regels’**

R.J. van de Kraats  
Chief Financial Officer,  
Randstad Holding

**Heeft de code Tabaksblat bijgedragen aan de aandacht die het onderwerp risicomanagement krijgt aan de bestuurstafel van Randstad?**

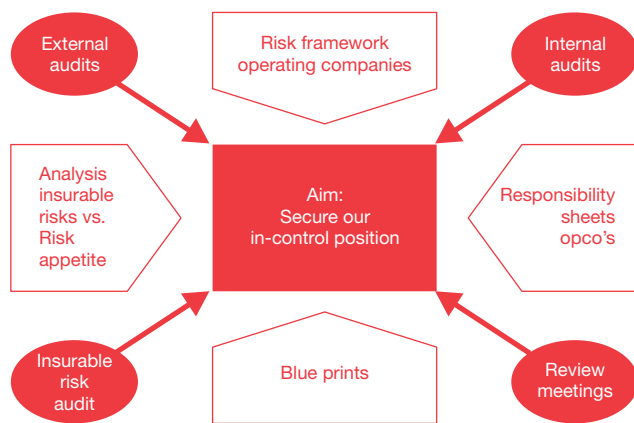
‘Al enkele jaren geleden zijn we binnen Randstad begonnen met het opbouwen van een risicomanagement systeem. Dat was ruim voor Tabaksblat. Wel hadden we toen natuurlijk al de 40 aanbevelingen van de commissie Peters, waar ook iets soortgelijks in stond. Echter het verschijnen van de code Tabaksblat heeft er wel voor gezorgd dat het onderwerp nog nadrukkelijker op de agenda is komen te staan. Wij onderschrijven ook het belang van de code. Het is goed dat er gestreefd wordt naar meer verantwoording en transparantie. Echter, over een aantal bepalingen uit de code ben ik minder enthousiast. Een voorbeeld hiervan is het maximum van één jaarsalaris dat wordt gesteld aan de vertrekpremie van

bestuurders. Gevolg hiervan is dat bestuurders minder rugdekking hebben bij het verdedigen van lastige issues richting de aandeelhouders. Bestuurders zullen eerder geneigd zijn mee te gaan in de, vaak meer op de korte termijn gerichte visie van de aandeelhouders. Ik vrees dat de code Tabaksblat op dit punt averechts zal werken.'

### Hoe ziet het risicomanagement systeem er binnen Randstad nu uit? Kunt u een korte beschrijving geven?

'Iets wat wij niet wilden was een stevig theoretisch verhaal de organisatie in duwen. Wij hebben op pragmatische wijze een benadering ontwikkeld die nauw aansluit op de bedrijfsstrategie en de operations. Risicomanagement is binnen Randstad verankerd in de basisstrategie. Één van de vier kernelementen van de basisstrategie is excellent execution. Als onderdeel daarvan is het Randstad Risk Management Framework ontwikkeld.

Figuur: Randstad Risk Management Framework



Dit framework kent vier hoofdcomponenten. De eerste is het risk framework voor de operating companies. Daarbij gaat het erom dat de afzonderlijke Randstad bedrijven op systematische wijze hun risico's in kaart hebben, de werking van de key controls wordt vastgesteld en dat hierover gerapporteerd wordt aan de holding. Het risk framework onderscheidt vijf risicogebieden: business risks (onderverdeeld naar strategisch en operationeel), legal risks, organizational risks, financial risks en reputation risks. De tweede hoofdcomponent van het Randstad Risk Management Framework is de responsibility sheet die door de directies van operating companies elk kwartaal ingevuld dient te worden. De responsibility sheet maakt eenduidig wat de kernverantwoordelijkheden van de lokale general manager zijn en hoe die op een verantwoorde wijze gedragen dienen te worden. Het derde hoofdcomponent zijn de blue prints. Dit zijn blauwdrukken van best practice processen, inclusief de beheersmaatregelen zoals wij vinden dat die aanwezig zouden moeten zijn binnen alle randstad bedrijven. De vierde hoofdcomponent is een periodieke analyse van de verzekerbare risico's om vast te stellen of die risico's getolereerd kunnen worden of dienen te worden verzekerd. Voor alle vier de hoofdcomponenten geldt dat actieve monitoring plaatsvindt.'

### Waren naar aanleiding van de code Tabaksblat wijzigingen of verbeteringen nodig in het risicomanagement systeem van Randstad?

'Wij zijn enige tijd geleden een project gestart waarin we per proces de key controls hebben gedefinieerd. De operating companies dienen deze controls in-place te hebben. We zijn momenteel druk doende de werking van de key controls systematisch te testen. De code Tabaksblat was één van de drijfveren voor deze toevoeging aan het bestaande risk management framework. Overigens bestaan er ook nog onduidelijkheden. Zo is het mij bijvoorbeeld nog niet duidelijk in hoeverre de werking van controls op lokaal niveau ook feitelijk door de holding nog eens moet worden geconstateerd. Wij doen dit momenteel voor de meest relevante key controls.

### Hoe wordt risicomanagement beleefd in de organisatie? Brengt het toegevoegde waarde?

'Toen wij een aantal jaren het onderwerp risicomanagement voor het eerst expliciet aan de orde was tijdens een bestuursvergadering plaatste één van mijn medebestuurders de opmerking dat hij elke dag al aan risicomanagement deed. En dat is natuurlijk een terechte opmerking. De kern is dat het bewust omgaan met risico in de aderen van het bedrijf moet zitten. Dat red je niet met alleen mooie frameworks en manuals. In de afgelopen jaren is er ook een bepaalde wijze van communiceren over risico's ontstaan. Begrippen als slendering risk en torpedo risk zullen een buitenstaander weinig zeggen. Binnen Randstad weet dan iedereen waar het over gaat. Althans, iedereen die het zou moeten weten. En als je nu aan een manager binnen Randstad vraagt of hij meerwaarde van risicomanagement ervaart dan is het antwoord overwegend positief. Al blijf ik erbij dat de echte toegevoegde waarde pas komt als ook de belegger het risicomanagement en de transparantie daarover weet te waarderen. Zolang de belegger het in zijn waardering niet mee laat wegen dat een onderneming zich op dit punt positief onderscheidt van bijvoorbeeld concurrenten uit Azië – waar men geen seconde over dit soort zaken na hoeft te denken – blijft het in zekere zin juist een ondermijning van de concurrentiepositie van met name westerse bedrijven.'

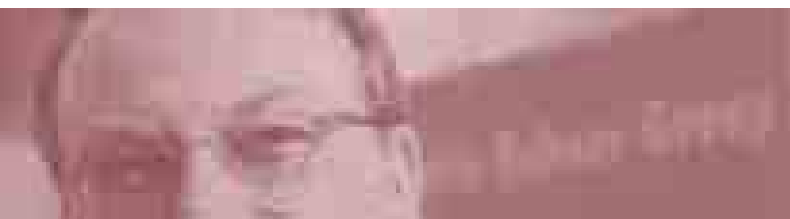
### In het jaarverslag over 2004 stelt de Raad van Bestuur van Randstad dat 'zij van mening is dat het interne risicobeheersings- en controlesysteem een redelijke mate van zekerheid geeft dat de (financiële) informatie dat uit deze systemen voortkomt betrouwbaar is en voldoet aan van toepassing zijnde wet- en regelgeving'. Waarom heeft u gekozen voor deze formulering?

'Wij wilden over 2004 door middel van dit statement laten zien dat we goed op weg zijn naar een meer uitgebreide verklaring over 2005. Verder was onze verwachting dat ook andere ondernemingen voorshands, in lijn met de Sarbanes-Oxley vereisten, deze focus zouden kiezen. Bij de bredere formulering voor 2005 zal het nog een uitdaging worden om hier te komen tot aansprekende en niet al te juridisch gedreven teksten. Gezien de ontwikkelingen ben ik op dit vlak niet hoopvol gestemd.'

## 3.2 Chris Spanjaard

### Hoofddirecteur, Informatie Beheer Groep

Chris Spanjaard is Hoofddirecteur van de Informatie Beheer Groep. De Informatie Beheer Groep (IB-Groep) voert als zelfstandig bestuursorgaan in opdracht van het ministerie van Onderwijs, Cultuur en Wetenschap een aantal wetten en -regelingen uit. De kerntaken van de IB-Groep zijn verstrekking van financieringen, informatiebeheer en het organiseren van examens. De heer Spanjaard trad in 2001 aan als Hoofddirecteur en heeft gedurende de afgelopen jaren onder meer nadruk gelegd op het verbeteren van de bedrijfsvoering. In dit interview vertelt hij samen met de heer Jan Jakob Boersma, Concerncontrolller bij de IB-groep, over deze ontwikkelingen en over de rol van risicomanagement in de bedrijfsvoering van de IB-groep.



**Risicomanagement speelt al enige tijd een rol binnen de bedrijfsvoering van de IB-groep. Wat waren aanleidingen om aan risicomanagement te gaan doen?**

‘Toen ik in 2001 aantrad als Hoofddirecteur was het verbeteren van de kwaliteit van de bedrijfsvoering een belangrijk speerpunt. De IB-groep kwam uit een periode waarin de prioriteiten wat anders lagen, met als gevolg dat de bedrijfsvoering wat minder de aandacht had gehad. We begonnen destijds met het optuigen van elementaire bouwstenen voor een goede bedrijfsvoering. Denk hierbij aan de inrichting van de AO/IC, verbeteren van de planning & control en het optuigen van een Internal Audit afdeling. Toen deze zaken vorm hadden gekregen wilden we verder gaan op de ingezette weg. We wilden (en willen nog steeds) de beste uitvoeringsorganisatie zijn. Risicomanagement gaf ons de mogelijkheid om gefundeerde keuze te maken bij het verder verbeteren van de bedrijfsvoering. Het was en is voor ons een ideaal instrument om focus aan te brengen. Ontwikkelingen in de bedrijfsvoering worden uiteraard ook besproken met de Raad van Toezicht van de IB-groep en binnen de Raad is de houding ten opzicht van risicomanagement ook positief. Mede gebaseerd op ervaringen elders. Ook dit heeft bijgedragen aan de keuze om een gestructureerd proces van identificeren, analyseren en managen van risico’s in de organisatie in te voeren.’

**Hoe heeft vervolgens het risicomanagement binnen de IB-groep vorm gekregen?**

‘In 2003 hebben we voor het eerst een risicoanalyse op strategisch niveau uitgevoerd. We zijn hierbij ondersteund door externen, hetgeen zeker voor zo’n eerste keer nuttig is. Het toen opgebouwde risicoprofiel heeft daarna nog wel wat bewerkingsslagen gekend. Het moet toch uiteindelijk toch ons

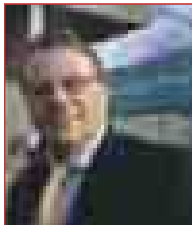
eigen verhaal worden en ook zo aanvoelen. In navolging van de strategische risicoanalyse hebben ook de directies een risicoanalyse uitgevoerd. De concerncontrolller is hier nauw bij betrokken. Inmiddels zijn we zover dat het rapporteren over risico’s een vast onderdeel is geworden van onze planning- en controlcyclus. De risico’s worden als het ware uit de organisatie ‘opgehaald’, waarmee ook op IB-groep niveau inzicht ontstaat in waar de prioriteiten in de organisatie dienen te liggen.’

**Hoe verhoudt dit zich tot de mededeling bedrijfsvoering in uw jaarverslag?**

‘Hetgeen we doen aan risicomanagement is één van de gronden waarop de mededeling bedrijfsvoering is gebaseerd. Wij gebruiken onder meer COSO en INK als referentie voor de beheersing van de bedrijfsvoering. De reikwijdte van de mededeling over de bedrijfsvoering beslaat alle elementen van de gehanteerde referentiemodellen. Onze externe accountant controleert de mededeling bedrijfsvoering aan de hand van een normatief raamwerk dat is gebaseerd op dezelfde referentiemodellen. Dus onder meer op COSO en het INK-model. Het raamwerk is voorzien van een groeimodel bestaande uit vijf fasen. Voor elk van de elementen uit het raamwerk wordt vastgesteld in welke fase de bedrijfsvoering van de IB-groep zich bevindt. Onze ervaringen met deze aanpak zijn erg positief. Het biedt een handvat om te communiceren over beheersing in de bedrijfsvoering en het maakt verbeteringen daarin ook inzichtelijk.’

**De IB-groep is één van de leden van de Handvestgroep Publiek Verantwoorden. Wat betekent dit voor het risicomanagement binnen de IB-groep?**

‘De Handvestgroep wordt gevormd door een tiental zelfstandige bestuursorganen (ZBO’s) die het Handvest Publieke Verantwoording hebben ondertekend. Met de ondertekening van het handvest geven de deelnemende organisaties aan dat ze zich, naast het afleggen van verantwoording aan de minister, ook willen verantwoorden aan klanten en samenleving over hun handelen en de kwaliteit van dienstverlening. De Handvestgroep heeft in juni 2004 de ‘code goed bestuur uitvoeringsorganisaties’ gepubliceerd. In de code goed bestuur staat – analoog aan de code Tabaksblat – dat de



## 'In de driver seat in plaats van te worden geleefd'

Chr. G. Spanjaard  
Hoofddirecteur, Informatie Beheer Groep

ZBO over een op de ZBO toegesneden intern risicobeheersings- en controlesysteem dient te beschikken. Tevens dient het bestuur van de ZBO in haar jaarverslag te verklaren in welke mate het interne risicobeheersings- en controlesysteem adequaat en effectief is. Voor de IB-groep had dit niet direct grote gevolgen. Wij waren immers al enige tijd met risicomangement bezig en dat paste uitstekend in de gedachte van de code goed bestuur. Dit geldt echter lang niet voor alle ZBO's. Wij hebben de indruk dat wij als IB-groep hierin redelijk voorop lopen. Dat merken we ook omdat we met enige regelmaat door collega ZBO's worden uitgenodigd om te komen vertellen hoe wij een en ander hebben aangepakt en ingericht.'

### Hoe komt het dat de IB-groep hierin voorop loopt?

'Ten eerste geldt hier de wet van de remmende voorsprong. Zoals we vertelden zijn we zo'n vier jaar geleden begonnen met het professionaliseren van de bedrijfsvoering. Dit gaf het goede momentum om vervolgens ook meer gevorderde instrumenten te introduceren. Een tweede reden is dat wij momenteel over een goede governance structuur beschikken waarin aandacht wordt geschonken aan dit soort zaken. Ook de samenstelling van de Raad van Toezicht speelt hier een rol. Ons inziens is het van groot belang dat in een Raad ook deskundigheid op het gebied van bedrijfsvoering aanwezig is. Ten derde komt de kwaliteit van de bedrijfsvoering expliciet aan bod in het prestatiecontract met de minister, waardoor continue aandacht voor het onderwerp is gewaarborgd.'

### Waarom zit naar uw idee de meerwaarde van risicomangement?

'Het belangrijkste is dat het je helpt om in de drivers seat te komen in plaats van te worden geleefd, simpelweg omdat je zaken eerder ziet aankomen en wordt gedwongen om daar iets mee te doen. Overigens zien wij risicomangement in beginsel gewoon als een orderingsinstrument zoals er vele andere zijn. Het helpt om de complexe werkelijkheid te ordenen en vervolgens op een gestructureerde wijze verbeteringen aan te brengen. Daarnaast merken wij vooral bij de risicoanalyses op lager niveau in de organisatie dat het een verfrissend werking heeft. Het dwingt de betrokkenen om van

buiten naar binnen te denken door de ogen van bijvoorbeeld klanten of de samenleving. Het geeft daardoor een goed inzicht in de eigen houding en gedrag. Wat overigens ook kan gebeuren is dat je door het openlijk rapporteren over risico's meer controle over je afroept. Dit geldt zeker in een bestuurlijke omgeving als die waar wij in opereren.

### Merkt u dat ook intern, dat men moeite heeft met openheid omdat met bang is voor te veel bemoeienis?

'Jazeker. Dat heeft in het begin wel de nodige moeite gekost. Sinds enige tijd verlangen wij van de managers van alle eenheden dat ze bij de maandrapportage een betrouwbaarheidsverklaring afgeven waarin zij verantwoordelijkheid nemen voor de kwaliteit van de bedrijfsvoering. Hierdoor worden ze tot openheid gedwongen over zaken die niet op orde zijn. Het benadrukt bovendien de persoonlijke verantwoordelijkheid. De betrouwbaarheidsverklaring heeft wel tot de nodige discussies geleid. Ook in gevallen waarin achteraf kon worden geconstateerd dat de openheid onvoldoende was, was er reden tot een goed gesprek. Wij ervaren die discussie overigens als iets positiefs. Mensen gaan nadenken over het onderwerp en hun eigen verantwoordelijkheden daarin.'

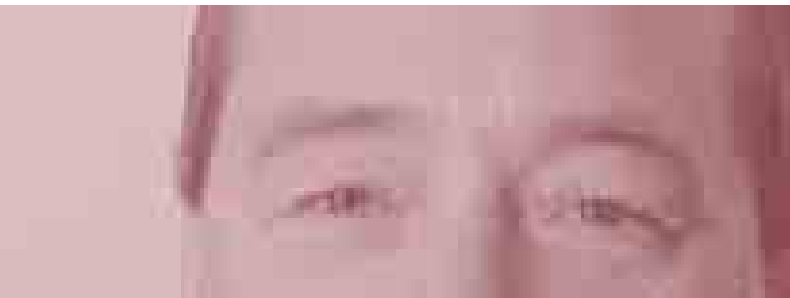
### Welke adviezen zou u collega bestuurders mee willen geven als zij risicomangement in willen voeren?

'Wat wij iedereen aan zouden willen raden is aan te haken bij natuurlijke steunpunten. Door het te koppelen aan zaken die er reeds zijn, voorkom je dat mensen het idee hebben dat ze iets geheel nieuws over zich uitgestort krijgen. Ook is het altijd goed om te rade te gaan bij mensen die reeds ervaringen hebben opgedaan. Dat kunnen externe adviseurs zijn, maar ook collega's bij andere organisaties. Ten slotte is het van belang om niet alles direct in een voorschrift te zetten. Beter is mensen eerst zelf de voordelen te laten ervaren door het gewoon te gaan doen'.

## 3.3 Frank Sonnemans

### Chief Financial Officer, Provimi

Frank Sonnemans is Chief Financial Officer van Provimi Holding B.V. (Provimi). Provimi is één van de grootste producenten van diervoeding ter wereld. Het bedrijf telt circa 8000 werknemers en is met ruim 100 productielocaties vertegenwoordigd in circa 30 landen. Provimi is genoteerd aan de Euronext in Parijs. Het hoofdkantoor is gevestigd in Rotterdam. Als Chief Financial Officer is de heer Sonnemans actief betrokken bij het risicomanagement binnen de onderneming. In dit interview vertelt hij onder meer over de effecten die de Franse beursnotering heeft op de wijze waarop Provimi met risicomanagement omgaat.



**Provimi is in Parijs aan de beurs genoteerd en dient daarmee te voldoen aan de 'Loi sur la Sécurité Financière' (LSF). Hoe ervaart u deze verplichting?**

'De verplichtingen samenhangend met de LSF uiten zich met name in het publiceren van een gedetailleerd Presidents Report in het jaarverslag met onder andere de interne controle procedures en de daarbij horende verklaring van de externe accountant. Inhoudelijk betekent dit dat Provimi moet kunnen aantonen dat zij in-control is.'

'De LSF trad in werking in oktober 2003, met terugwerkende kracht vanaf 1 januari 2003. Dat betekende dat er slechts twee maanden resteerden om aan de gestelde eisen te voldoen. We hebben in die twee maanden de stappen gezet die ons inziens minimaal nodig waren om aan de LSF te kunnen voldoen. Achteraf bleek dat hetgeen wij als minimaal beschouwden, meer was dan vrijwel alle andere bedrijven hadden gedaan. We bleken met ons President's Report ineens tot de beste jongetjes van de klas te behoren. Dit werd ook ingegeven door het feit dat de LSF ondernemingen in grote mate vrij laat ten aanzien van de wijze waarop zij aantoonbaar in-control wil zijn. Veel bedrijven hebben in afwachting van nadere richtlijnen geen stappen ondernomen. In reactie op deze ontwikkeling heeft ook Provimi een pas op de plaats gemaakt. Onze verklaring in het Presidents Report in het jaarverslag over 2004 is vrijwel hetzelfde als over 2003.'

**Hoe zag de initiële reactie op de LSF eruit? Welke stappen zijn op het gebied van risicomanagement gezet?**

'We hebben eind 2003 een risk assessment uitgevoerd om de belangrijkste business risks voor de organisatie vast te stellen in termen van impact en likelihood of occurrence. Op basis van deze assessment zijn de belangrijkste acht risico's voor Provimi Group beschreven en gedocumenteerd. Bepaald is welke van deze acht risico's door Provimi intern te beheersen zijn. Daarnaast werd voor risico's van buitenaf bepaald of voldoende is gedaan om mogelijke negatieve effecten te minimaliseren. In 2004 zijn de risico's opnieuw geëvalueerd. Voor de risico's die zijn te beheersen zijn door Internal Audit test templates geschreven (in samenwerking

met de externe accountant). Op basis van deze templates zijn in 2004 bij bedrijven in de groep die 50% van de omzet genereren audits uitgevoerd. Op basis van de audits zijn remedial action plans geformuleerd. De meeste recente ontwikkeling aangaande het risk management systeem van Provimi is dat we begin dit jaar een Control Self Assessment (CSA) hebben uitgevoerd bij 90% van de profit centers van de groep. Op deze wijze zijn de belangrijkste risico's op profit center niveau geïdentificeerd. Gebaseerd op de uitkomsten van de CSA zijn de key controls voor de organisatie verder gedefinieerd. De profit centers zullen aandacht moeten schenken aan de uitkomsten van de CSA en daar waar nodig verbeteringen in de interne beheersing moeten aanbrengen.'

#### Hoe is nu de houding ten aanzien van risicomanagement binnen Provimi? Wordt het als nuttig ervaren?

'Genoemde ontwikkelingen hebben zeker bijgedragen aan een verhoogd bewustzijn van risico's en de beheersing daarvan. Het grote verschil is ook dat we alles nog eens netjes volgens een vast stramien hebben opgeschreven en besproken. De beheersing is aantoonbaar gemaakt. We hebben zelf meer zekerheid gekregen over de mate waarin we in-control zijn en die (redelijke mate van) zekerheid kunnen we nu ook beter verschaffen aan de buitenwereld. Daar zou dan ook de toegevoegde waarde vandaan moeten komen. Er zal bij de belegger waardering moeten ontstaan voor het feit dat we de zaken goed op orde hebben. Hetzelfde zie je op het terrein van kwaliteitsbeheersing. De eisen die Provimi inzake kwaliteit stelt aan haar bedrijven zijn hoog. In sommige landen betekent dit dat we veel meer doen dan de concurrentie. Echter klanten zijn bereid om de hogere prijzen die hier het gevolg van zijn te betalen. Zij weten de kwaliteitsbeheersing van Provimi op waarde te schatten.'

'Wat betreft daadwerkelijke verbetering van de interne beheersing is het met name de Control Self Assessment die als waardevol wordt beleefd, met name ook door de general managers in de landen. Aan de hand van dit instrument worden verbeterpunten in de risicobeheersing van de profit centers opgespoord en zodra de verbeteracties zijn uitgevoerd zal er ook daadwerkelijk sprake zijn van een verbeterde interne beheersing.'

#### U noemde kwaliteitsbeheersing. Op dit terrein is binnen een bedrijf als Provimi waarschijnlijk al zeer veel ingericht. Hoe verbind u dit met de meer algemene risicomanagement benadering?

'Één van de top acht risico's uit het risk assessment was het risico van product contamination. Dit risico heeft uiteraard al jaren de aandacht van het management, zowel lokaal als corporate, en is voortdurend onderwerp van interne kwaliteitscontrole en audits. Alle Provimi werkmaatschappijen dienen te voldoen aan GMP (good manufacturing practice) en HACCP (hazard analysis and critical control point). Aan de wijze waarop dit risico wordt beheerst is geen verandering aangebracht. Wel hebben we dit in het kader van risicomanagement nog eens netjes opgeschreven.'

#### Hoe zullen de ontwikkelingen inzake de LSF verder gaan verlopen? Wat komt er nog op u af?

'De verwachting is nog steeds dat er nadere richtlijnen zullen komen waarin wat meer concreet wordt beschreven aan welke normen voldaan moet worden. Welke kant het opgaat is moeilijk in te schatten. Al enige tijd geleden heeft de verantwoordelijke Franse minister in een brief verklaard dat de eisen ten aanzien van het testwerk minder stringent zouden kunnen. Aan de andere kant heeft de Franse beurstoezichthouder, de Autorité des Marchés Financiers (AMF), laten weten dat zij toe willen naar een uitspraak over de werking van het risicobeheersings- en controlesysteem.' Duidelijkheid is belangrijk, mits de richtlijnen werkbaar en zinvol zijn en daadwerkelijk bijdragen tot een betere risicobeheersing. Onze voorkeur gaat er naar uit om met enige vrijheid het risicomanagement in de organisatie verder te ontwikkelen.'



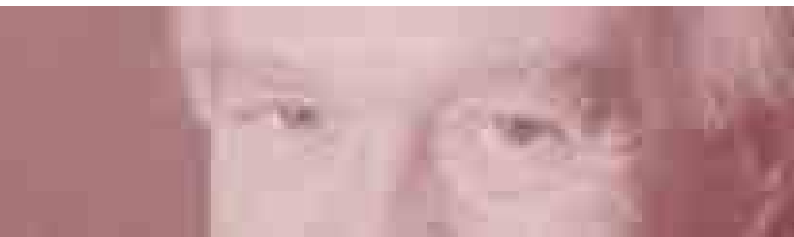
'We bleken ineens tot de beste jongetjes van de klas te behoren'

F. Sonnemans  
Chief Financial Officer, Provimi

## 3.4 Hans Leenaars

### lid Raad van Bestuur, Bank Nederlandse Gemeenten

Hans Leenaars is lid van de Raad van Bestuur van de N.V. Bank Nederlandse Gemeenten (BNG). De BNG is de bank van en voor overheden, zoals gemeenten, provincies, gemeenschappelijke regelingen, politieregio's en met overheden verbonden instellingen en bedrijven op het terrein van volkshuisvesting, openbaar nut, onderwijs en gezondheidszorg. Met gespecialiseerde dienstverlening draagt de BNG bij aan zo laag mogelijke kosten van maatschappelijke voorzieningen voor de burger. De heer Leenaars is binnen de Raad van Bestuur verantwoordelijk voor Treasury, Capital Markets, Juridische Zaken en de Interne Accountantsdienst. Tevens is hij voorzitter van het kredietcomité van de BNG. Vanuit zijn verantwoordelijkheidsgebieden is de heer Leenaars nauw betrokken bij de ontwikkelingen op het terrein van risicomanagement, zowel binnen als buiten de bank. Ook zijn achtergrond van Register Accountant maakt dat de heer Leenaars bij het onderwerp betrokken is en een duidelijke visie op het onderwerp heeft.



De financiële dienstverlening heeft als geen andere branche te maken met een opeenstapeling van eisen van overheden en toezichthouders aangaande de inrichting van risicobeheersings- en controlesystemen (denk aan Bazel II, ROB, nFTK, Sovency II, naast algemene corporate governance codes als de code Tabaksblat en de Amerikaanse Sarbanes-Oxley wetgeving). Hoe ervaart u deze ontwikkeling?

‘Laat ik beginnen met te zeggen de toenemende integratie van het risicodenken in de wijze waarop organisaties worden bestuurd mijns inziens een goede ontwikkeling is. Het expliciet maken van de risk/reward trade-off bij dagelijkse managementbeslissingen draagt bij aan een betere besluitvorming. Risk-adjusted return concepten zijn zinvolle maatstaven om naar rendementen te kijken. Aan de andere kant ervaar ik de eisen vanuit de diverse wet- en regelgevingen ook zo nu en dan als een last. Natuurlijk is het goed dat ondernemingen naar de buitenwereld transparant zijn over de wijze waarop de onderneming wordt bestuurd en de risico's die daarbij worden gelopen. Maar de inspanningen die dat vergt van de organisatie zijn hoog, zeker in de financiële sector, en niet altijd is duidelijk hoe de organisatie ervan profiteert. Het gevoel van een last en het moeten steekt dan al snel de kop op. We moeten overigens ook niet vergeten dat risicomanagement relatief nieuw is. Tien jaar geleden bestond het als zodanig nauwelijks in Nederland. Het is dus ook niet zo vreemd dat we de juiste modus nog niet hebben gevonden. Maar dat risicomanagement toegevoegde waarde heeft staat voor mij buiten kijf. Goed risicomanagement stelt je in staat om risico's en rendementen beter op elkaar af te stemmen. Daar kan toch niemand tegen zijn.’

### Op welke wijze heeft de BNG gereageerd op de van toepassing zijnde wet- en regelgevingen op dit terrein?

'Wij hebben ervoor gekozen reeds per 1 januari 2007 te willen werken conform de eisen uit het Bazel II akkoord, vooralsnog volgens de standardised approach. Ruim een jaar geleden is een projectteam van start gegaan om dit doel te bereiken. De bemensing van het project is vrijwel volledig gebaseerd op de bestaande organisatie. Er is vooralsnog nauwelijks extra capaciteit voor nodig gebleken. De afdeling Credit Risk Management van de BNG heeft het voortouw in het project.

'Ten aanzien van de code Tabaksblad hebben wij op enkele punten gebruik gemaakt van het comply or explain principe. Hoewel wij op vrijwel alle punten aan de code voldoen, zijn er enkele punten waar wij uitgelegd hebben waarom wij niet aan de betreffende bepaling voldoen of willen voldoen. Een voorbeeld hiervan is de benoemings-termijn van bestuurders. Wij zijn van mening dat een termijn van 4 jaren te kort is.

'Overigens heeft ook de invoering van de International Financial Reporting Standards (IFRS) nogal wat voeten in de aarde als het gaat om de wijze waarop risico's gemanaged worden. Dan heb ik het met name over de marktrisico's en in het bijzonder het renterisico. IFRS brengt gewijzigde definities voor de waardering van primaire en afgeleide financiële instrumenten met zich mee. Deze wijzigingen werken vervolgens door in alle facetten van de organisatie waar het renterisico speelt.'

### Waar staat de BNG op dit moment. Loopt u op schema?

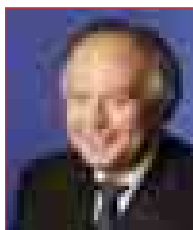
'Dat is moeilijk om te zeggen. Ik spreek als het om projecten gaat wel eens van de 200-200-50-regel. Projecten duren vaak 2 keer langer dan gepland, kosten 2 keer zoveel budget als ingecalculeerd en leveren slechts 50% van de vooraf beoogde functionaliteit. Of die regel ook opgaat voor ons Bazel II-project is op dit moment nog niet te voorspellen, maar het ligt niet erg voor de hand. Vooralsnog liggen we aardig op schema en we zullen er alles aan doen om dat zo te houden.'

### Hoe is de Raad van Bestuur in de praktijk betrokken bij het managen van risico's in de organisatie?

'De verantwoordelijkheid voor risicomanagement hebben wij nadrukkelijk belegd bij de Raad van Bestuur als geheel. Bij het managen van het kredietrisico ben ik nauw betrokken als voorzitter van de kredietcommissie. Het marktrisico en het renterisico komen aan bod in de Asset & Liability Commissie waar ik lid van ben. Ik zou daar trouwens geen voorzitter van kunnen zijn omdat ik de verantwoordelijkheid draag voor Treasury. Voor operationele risico's hebben wij momenteel geen commissie. We zijn de mogelijke varianten aan het onderzoeken om ook de operationele risico's in een commissie te behandelen. Management van operationele risico's wordt momenteel gecoördineerd door onze stafafdeling OIC (organisatiebeheersing, informatie & compliance).

### Een belangrijke reden voor de huidige belangstelling voor risicomanagement is de gedachte dat het organisaties in staat stelt om 'in-control' te geraken dan wel te blijven. Maar wanneer is een organisatie eigenlijk 'in-control'?

'Mijn achtergrond is die van Register Accountant. Ik maak nog vaak gebruik van de binnen het vakgebied van administratieve organisatie en interne controle (AO/IC) gangbare begrippen opzet, bestaan en werking. Vanuit het perspectief van opzet en bestaan kan ik me nog voorstellen dat het mogelijk is om te bepalen of een organisatie in-control is. Echter, te stellen dat een risicobeheersings- en controlesysteem over een bepaalde periode gedurig heeft gewerkt, ik denk dat er geen accountant te vinden is die zich daar aan wil wagen. En als er al één te vinden is, dan zal het hooguit zijn in de vorm van negative assurance (ons is niet gebleken dat ..... niet goed heeft gewerkt). En als een accountant de gedurige werking al niet kan vaststellen, hoe kun je dan van een bestuurder verwachten dat hij dat wel kan? Ik ben dan ook van mening dat er nog al wat haken en ogen zitten aan de in-control verklaring die bestuurders onder de code Tabaksblad – al dan niet expliciet - moeten afgeven. Over de vraag wanneer een organisatie in-control is en hoe je dat vaststelt zal nog veel worden gesproken.'



### 'Balanceren tussen risico en rendement'

Prof. Dr. J.J.A. Leenaars  
Lid Raad van Bestuur, Bank Nederlandse Gemeenten



RuG

De Rijksuniversiteit Groningen verzorgt in een breed en gevarieerd scala aan vakgebieden kwalitatief hoogstaand onderwijs en onderzoek. Eén van de opleidingen van de RuG is de postdoctorale controllersopleiding. Met zijn integratie van theorie en praktijk biedt deze opleiding een uitstekende basis voor zware financiële management en adviesfuncties zowel binnen het bedrijfsleven als bij (semi-) overheidsorganisaties. Afronding van de opleiding geeft recht op inschrijving in het Register van de Vereniging van Registercontrollers en het voeren van de RC-titel. Het parttime programma duurt twee jaar. De Postdoctorale Controllersopleiding is een gezamenlijke opleiding van de Faculteit Bedrijfskunde en de Economische Faculteit voor bedrijfseconomen, bedrijfskundigen (richting controlling of accountancy) en registeraccountants. Meer informatie vindt u op [www.rug.nl/bdk/onderwijs/postacademischonderwijs](http://www.rug.nl/bdk/onderwijs/postacademischonderwijs).

PRICEWATERHOUSECOOPERS 

Bij PricewaterhouseCoopers Nederland werken ruim 4.000 professionals met elkaar samen vanuit 19 kantoren en drie verschillende invalshoeken: Assurance, Tax en Human Resource Services, Advisory. Op basis van ons gedachtegoed Connected Thinking leveren we sectorspecifieke diensten en zoeken we verrassende oplossingen. Niet alleen voor grote nationale en internationale ondernemingen. Ook voor overheden en non-profitorganisaties. En net zo goed voor middelgrote en kleinere ondernemingen.

Als zelfstandig onderdeel van een wereldwijd netwerk met ruim 130.000 collega's in 148 landen beschikken we over veel kennis en ervaring. Die delen we met elkaar, met onze cliënten en hun stakeholders. We voelen ons betrokken, zijn gewend om goed te luisteren en vinden het de gewoonste zaak van de wereld om ook zelf rekening en verantwoording af te leggen over onze prestaties.

