



Inzicht in Onzekerheid

Onderzoek naar de risicoparagrafen in de
jaarverslagen 2007 van beursfondsen

Prof. dr. G.M.H. Mertens & drs. I.H.C. Blij CFA
Juni 2008



Inzicht in Onzekerheid

Onderzoek naar de risicoparagrafen in de
jaarverslagen 2007 van beursfondsen

Prof. dr. G.M.H. Mertens & drs. I.H.C. Blij CFA
Juni 2008



Titel:

Inzicht in onzekerheid. Onderzoek naar de risicoparagrafen in de jaarverslagen 2007 van beursfondsen

Auteurs:

Gerard Mertens en Ivo Blij (met medewerking van Mario Brink, Mark Nijman, Fleur Verbeek en Floris Verveen)

In opdracht van het Koninklijk NIVRA en Eumedion gepubliceerd door:

Shareholder Support

Correspondentie:

Gerard Mertens
Shareholder Support
Molenberglaan 87
6416 EL Heerlen
Email: info@shareholdersupport.nl



Voorwoord

Geachte lezer,

Voor u ligt het eindresultaat van enkele maanden intensief onderzoek. Begin 2008 benaderden het NIVRA en Eumedion ondergetekende met het verzoek een empirisch onderzoek uit te voeren naar de informatieverstrekking over risico's en beheersingssystemen in de risicoparagrafen van de jaarverslagen 2007. Beide organisaties zijn al langere tijd nauw betrokken bij het debat over risicobeheersing. Eumedion heeft in haar speerpuntenbrief 2008 één speerpunt gedefinieerd dat specifiek betrekking heeft op de bedrijfsstrategie en het risicomanagement van de beursgenoteerde ondernemingen. Het NIVRA, de beroepsvereniging van registeraccountants, wil graag het debat tussen het accountantsberoep en de samenleving over risicobeheersing stimuleren en faciliteren. Dit rapport vormt derhalve belangrijke input voor de discussie die tijdens het seminar op 24 juni 2008 zal plaatsvinden.

Risicomanagement is een onderwerp dat volop in de belangstelling staat. In de Nederlandse Corporate Governance Code is onder meer opgenomen dat ondernemingen moeten beschikken over een 'adequaat en effectief intern risicobeheersings- en controlesysteem'. Tevens moeten bestuurders van ondernemingen sinds 2004 een zogenoemde 'in control'-verklaring afgeven. De Monitoring Commissie Corporate Governance heeft in de afgelopen jaren aanbevelingen gedaan; die vormen samen met de Code een belangrijke stimulans voor meer transparante verslaggeving over het risicomanagement van beursondernemingen. Ook vanuit ondernemingen is er groeiend besef dat risicomanagement een kritische succesfactor is, die bijdraagt aan het (financiële) succes van de onderneming.

Het is positief om te constateren dat de aandacht voor dit onderwerp zijn weerslag heeft in de verslaggeving van ondernemingen: de informatie over risico's en de beheersingssystemen in de jaarverslagen is sinds 2004 duidelijk in omvang en kwaliteit toegenomen.

Echter, zoals uit de conclusies van dit onderzoek blijkt, is er nog veel ruimte voor verdere verbetering. Met het oog op de voorgenomen herziening van de Code eind 2008, kan dit rapport bijdragen aan een fundamentele discussie over het nut en de noodzaak van meer transparantie in de verslaggeving van Nederlandse beursfondsen. Daarbij zou de nadruk meer moeten liggen op de analyse van de risico's van de onderneming dan op de tot nu toe gebruikelijke beschrijving van de beheersingssystemen.

Om het onderzoek goed te kunnen uitvoeren, hebben ik en mede-onderzoeker Ivo Blij een beroep kunnen doen op een kwartet bekwame en uiterst loyale master-studenten aan de Erasmus Universiteit Rotterdam. Een bijzonder woord van dank aan Mario Brink en Floris Verveen; zij hebben ons tot het laatste moment ondersteuning geboden. Ook wil ik Rients Abma, Edwin Bolten en Johan Scheffe bedanken voor hun waardevolle input en de prettige samenwerking gedurende de afgelopen maanden.

Heerlen, juni 2008



Prof. dr. Gerard Mertens
Rotterdam School of Management
Erasmus University



Copyright

Statusomschrijving

Deze publicatie is samengesteld voor leden en derden. De publicatie heeft geen status in het kader van de beroepsuitoefening, wel kan worden verwezen naar publicaties die een dergelijke status wel hebben.



Inhoudsopgave

Voorwoord	3
Samenvatting	6
Executive summary	8
1 Inleiding	10
1.1 Aanleiding, motivatie en doelstelling onderzoek	10
1.2 Risicomanagement: een nadere afbakening	11
1.3 Overzicht inhoud rapport	11
2 Institutionele aspecten	13
2.1 Overzicht ontwikkelingen risicomanagement	13
2.2 Code Tabaksblad	15
2.3 Monitoring Commissie Corporate Governance	16
2.4 Speerpuntenbrief Eumedion	18
2.5 Overige relevante wet- en regelgeving	19
3 Dataselectie en onderzoeksaanpak	21
3.1 Dataselectie en samenstelling onderzoekspopulatie	21
3.2 Onderzoeksaanpak	22
4 Resultaten empirisch onderzoek	23
4.1 Inleiding	23
4.2 Informatie over risico's	23
4.3 Informatie over risicobeheersings- en controlesystemen	29
4.4 'In control'-verklaring	32
4.4.1 'In control'-verklaring	33
4.4.2 'In control'-verklaring met brede scope	37
4.4.3 'In control'-verklaring met betrekking tot financiële verslaggevingsrisico's	39
5 Samenvatting en conclusies	43
Bijlagen	
A Speerpuntenbrief Eumedion	47
B Europese Richtlijn 2006/46/EG	51
C Vragenlijst	53
D Best Practices	55



Samenvatting

In dit rapport staat de informatieverstrekking over risico's en beheersingssystemen door Nederlandse beursgenoteerde ondernemingen centraal. Risicomanagement is het geheel van activiteiten en maatregelen dat gericht is op het beheersen van risico's. Het onderhavige onderzoek verschaft inzicht in de verslaggeving omtrent risico's en beheersingssystemen van beursgenoteerde ondernemingen op basis van een inventarisatie van de jaarverslagen over het boekjaar 2007. Het empirisch onderzoek besteedt aandacht aan:

1. de informatie over risico's van de onderneming
2. de informatie over risicobeheersings- en controlesystemen van de onderneming
3. de 'in control'-verklaring

Overall beeld ten aanzien van de informatie over risicomanagement

Risicomanagement is een onderwerp dat volop in de belangstelling staat. Het is positief om te constateren dat de aandacht voor dit onderwerp in de jaarverslaggeving van ondernemingen duidelijk is toegenomen. Informatieverschaffing over risicomanagement is onmiskenbaar in ontwikkeling. Wij hebben geconstateerd dat het onderwerp ook in het jaarverslag aan belang wint, maar daarbij dient te worden opgemerkt dat er nog geen onderneming is die alle aspecten in haar jaarverslag heeft opgenomen.

Tevens komt uit het onderzoek naar voren dat er in de verslaggeving omtrent risicomanagement sprake is van grote diversiteit in:

1. de mate van diepgang
2. de beschrijving van risico's en beheersingssystemen
3. de kwaliteit van de 'in control'-verklaring

Opvallend is dat de verschillen in transparantie tussen AEX-, AMX- en AScX-ondernemingen op een aantal aspecten afwijken van de algemene beeldvorming: uit het onderzoek komt naar voren dat de AMX- en AScX- meer transparant zijn dan de AEX-ondernemingen.

Informatie over risico's van de onderneming

62% verstrekt informatie over de belangrijkste risico's die zijn verbonden aan de strategie. De meest genoemde categorieën risico's zijn operationele en financiële risico's. Risico's omtrent wet- en regelgeving en financiële verslaggevingsrisico's worden minder vaak vermeld.

Een luttel 10% verschaft inzicht in de belangrijkste risico's. Ondernemingen doen weliswaar vrij uitvoerig verslag van alle risico's, maar een prioritering ontbreekt in de meeste gevallen. Wij hebben uitvoerige opsommingen van risico's aangetroffen, zonder dat deze worden gekwantificeerd of dat daarbij een relatie met de ondernemingsstrategie wordt gelegd.

Bij de kwantificering van risico's is sprake van aanzienlijke verschillen tussen de categorieën ondernemingen. De AEX-ondernemingen rapporteren frequenter en het aantal onderscheiden risico's is meer divers van aard. Gekwantificeerde risico's zijn meestal 'hard' en financieel van aard. In de verslaggeving over risico's is geen informatie aangetroffen over de samenhang tussen bepaalde risico's. Driekwart van de ondernemingen die de risico's kwantificeren, verstrekt informatie over het effect op het resultaat: de helft rapporteert de impact op het eigen vermogen. De informatie hierover neemt af naarmate ondernemingen kleiner zijn. Geen van de onderzochte ondernemingen heeft bij de gepresenteerde risico's aangegeven wat de kans is op het zich voordoen van een dergelijk risico.

Slechts 15% van de onderzochte ondernemingen geeft een indicatie van haar risicobereidheid; de *risk appetite* wordt nog te weinig concreet beschreven.

Informatie over risicobeheersings- en controlesystemen van de onderneming

Alle AEX- en AMX-ondernemingen hebben informatie opgenomen over de systemen en de procedures, dat geldt niet voor de AScX- en de Overige ondernemingen. De kwaliteit van de hierover verstrekte informatie verschilt sterk. Met name voor de kleine ondernemingen geldt dat informatie over de procedures niet of slechts beperkt aanwezig is. Ruim de helft verwijst in de beschrijving van de systemen naar het werk van de controlerende accountant en driekwart van alle ondernemingen naar de interne accountant en/of stafdiensten met een controlerende taak.



In vrijwel alle jaarverslagen wordt melding gemaakt van een periodieke evaluatie, maar in minder dan 5% wordt daadwerkelijk informatie over de uitkomsten van de evaluatie verstrekt. AScX-ondernemingen zijn het meest transparant (14%), de AEX-ondernemingen daarentegen zijn volledig intransparant, zij lijken geen inzicht te willen geven in mogelijke tekortkomingen van de risicobeheersings- en controlesystemen.

71% van de ondernemingen beschrijven de risico's en de systemen in één hoofdstuk of apart onderdeel van het jaarverslag. De AScX- en de Overige ondernemingen scoren beter dan de AEX- en AMX-ondernemingen. Ruim een derde van de ondernemingen heeft de 'in control'-verklaring niet opgenomen in de risicoparagraaf, vooral de AEX-ondernemingen blijken hiervan af te wijken.

Het meest gebruikte risicoraamwerk is het COSO-model, iets minder dan de helft van de ondernemingen verwijst hiernaar (voor de AEX ligt dit op 91%). Opvallend is dat het meest wordt verwezen naar het (oudere) COSO-IC model. Twee derde van de AEX-ondernemingen verwijst naar het oorspronkelijke COSO-model, bij de AMX en AScX wordt relatief vaker verwezen naar COSO-ERM.

De 'in-control' verklaring

Slechts een kwart van de ondernemingen verwijst in de 'in control' verklaring expliciet naar best practice bepaling II.1.4, eenderde verwijst naar de aanbevelingen van de Monitoring Commissie.

Minder dan een kwart van alle ondernemingen rapporteert over de werking van de risicobeheersings- en controlesystemen in het boekjaar. De verslaggeving over de werking van de systemen heeft merendeels betrekking op de financiële verslaggeving. Iets minder dan één op de tien ondernemingen verklaart in brede zin dat de systemen effectief zijn: zeven ondernemingen verklaren dat de systemen effectief en adequaat zijn. Slechts één onderneming geeft een onderbouwing van de verklaring omtrent de effectiviteit en adequaatheid van de interne risicobeheersings- en controlesystemen. Wat betreft de werking van risico-beheersings- en controlesystemen blijken de afgegeven verklaringen niet goed aan te sluiten bij best practice bepaling II.1.4 van de Code.

De 'in control'-verklaring die betrekking heeft op de risico's met betrekking tot de financiële verslaggeving (conform de guidance van de Monitoring Commissie) is in 85% van de jaarverslagen aangetroffen. De AEX- en AMX-ondernemingen scoren 100%, bij de AScX- en Overige ondernemingen is dit 86% respectievelijk 69%. Het forward looking statement is in 65% van de jaarverslagen aangetroffen. Opvallend is de relatief lage score van de AEX (76%).

Tenslotte is nagegaan of de risicoparagraaf, voor zover betrekking hebbend op de financiële verslaggevings-risico's, informatie bevat over eventuele tekortkomingen en/of doorgevoerde of geplande verbeteringen zijn aangegeven. Slechts 4% van de ondernemingen vermeldt eventuele materiële tekortkomingen die zijn geconstateerd, terwijl één op de vijf ondernemingen melding maakt van doorgevoerde of geplande verbeteringen. Ondernemingen wensen klaarblijkelijk liever geen inzicht te geven in mogelijke tekortkomingen van de risicobeheersings- en controlesystemen. Dit geldt het sterkst voor de grote ondernemingen.

Op basis van de uitkomsten van dit onderzoek is in het laatste hoofdstuk van dit rapport (hoofdstuk 5) een aantal aandachtspunten geïdentificeerd ter verbetering van de verslaggeving over risico's en beheersings-systemen:

1. de toegankelijkheid van de verschafte informatie
2. de voorzichtigheid bij ondernemingen aangaande de 'in control'-verklaring
3. de presentatie van de informatie over risicomanagement
4. de informatie over risico's
5. de informatie over *risk appetite*



Executive Summary

Risk management includes all activities and procedures aimed at minimizing and controlling risks. This research focuses on risk management of Dutch public companies. It provides insights in the disclosure of risks and internal control systems of public companies, based on the analysis of annual reports regarding 2007. The empirical part focuses on:

1. the information on risks
2. the information on risk management and control systems
3. the 'in control'-statement

Overall conclusion regarding the disclosure of risk management information

Risk management is a frequently debated topic in the corporate governance world. We observe that the topic receives more and more attention in financial reporting, which is a positive development. However, based on the results of this research we conclude that none of the public companies report on all aspects of risk management.

Furthermore, our empirical research has revealed, that disclosure practices regarding risks and internal control systems show a wide diversity regarding:

1. the level of detail
2. the description of the risks and control systems
3. the quality and the scope of the 'in control'-statement

A remarkable finding is that the differences in transparency between the LargeCap, MidCap- and SmallCap companies are not in line with the general idea that large firms are more transparent. Instead, our findings show that Mid- and SmallCaps are more transparent than the LargeCaps in various aspects of disclosure regarding risk management.

Information regarding company risks

Only 62% of the companies provides information on the most important risks related to the company's strategy. Operational and financial risks are mentioned most, whereas compliance and financial reporting risks are reported least.

A mere 10% gives insight into the most important risks associated with the company's strategy. Although most companies report quite extensively on all risks, a majority of the financial reports lack information on the most important risks. Neither are these risks quantified, nor are they company specific.

Concerning risks that are quantified, we observe substantial differences between companies. LargeCaps quantify more risks and they distinguish more types of risks. Typically, the risks that are quantified relate to financial risks. There is no information available on the relationship (correlation) between different risks. 50% reports on the impact of risks on equity, 75% reports on the impact on the results. SmallCaps provide less disclosure on this aspect. None of the disclosures on risks provide information regarding the probability of these risks occurring.

Only 15% reports on the risk appetite; this concept clearly is not yet well described in the financial statements.

Information regarding the company's internal risk management and control systems

All Large- and MidCaps provide information on the control systems and procedures in place, though the quality of the information varies widely. SmallCaps either lack an adequate description of the control systems and procedures, or they report no information at all. Approximately half of the companies refer to the work of the external auditor when describing the systems and procedures. 75% refers to the internal auditor. Although in almost all annual reports the evaluation of the systems and procedures is mentioned, less than 5% has information on the outcome. To our surprise the SmallCaps turned out to be more transparent than the Mid- and LargeCaps. The latter provide no information at all on this item. From this we conclude that larger companies, LargeCaps in particular, seem to be reluctant to provide any information on deficiencies or weaknesses of their control systems.



71% of the companies provide information on their risk management in one section of the annual report, with the Small Caps being better than the Mid- and LargeCaps. A third of the companies disclose their 'in control'-statement in different parts of the annual report. COSO was used the most as risk management framework: almost 50% refers to it (91% of the LargeCaps). Remarkably, companies refer more often to the (older) COSO-IC framework than to the COSO-ERM. The latter is more present in Mid- and SmallCap companies.

'In control'-statement

Only 25% of all companies refers explicitly to best practice provision II.1.4 of the Dutch Corporate Governance Code in the 'in control'-statement and reports on the performance of the internal risk management and control systems.

The information provided on the performance of the risk management and control systems mainly deals with financial reporting risks; there is far less disclosure on other risks. Less than 10% provides an 'in control'-statement beyond the scope of the financial reporting risks: 7 companies declare that the internal risk management and control systems are effective and adequate; only one of them provides clear substantiation for this.

85% of the companies provides an 'in control'-statement regarding the financial reporting risks. All Large- and MidCaps present the statement, compared to 86% of the SmallCaps and 69% of the other companies. 65% has a forward looking statement (LargeCaps less than MidCaps).

We have also examined if the risk management section of the annual report contains any information on deficiencies and significant changes in the systems or any planned improvements. Only 4% reports on large deficiencies; 20% reports on changes and planned improvements. Companies apparently hesitate to provide information on the potential weaknesses of their internal risk management and control systems.

Based on the findings of our research the last chapter of this report provides key areas for improving the quality of information on risk management. These refer to:

1. the accessibility of the information
2. the cautiousness regarding the use (and scope) of the 'in control'-statement
3. the presentation of the information on risk management
4. the information on risks
5. the information on risk appetite



1 Inleiding

1.1 Aanleiding, motivatie en doelstelling onderzoek

Aanleiding

Op 8 november 2007 publiceerde Eumedion, het corporate governance platform voor institutionele beleggers, haar speerpuntenbrief 2008. Deze brief bevat belangrijke onderwerpen die de bij Eumedion aangesloten deelnemers onder de aandacht willen brengen bij de 75 grootste Nederlandse beursgenoteerde ondernemingen. Voor 2008 heeft Eumedion één speerpunt gedefinieerd dat specifiek betrekking heeft op de bedrijfsstrategie en het risicomanagement van de beursgenoteerde ondernemingen. Ze roept de ondernemingen op in hun jaarverslag over het boekjaar 2007 een informatieve en inzichtelijke, brede risicoparagraaf op te nemen.

Registeraccountants dragen bij aan een duurzame en stabiele samenleving. Zij wensen een signalerende rol te vervullen in het maatschappelijk debat en als spil te fungeren tussen belanghebbende partijen. Hun doel is bij te dragen aan de verbetering van transparantie, risicobeheersing en doelmatigheid van de onderneming. Het NIVRA, de beroepsvereniging van registeraccountants, wil de signalerende rol graag stimuleren en faciliteren. De opening van het nieuwe kantoor van het NIVRA door H.M. de Koningin, op 16 april 2008, vormde onder meer de aanleiding voor een debat tussen het accountantsberoep en de samenleving over risicobeheersing. In 2006 publiceerde het NIVRA de resultaten van een onderzoek naar de informatieverzorging omtrent risico's in het directieverslag¹. Dit onderzoek naar de actuele verslaggevingspraktijken omtrent risico's en beheersingssystemen van Nederlandse beursgenoteerde ondernemingen kan worden gezien als een vervolg daarop.

Voorvallen in het recente verleden tonen aan wat de negatieve gevolgen kunnen zijn van onvoldoende (toe)zicht op de risico's van ondernemingen en/of een niet goed functionerend risicomanagement². Vandaar dat beleggers, maar ook andere stakeholders, in toenemende mate informatie eisen over de aard en de omvang van de risico's waaraan de onderneming is blootgesteld en de maatregelen die zij al dan niet neemt om deze risico's te beheersen.

Motivatie

In dit rapport staat de informatieverstrekking over risicomanagement door Nederlandse beursgenoteerde ondernemingen centraal. In de kern handelt corporate governance over het afleggen van verantwoording en het creëren van transparantie. Onderdeel van een goed functionerende corporate governance binnen een onderneming is het beheersen van risico's en de verslaggeving hieromtrent. Risico's zijn inherent aan ondernemerschap: elke onderneming heeft ermee te maken, ongeacht haar aard en omvang. Zowel voor de onderneming als haar stakeholders is het van groot belang goed inzicht te hebben in de risico's. Vanuit de onderneming is er een groeiend besef dat een goede beheersing van risico's een belangrijke bijdrage kan leveren aan de performance. Hierdoor is bij het management meer aandacht ontstaan voor de strategische en operationele risico's³. Daarnaast zijn er institutionele factoren, zoals wet- en regelgeving, die ondernemingen ertoe dwingen om risicomanagement meer aandacht te geven.

Mede vanwege het belang van een goede corporate governance wordt informatie over risico's door ondernemingen steeds belangrijker. Belangrijk voor Nederland is in dit verband natuurlijk de publicatie van de Nederlandse Corporate Governance Code op 9 december 2003 door de Commissie Tabaksblat. In deze code is onder meer opgenomen dat ondernemingen dienen te beschikken over een 'adequaat en effectief intern risicobeheersings- en controlesysteem'. Tevens worden bestuurders van ondernemingen vanaf het boekjaar 2004 verplicht om een zogenoemde 'in control'-verklaring af te geven. Hierin dienen zij onder andere te verklaren dat de onderneming beschikt over adequate en effectieve risicobeheersings- en controlesystemen. In december 2007 heeft de Monitoring Commissie Corporate Governance, die onder andere als taken heeft de actualiteit van de Code te waarborgen en de bruikbaarheid te bevorderen, in haar jaarlijkse evaluatie van de naleving van de best practice bepalingen van de Code aanvullende criteria opgesteld die betrekking hebben

¹ De Groot, Kuijl en Scheffe (2006), Informatieverzorging over risico's in het directieverslag, hst 5, In: Het jaar 2005 verslagen, NIVRA, Kluwer.

² Daarbij kan worden gedacht aan onder andere inmiddels klassieke voorbeelden als Barings, Orange County, Enron, Ahold en Parmalat, maar ook de meer recente crises bij financiële instellingen (waaronder Société General, Bear Stearns en Northern Rock) kunnen in dit verband worden aangehaald.

³ De Pooter (2008), Risicomanagement: strategische ondernemingsrisico's effectief beheersen. MCA, april, nr. 2.



op de 'in control'-verklaring. In Nederland vormen deze bepalingen tezamen een belangrijke stimulans voor meer transparante verslaggeving omtrent het risicomanagement van beursondernemingen⁴.

Doelstelling

Eumedion en het NIVRA hebben de volgende onderzoeksvragen geformuleerd:

1. hoe is door Nederlandse beursgenoteerde ondernemingen gerapporteerd over de risico's en de beheersingssystemen?
2. welke informatie is omtrent deze risico's en de beheersingssystemen opgenomen in het jaarverslag (en op de website) van de ondernemingen?
3. welke best practices zijn er voor risicomanagement?

Dit rapport beoogt inzicht te verschaffen in de verslaggeving omtrent risico's en beheersingsmaatregelen van beursgenoteerde ondernemingen op basis van een inventarisatie van de jaarverslagen over het boekjaar 2007. Tevens tracht het aan de hand van de verkregen inzichten bij te dragen aan de verbetering van verslaggeving en transparantie op het gebied van risicomanagement. Om het onderzoek te kunnen uitvoeren zijn data verzameld met behulp van een vragenlijst, waarin specifieke vragen zijn opgenomen op basis waarvan de aanwezigheid en de aard van de informatie omtrent risico's en beheersingsmaatregelen is onderzocht. De volledige onderzoeksopzet wordt in hoofdstuk drie beschreven. In de navolgende paragraaf staan wij stil bij het begrip risicomanagement.

1.2 Risicomanagement: een nadere afbakening

Risicomanagement kan in algemene zin worden omschreven als het geheel van activiteiten en maatregelen die gericht zijn op het beheersen van risico's. Risicomanagement bestaat uit een aantal onderdelen.

Het eerste onderdeel betreft een periodieke en systematische inventarisatie van de belangrijkste risico's die verbonden zijn aan de onderneming. Het tweede onderdeel omvat een inschatting van (a) de kans dat deze risico's zich voordoen en (b) de omvang van de (financiële) consequenties bij het optreden van deze risico's. Ten derde omvat risicomanagement het ontwikkelen van beleid gericht op het controleren en beheersen van de risico's en de mogelijke gevolgen daarvan. Tenslotte dient de werking van het risicomanagementsysteem te worden gecontroleerd. Integraal vormen deze aspecten de basis van het risicomanagementraamwerk van een onderneming⁵.

De reikwijdte van het begrip risico is breder dan alleen financiële risico's. Zo onderscheidt het Committee Of Sponsoring Organisations (COSO) vier soorten risico's:

1. operational
2. reporting (financiële verslaggeving)
3. compliance (wet- en regelgeving)
4. strategic (COSO, 2004)

In navolging van COSO hanteert ook de Monitoring Commissie Corporate Governance Code (Frijns) hierna te noemen Monitoring Commissie dezelfde categorieën risico's⁶.

1.3 Overzicht inhoud rapport

Het vervolg van dit rapport is als volgt opgebouwd. In hoofdstuk 2 zal het institutionele kader worden geschetst, dat van belang is voor het vertrekpunt van dit onderzoek. Daarbij zal achtereenvolgens aandacht worden besteed aan het risicoraamwerk van COSO, de belangrijkste bepalingen van de Sarbanes Oxley wetgeving en de *Turnbull guidance*. Uiteraard wordt in dit hoofdstuk ook aandacht besteed aan de relevante bepalingen van de Code Tabaksblat en de aanbevelingen van de Monitoring Commissie. Tevens zal de speerpuntenbrief van Eumedion worden besproken. Tot slot van dit hoofdstuk is er aandacht voor recente

⁴ Volledigheidshalve dient te worden opgemerkt dat de reikwijdte van de best practice bepalingen van de Code Tabaksblat en de aanbevelingen van de Monitoring Commissie niet beperkt blijven tot de beursgenoteerde ondernemingen. Ook grote, niet beursgenoteerde ondernemingen passen de best practice bepalingen en aanbevelingen toe (op vrijwillige basis).

⁵ Zie voor een uitvoerige verhandeling van risicomanagement en interne risicobeheersing Anthony and Govindarajan (2007), *Management Control Systems*, McGraw-Hill.

⁶ Hoewel qua uitwerking verschillend, geldt ook voor de Sarbanes Oxley wetgeving (2002) en de Turnbull Guidance (2005), dat beiden het COSO-raamwerk als uitgangspunt hanteren.



ontwikkelingen op het gebied van wet- en regelgeving, meer in het bijzonder de Europese Richtlijn 2006/46/EG, die is toegespitst op corporate governance en informatie over risicobeheersing. Vervolgens komen in hoofdstuk 3 de dataselectie, de onderzoekspopulatie en de onderzoeks aanpak aan de orde. Hoofdstuk 4 vormt het belangrijkste hoofdstuk; hierin worden de resultaten van het onderzoek gepresenteerd. Naast een gedetailleerde weergave van de verslaggeving omtrent de drie hoofdthema's risico's, risicomanagement en beheersingsmaatregelen, zullen eveneens best practice voorbeelden worden aangehaald op basis van de onderscheiden elementen van risicomanagement. Ten slotte bevat hoofdstuk 5 de belangrijkste bevindingen en conclusies van dit onderzoek.



2 Institutionele aspecten

In dit hoofdstuk wordt een overzicht gepresenteerd van de belangrijkste institutionele ontwikkelingen op het gebied van risico's en beheersingssystemen. Eerst volgt een korte beschrijving van het COSO-raamwerk en de relevante bepalingen van de Turnbull Committee en de Sarbanes Oxley wetgeving (hierna SOX). Vervolgens staan we stil bij de relevante (best practice) bepalingen van de Code Tabaksblat, de aanbevelingen van de Monitoring Commissie en de speerpuntenbrief van Eumedion. Tot slot van dit hoofdstuk is er aandacht voor recente ontwikkelingen op het gebied van wet- en regelgeving, meer in het bijzonder de Europese Richtlijn 2006/46/EG.

Tezamen vormen de bovengenoemde instituties het krachtenveld waarbinnen Nederlandse beursfondsen thans opereren. In het vervolg van dit onderzoeksrapport zal dan ook op basis hiervan een nadere concretisering plaatsvinden van de specifieke aspecten van risico's en beheersingssystemen die nader zullen worden onderzocht.

2.1 Overzicht ontwikkelingen risicomanagement

Het Committee of Sponsoring Organizations of the Treadway Commission, hierna COSO, heeft een belangrijke bijdrage geleverd aan de ontwikkeling van risicomanagement.

COSO is een vrijwillige private-sector organisatie en heeft als doel bestuurders en toezichhouders te helpen om op wereldschaal te komen tot effectieve, efficiënte en ethische bedrijfsvoering. Op basis van onderzoek en best practices worden raamwerken ontwikkeld en verspreid. COSO is opgericht in 1985 voor de sponsoring van de Nationale Commissie voor Frauduleuze Financiële Rapportering (NCFFR), een onafhankelijk privaat initiatief, dat de oorzakelijke factoren onderzocht die kunnen leiden tot frauduleuze financiële rapportering. De NCFFR ontwikkelde ook aanbevelingen voor beursgenoteerde ondernemingen en hun externe accountants, voor de Amerikaanse toezichthouder (SEC) en andere regelgevers alsmede voor opleidingsinstituten⁷.

In 1992 verscheen een gezaghebbende studie over interne beheersing en beheersingssystemen. Deze studie, waarin ook aanbevelingen worden gedaan voor de opzet en evaluatie van beheersingssystemen, wordt alom gezien als één van de belangrijkste op dit terrein. COSO (1992, p.3) definieert daarin interne beheersing als:

“a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- *Operational: effectiveness and efficiency of operations*
- *Reporting: reliability of financial reporting*
- *Compliance: compliance with applicable laws and regulations.”*

Interne beheersing dient de ondernemingsleiding in staat te stellen om adequaat te reageren op veranderingen of afwijkingen in de interne en externe omgeving, de efficiency te bevorderen, het risico van verlies te beperken, de betrouwbaarheid van financiële verslaglegging te waarborgen en te voldoen aan wet- en regelgeving (COSO, 1992).

Het COSO Internal Control (COSO-IC) raamwerk van 1992 is in 2004 uitgebreid tot het Enterprise Risk Management (COSO-ERM) raamwerk. Het nieuwe raamwerk voegt naast de drie genoemde beheersingsdoelstellingen een vierde doelstelling toe, te weten risicobeheersing ten aanzien van strategie (*strategic: high-level goals, aligned with and supporting its mission*). COSO benadrukt de relevantie van de strategie van een organisatie voor de inrichting van haar risicomanagement en interne beheersingssystemen.

⁷ De NCFFR werd gesponsord door 5 grote Amerikaanse professionele organisaties: de American Accounting Association (AAA), de American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), het Institute of Internal Auditors (IIA), en de National Association of Accountants (huidige naam Institute of Management Accountants [IMA]). De NCFFR bestaat uit vertegenwoordigers van bedrijven, externe accountants, investeerders en de New York Stock Exchange (Bron: <http://www.coso.org>).



Het COSO-ERM-raamwerk legt in vergelijking met zijn voorganger meer nadruk op risicomanagement. Daar waar COSO-IC risico's impliciet zag als negatieve (verliesgevende) gebeurtenissen, wordt bij COSO-ERM aangegeven dat risico's ook kansen bieden die, mits goed beheerst, kunnen bijdragen aan het waardecreërend vermogen van de onderneming. Een ander belangrijk nieuw element in het COSO-ERM-raamwerk is het begrip *risk appetite*. Gedoeld wordt daarbij op de risicobereidheid van de ondernemingsleiding. Hiervoor is het belangrijk om inzicht te hebben in de kans en de impact van de risico's verbonden aan de ondernemingsdoelstellingen alsmede het vermogen van de onderneming om zich aan te passen aan veranderende omstandigheden. Het begrip *risk appetite* komt later ook aan de orde bij de bespreking van de aanbevelingen van de Monitoring Commissie (2.4).

COSO wordt nog steeds gezien als het belangrijkste raamwerk voor interne controle en risicobeheersing. Niet alleen de Code Tabaksblat en de Monitoring Commissie verwijzen naar de uitgangspunten en onderdelen van het COSO-raamwerk, ook SOX is voor een belangrijk deel gebaseerd op het COSO-raamwerk⁸.

SOX is het Amerikaanse antwoord op diverse schandalen begin deze eeuw waarbij grote (Amerikaanse) ondernemingen betrokken waren. Hierdoor kreeg het vertrouwen van de beleggers in de waarheidsgetrouweheid van de financiële rapportering een flinke deuk. SOX beoogt deugdelijk ondernemingsbestuur te garanderen en zo het geschonden vertrouwen van de beleggers te herstellen. De invoering van SOX heeft directe gevolgen gehad voor het gedeelte van de Nederlandse beursgenoteerde ondernemingen met een beursnotering in de Verenigde Staten. In *sectie 302* en *sectie 404* van de wet wordt geregeld dat de bestuurders van beursgenoteerde ondernemingen een tweetal verklaringen moeten afgeven. *Sectie 302* bepaalt dat de CEO en CFO moeten verklaren dat de onderneming een adequaat systeem voor 'internal control over financial reporting' en 'disclosure controls'⁹ heeft ingericht. De jaarrekening en toelichting dienen in elk materieel opzicht een 'getrouwe weergave' te vormen van de resultaten en de financiële positie van de onderneming. Tevens moeten zij verklaren dat alle 'wezenlijke tekortkomingen' in opzet of werking van het systeem van interne beheersing aan de accountant en de audit commissie zijn bekendgemaakt. *Sectie 404* verlangt een verklaring van het bestuur over de opzet en werking van het systeem van interne beheersing voor financiële verslaggeving. Jaarlijks dient de ondernemingsleiding een rapport over de interne beheersing op te stellen waarin de verantwoordelijkheid van het management vermeld wordt voor het opzetten en in stand houden van een adequaat systeem van interne beheersing en procedures voor de financiële verslaggeving. Tevens is een beoordeling per het einde van het boekjaar opgenomen van de effectiviteit van de interne beheersingsmaatregelen van de onderneming voor de financiële verslaggeving.

De controlerend accountant dient deze verklaringen van het management te bevestigen en te vermelden in zijn rapport.

Belangrijk is de constatering dat het COSO-raamwerk een brede interne beheersingsdoelstelling hanteert, terwijl SOX zich beperkt tot de betrouwbaarheid van de financiële rapportage.

In het Verenigd Koninkrijk is de *Turnbull Guidance on Internal Control* ontwikkeld¹⁰. Hierin treffen we een intern beheersingsraamwerk aan met een brede scope, vergelijkbaar met COSO. Ook hanteert de *Turnbull Guidance* dezelfde 3 doelstellingen als het COSO-IC raamwerk. De *Turnbull Guidance* vraagt om een beschrijving van de belangrijkste kenmerken van het internal control systeem inzake alle risicogebieden, namelijk financiële rapportage, operationele en compliance risico's. Het management hoeft voorts alleen te verklaren dat zij hiervoor verantwoordelijk is en dat een review van de effectiviteit is uitgevoerd. De controlerend accountant heeft hierin geen verantwoordelijkheid zoals in de Verenigde Staten.

Hieruit kan worden afgeleid dat de eisen zoals gesteld in de *Turnbull Guidance* minder vergaand zijn dan de hiervoor beschreven SOX-wetgeving.

⁸ Sampers (2005), Het in control statement, Eerste aanzet tot bestuursverklaring inzake interne beheersing voor Nederlandse beursfondsen. Maandblad voor Accountancy en Bedrijfseconomie, juli/augustus.

⁹ Sampers (2005), pagina 364.

¹⁰ Financial Reporting Council, Internal Control, revised guidance for directors on the combined code, October 2005.



2.2 Code Tabaksblat

Op 10 maart 2003 werd de Commissie Corporate Governance geïnstalleerd. Deze commissie publiceerde in december 2003 de Nederlandse corporate governance code, hierna de Code Tabaksblat. In hoofdstuk twee van de Code Tabaksblat wordt nader ingegaan op de taak en werkwijze van het bestuur. Hierover zegt de Code Tabaksblat het volgende:

“II.1 Taak en werkwijze

Het bestuur is belast met het besturen van de vennootschap, hetgeen onder meer inhoudt dat hij verantwoordelijk is voor de realisatie van de doelstellingen van de vennootschap, de strategie en het beleid en de daaruit voortvloeiende resultatenontwikkeling. Het bestuur legt hierover verantwoording af aan de raad van commissarissen en aan de algemene vergadering van aandeelhouders. Het bestuur richt zich bij de vervulling van zijn taak naar het belang van de vennootschap en de met haar verbonden onderneming en weegt daartoe de in aanmerking komende belangen van bij de vennootschap betrokkenen af. Het bestuur verschaft de raad van commissarissen tijdig alle informatie die nodig is voor de uitoefening van de taak van de raad van commissarissen. Het bestuur is verantwoordelijk voor de naleving van alle relevante wet- en regelgeving, het beheersen van de risico's verbonden aan de ondernemingsactiviteiten en voor de financiering van de vennootschap. Het bestuur rapporteert hierover aan en bespreekt de interne risicobeheersings- en controlesystemen met de raad van commissarissen en zijn auditcommissie.”

Volgens de Code Tabaksblat is het bestuur verantwoordelijk voor adequaat functionerende risicobeheersings- en controlesystemen binnen de onderneming. De Code werkt deze verantwoordelijkheid uit in best practice bepalingen II.1.3 en II.1.4:

“II.1.3 In de vennootschap is een op de vennootschap toegesneden intern risicobeheersings- en controlesysteem aanwezig. Als instrumenten van het interne risicobeheersings- en controlesysteem hanteert de vennootschap in ieder geval:

- a) risicoanalyses van de operationele en financiële doelstellingen van de vennootschap;
- b) een gedragscode die in ieder geval op de website van de vennootschap wordt geplaatst;
- c) handleidingen voor de inrichting van de financiële verslaggeving en de voor de opstelling daarvan te volgen procedures;
- d) een systeem van monitoring en rapportering.

II.1.4 In het jaarverslag verklaart het bestuur dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn en geeft het 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.”

In de toelichting van de Code is verder opgenomen: “Het ligt in de rede dat het bestuur in de verklaring over de interne risicobeheersings- en controlesystemen aangeeft welk raamwerk of normenkader (zoals het COSO-raamwerk voor interne beheersing) het heeft gehanteerd bij de evaluatie van het interne risicobeheersings- en controlesysteem.” Omdat de Code verwijst naar het COSO-raamwerk betekent dit dat de oorspronkelijke scope van de verklaring over interne risicobeheersings- en controlesystemen breed is. Een dergelijke verklaring gaat dus verder dan een ‘in control’-verklaring ten aanzien van financiële verslaggeving. In vergelijking met SOX kent de Code Tabaksblat vergaande eisen op het gebied van risicomanagement en risicoverslaggeving. De ‘in control’-verklaring die het bestuur op grond van best practice bepaling II.1.4 moet afleggen omvat zowel de verklaring en onderbouwing dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn als een rapportage over ‘de gevoeligheid van de resultaten van de vennootschap ten aanzien van externe omstandigheden en variabelen’ (de Groot et al., 2006)¹¹. Sampers (2005) concludeert dat een tegenstelling lijkt te bestaan tussen het hanteren van een brede definitie en de eis om tot een specifieke ‘in control’-verklaring te komen¹². Mede naar aanleiding van de onduidelijkheid die hierover ontstond bij de implementatie van deze best practice bepalingen is de Monitoring Commissie met aanvullende bepalingen gekomen.

¹¹ De Groot, Kuijl en Scheffe (2006).

¹² Sampers (2005).



2.3 Monitoring Commissie Corporate Governance

In haar nalevingsrapport van 2005 heeft de Monitoring Commissie uitvoerig stilgestaan bij de toepassing van best practice bepaling II.1.4. Sinds het verschijnen van de Code bestaat discussie over de reikwijdte van de zogenaamde 'in control'-verklaring (best practice bepaling II.1.4). De Monitoring Commissie schrijft daarover het volgende:

“De Code Tabaksblad combineert in de gevraagde verklaring een brede reikwijdte van de risico's zoals in Turnbull met de eis dat ten aanzien van deze risico's de risicobeheersing- en controlesystemen adequaat en effectief zijn, zoals in SOX vereist wordt ten aanzien van financiële verslaggeving risico's. Naast interne beheersingsmaatregelen over financiële informatie is voor investeerders (zo blijkt ook uit de Turnbull Review) ook informatie over de andere doelstellingen van COSO van belang. Om zoveel mogelijk aan te sluiten bij internationaal gangbare best practices en heersende opvattingen over de praktische uitwerking daarvan ligt het naar het oordeel van de Commissie in de rede om in de verklaring van het management uit hoofde van II.1.4 te differentiëren naar soort risico in die zin dat ten aanzien van financiële verslaggeving risico's het management met een “redelijke mate van zekerheid” verklaart dat de beheersingssystemen adequaat en effectief zijn terwijl ten aanzien van operationele en compliance risico's de beheersingssystemen op hoofdlijnen worden beschreven”.¹³

Op basis van haar onderzoek naar de jaarverslagen 2004 komt de Monitoring Commissie tot de conclusie dat beursvennootschappen en beleggersorganisaties behoefte hebben aan meer guidance ten aanzien van de verklaring van adequaatheid en effectiviteit. Dit heeft geleid tot een aantal aanbevelingen (*good practices*) omtrent de toepassing van best practice bepaling II.1.4. Naar haar mening voldoen ondernemingen aan best practice bepaling II.1.4 als:

“1. Ten aanzien van financiële verslaggeving risico's:

- wordt verklaard dat de risicobeheersings- en controlesystemen een redelijke mate van zekerheid geven dat de financiële verslaggeving geen onjuistheden van materieel belang bevat;
- wordt verklaard dat de risicobeheersings- en controlesystemen in het verslagjaar naar behoren hebben gewerkt;
- wordt verklaard dat er geen indicaties zijn dat de risicobeheersings- en controlesystemen in het lopende jaar niet naar behoren zullen werken;
- eventuele tekortkomingen die mogelijk materiële gevolgen kunnen hebben en in het verslagjaar respectievelijk het lopende jaar zijn geconstateerd worden gemeld, waarbij tevens aangebrachte of geplande verbeteringen worden aangegeven.

2. Ten aanzien van andere risico's (operationele/strategische risico's en wet- en regelgeving risico's):

- een beschrijving van de risicobeheersings- en controlesystemen op basis van de geïdentificeerde belangrijke risico's wordt gegeven;
- indien van toepassing, belangrijke tekortkomingen die in het verslagjaar zijn geconstateerd worden gemeld, waarbij tevens aangebrachte of geplande verbeteringen worden aangegeven.

Voor wat betreft de inhoud van een 'redelijke mate van zekerheid' dient uitgegaan te worden van wat als zodanig geldt voor een zorgvuldig handelend bestuurder in de gegeven omstandigheden”.¹⁴

Met deze nadere invulling van best practice bepaling II.1.4 denkt de Monitoring Commissie beter aan te sluiten bij de internationale praktijk, en door in de 'in control'-verklaring een gedifferentieerd oordeel aan te bevelen de bruikbaarheid van de Code Tabaksblad te vergroten. Wat opvalt bij deze nadere invulling is dat enerzijds de scope van de 'in control'-verklaring vooral wordt toegespitst op de risico's met betrekking tot de financiële verslaggeving, maar dat anderzijds de periode waarover het bestuur dient te verklaren is opge-rekt door daar ook het lopende jaar in te betrekken. In die zin wordt een uitspraak gedaan over de toekomst, namelijk over de werking van de interne risico- en beheersingssystemen in het resterende deel van het jaar waarin het bestuur verklaart 'in control' te zijn.

¹³ Monitoring Commissie Corporate Governance (2005), Rapport over de naleving van de Nederlandse corporate governance code, pagina 52.

¹⁴ Monitoring Commissie Corporate Governance (2005), Rapport over de naleving van de Nederlandse corporate governance code, pagina 64.



Voor de overige risico's kan worden volstaan met het geven van een beschrijving. Vanuit bestuurders-aansprakelijkheid gezien lijkt een dergelijke verklaring minder risico's met zich mee te brengen¹⁵.

In haar nalevingsrapport van december 2007 - over het boekjaar 2006 - constateert de Monitoring Commissie dat de naleving op het gebied van interne risicobeheersing weliswaar licht is verbeterd ten opzichte van 2005, maar ziet zij desondanks ruimte voor verdere verbetering van met name de beschrijving van strategische, operationele, financiële en wet- en regelgevingsrisico's.¹⁶ Derhalve formuleert zij in haar rapport aanvullende aanbevelingen voor de beschrijving van het risicoprofiel en het interne risicobeheersings- en controlesysteem:

“Beschrijving van het risicoprofiel

In de beschrijving van het risicoprofiel geeft de onderneming aan met welke risico's zij in aanraking komt bij het uitvoeren van haar strategie. De onderneming geeft daarnaast aan welke risico's zij bereid is te nemen om haar doelstellingen te realiseren en kwantificeert deze zo mogelijk, door middel van een gevoeligheidsanalyse.

In de beschrijving wordt ten minste aandacht besteed aan:

- de voornaamste risico's gerelateerd aan de strategische doelstellingen van de onderneming,
- alsmede de houding ten opzichte van deze risico's (*risk appetite*);
- een beschrijving van de voornaamste strategische, operationele, financiële, wet- en regelgeving en financiële verslaggevingsrisico's van de onderneming, waarbij in ieder geval de kwalitatieve impact van deze risico's wordt beschreven;
- een gevoeligheidsanalyse van de geïdentificeerde risico's, indien deze analyse redelijkerwijs verwacht mag worden gelet op de 'best practices' in de desbetreffende sector.

Uit de beschrijving van het interne risicobeheersings- en controlesysteem moet blijken welke acties de vennootschap heeft ondernomen om de geïdentificeerde risico's te beheersen. Het gaat hierbij niet alleen om het systeem zelf, maar ook om de inbedding ervan in de organisatie. Het verdient aanbeveling de volgende punten te bespreken:

- de risico's die door het interne risicobeheersings- en controlesysteem worden beheerst en zonodig het referentiemodel dat is gebruikt om het systeem te ontwerpen;
- de organisatie van het interne risicobeheersings- en controlesysteem en de inbedding daarvan in de organisatie;
- de resultaten van een periodiek te verrichten evaluatie van het interne risicobeheersings- en controlesysteem en, voor zover van toepassing, de naar aanleiding daarvan getroffen verbetermaatregelen¹⁷.

De aanbevelingen van de Monitoring Commissie zijn eind 2007 gepubliceerd. In het empirische deel van dit onderzoek zal onder andere worden onderzocht in hoeverre ondernemingen in hun verslaggeving over het boekjaar 2007 de aanbevelingen van de Monitoring Commissie hebben opgevolgd.

Op 4 juni 2008 is de Monitoring Commissie met voorstellen gekomen voor aanpassing van de Code.¹⁸ Deze zijn gebaseerd op de aanbevelingen in de drie nalevingsrapporten en het advies van de Commissie aan het kabinet van mei 2007, met inachtneming van de relevante ontwikkelingen op het terrein van corporate governance sinds de inwerkingtreding van de Code in 2004. Op de voorstellen van de Commissie kan tot 15 september 2008 worden gereageerd. In december 2008 wordt naar verwachting de aangepaste Code vastgesteld en gevraagd deze wettelijk te verankeren.

In het kader van dit onderzoek worden in deze paragraaf de voorstellen besproken die betrekking hebben op het onderwerp risicomanagement.

¹⁵ De Groot, Kuijl en Scheffe (2006).

¹⁶ Deze vier onderdelen zijn identiek aan de onderdelen zoals genoemd in het COSO-ERM raamwerk.

¹⁷ Monitoring Commissie (2007), Derde rapport over de naleving van de Nederlandse corporate governance code, pagina 7-8.

¹⁸ Monitoring Commissie Corporate Governance Code, Rapport over de evaluatie en actualisering van de Nederlandse corporate governance code, juni 2008 (www.corpgov.nl).



Op pagina 47 van het rapport schrijft de Commissie:

“Ten aanzien van de aanbevelingen die de Monitoring Commissie in 2005 en 2007 heeft gedaan over de toepassing interne risicobeheersing heeft de Monitoring Commissie geen reacties ontvangen die tot nieuwe inzichten hebben geleid. De Commissie meent daarom dat de aanbevelingen als volgt in de best practice bepalingen II 1.4, II.1.4a (nieuw) en III.1.8 kunnen worden geïncorporeerd.

II.1.4 In het jaarverslag geeft het bestuur:

- a) een beschrijving van de opzet en werking van de interne risicobeheersings- en controlesystemen met betrekking tot de voornaamste risico's zoals die zich in het boekjaar konden voordoen;
- b) een beschrijving van eventuele belangrijke tekortkomingen in de interne risicobeheersings- en controlesystemen die in het boekjaar zijn geconstateerd en welke eventuele significante wijzigingen in die systemen zijn aangebracht, welke eventuele belangrijke verbeteringen van de systemen zijn gepland en dat één en ander met de auditcommissie en de raad van commissarissen is besproken.

Het bestuur geeft hiervan een duidelijke onderbouwing.

II.1.4a. Ten aanzien van financiële verslaggevingsrisico's verklaart het bestuur in het jaarverslag:

- a) dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn en een redelijke mate van zekerheid geven dat de financiële verslaggeving geen onjuistheden van materieel belang bevat;
- b) dat de risicobeheersings- en controlesystemen in het verslagjaar naar behoren hebben gewerkt,
- c) dat er geen indicaties zijn dat de risicobeheersings- en controlesystemen in het lopende jaar niet naar behoren zullen werken.

Het bestuur geeft hiervan een duidelijke onderbouwing.

De Monitoring Commissie meent dat het niet nodig is de aanbevelingen die in het derde rapport zijn opgesteld voor de beschrijving van het risicoprofiel en de interne risicobeheersings- en controlesystemen integraal in een Codebepaling te vervatten. Deze aanbevelingen blijven niettemin van belang voor de invulling van de Codebepalingen en zullen daarom als toelichting bij de bovenstaande Codebepaling kunnen worden opgenomen.

III.1.8 De raad van commissarissen bespreekt in ieder geval één maal per jaar de strategie en de voornaamste risico's verbonden aan de onderneming en de uitkomsten van de beoordeling door het bestuur van de opzet en werking van de interne risicobeheersings- en controlesystemen alsmede de significante wijzigingen hierin. Van het houden van de besprekingen wordt melding gemaakt in het verslag van de raad van commissarissen.”

De belangrijkste conclusie is dat de Commissie in haar voorstel voor wijziging van de Code een belangrijk deel van haar aanbevelingen buiten de Code wil houden. Zij acht het niet nodig de aanbevelingen integraal in een Codebepaling te vervatten, maar stelt voor om deze als toelichting bij de Codebepaling op te nemen. Best practice bepaling II.1.4 heeft een bredere scope en vraagt onder meer een beschrijving van de opzet en werking van de interne risicobeheersings- en controlesystemen met betrekking tot de voornaamste risico's zoals die zich in het boekjaar konden voordoen. Best practice bepaling II.1.4a bevat de 'in control'-verklaring, die zich beperkt tot de financiële verslaggevingsrisico's. Vooralsnog kan worden geconcludeerd dat de aanpassingen zoals voorgesteld door de Commissie niet zullen leiden tot majeure wijzigingen.

2.4 Speerpuntenbrief Eumedion

Op 8 november 2007 publiceerde Eumedion haar speerpuntenbrief 2008. Daarin heeft Eumedion voor 2008 één speerpunt gedefinieerd dat specifiek betrekking heeft op de bedrijfsstrategie en het risicomanagement van de beursgenoteerde ondernemingen. Eumedion verwoordt haar speerpunt als volgt:¹⁹

¹⁹ Zie bijlage A.



“1. Speerpunt: bedrijfsstrategie en risicomanagement

Ondernemers moeten ondernemingskansen blijven nemen. Onlosmakelijk hoort het nemen van ondernemingsrisico's daarbij. Aandeelhouders vragen om een heldere en overtuigende strategie, waarbij naast de strategische kansen de aan deze strategie verbonden risico's inzichtelijk worden gemaakt en de beheersmaatregelen die daarop van toepassing zijn.

Aandeelhouders willen kortom graag antwoord op de vragen:

- i) wat is de middellange en lange termijn strategie?;
- ii) op welke kansen zet de onderneming bewust in?;
- iii) welke risico's zijn aan de strategie verbonden, wat is de kans dat deze risico's zich voordoen en wat is de omvang daarvan in termen van impact op resultaat en eigen vermogen? Institutionele beleggers hebben behoefte aan een overzicht van de, zeg vijf, belangrijkste risico's in plaats van een vermelding van alle denkbare risico's;
- iv) hoe zien de interne risicobeheersings- en controlesystemen er uit en welke procedures zijn er?;
- v) welke aanpassingen en verbeteringen zijn in het afgelopen boekjaar in deze systemen doorgevoerd en worden in het lopende boekjaar nog doorgevoerd? Waar zitten nog tekortkomingen en wat heeft prioriteit in aanpak?

Aandeelhouders hebben vanuit dit oogpunt meer behoefte aan een 'brede risicoparagraaf' dan aan een algemene bestuursverklaring over de beheersing van de financiële verslaggevingsrisico's, zoals deze zich in de afgelopen jaren heeft ontwikkeld. Eumedion constateert dat de beschrijving van de interne risicobeheersings- en controlesystemen ten aanzien van de belangrijkste (strategische en operationele) risico's weinig informatief is of dat een beschrijving in haar geheel ontbreekt. De ervaring leert echter dat juist de strategische en operationele risico's debet waren aan deconfitures, bijna deconfitures of strategisch falen van ondernemingen in de afgelopen decennia hetgeen het belang van inzicht in deze risico's onderstreept. Daarnaast constateert Eumedion dat de risico's, ook de financiële, slechts in een beperkt aantal gevallen worden gekwantificeerd en dat de rapportages over de risico's en het risicobeheer verspreid zijn opgenomen in het jaarverslag en in de jaarrekening.

Eumedion zou graag zien dat in het jaarverslag over boekjaar 2007 een informatieve en inzichtelijke brede risicoparagraaf in het jaarverslag wordt opgenomen, waarin **alle** gegevens ten aanzien van risico's en risicobeheer geconcentreerd op die plek in het jaarverslag zijn opgenomen. Voor alle duidelijkheid: de deelnemers van Eumedion vinden deze informatie van een groter belang dan de verklaring die het bestuur opstelt over de effectiviteit en adequaatheid van de interne risicobeheersings- en controlesystemen ten aanzien van de financiële verslaggevingsrisico's.”

De door Eumedion naar voren gebrachte vragen worden, evenals de aanbevelingen van de Monitoring Commissie en de best practice bepalingen van de Code Tabaksblat, meegenomen in het inventariserend onderzoek.²⁰

2.5 Overige relevante wet- en regelgeving

Tot besluit van dit hoofdstuk wordt aandacht besteed aan enkele belangrijke Europese ontwikkelingen op het terrein van wet- en regelgeving die invloed zullen hebben op corporate governance, meer in het bijzonder op verslaggeving over risico's en beheersingsmaatregelen.

Met ingang van 2005 moeten beursgenoteerde ondernemingen hun jaarrekening opstellen op basis van internationale verslaggevingsstandaarden, de zogenaamde IFRS (International Financial Reporting Standards). IFRS 7 behandelt de informatieverschaffing met betrekking tot financiële instrumenten. Deze IFRS heeft tot doel om lezers van een jaarrekening in staat te stellen om te beoordelen wat de aard en omvang is van uit financiële instrumenten voortvloeiende risico's en de wijze waarop deze risico's door de onderneming worden beheerst. Deze risico's (ontstaan uit financiële instrumenten) omvatten met name kredietrisico's, liquiditeitsrisico's en marktrisico's. Ondernemingen zijn derhalve verplicht om deze informatie in de toelichting op de jaarrekening op te nemen.

²⁰ Voor zover de informatie aspecten die door Eumedion worden gewenst te scoren zijn op basis van aanwezigheid in de verslaggeving van ondernemingen deze meegenomen. De scope van het onderzoek is echter beperkt door geen daadwerkelijke beschrijvingen van bijvoorbeeld middellange en lange termijn strategie op te nemen (vraag i). Dit geldt ook voor de tweede vraag (ii) in de speerpunten-brief.



Op 27 september 2004 gaf de Europese Commissie goedkeuring aan een mededeling betreffende het voorkomen en bestrijden van financiële wanpraktijken van ondernemingen. Hierin wordt onder andere een beeld geschetst van de beleidsinitiatieven van de Europese Commissie ten aanzien van de interne controle bij ondernemingen en de verantwoordelijkheid van de leden van de bestuurs-, leidinggevende en toezicht houdende organen. Aangekondigd werd om op dit laatste vlak een richtlijn op te stellen. Deze richtlijn werd in 2006 door de Europese Raad en het Europees Parlement vastgesteld (Richtlijn 2006/46/EG).

Richtlijn 2006/46/EG verplicht beursgenoteerde vennootschappen om een verklaring inzake corporate governance op te nemen, hetzij in een specifiek deel van het jaarverslag, hetzij in een afzonderlijk verslag dat samen met het jaarverslag wordt gepubliceerd.

Deze verklaring dient de aandeelhouders op zijn minst belangrijke, gemakkelijk toegankelijke informatie te verschaffen over de feitelijk toegepaste corporate governance praktijken, met inbegrip van een beschrijving van de belangrijkste kenmerken van eventuele bestaande risicobeheersingssystemen en interne controles met betrekking tot het proces van financiële verslaggeving. In de verklaring inzake corporate governance moet duidelijk worden gemaakt of de onderneming andere corporate governance bepalingen toepast dan voorzien in het nationale recht, ongeacht de vraag of deze bepalingen rechtstreeks zijn vastgelegd in een corporate governance code waaraan een onderneming is onderworpen en ongeacht welke corporate governance code de onderneming heeft besloten toe te passen.

Bovendien kunnen ondernemingen een analyse van sociale en milieuaspecten verschaffen als dat nodig is voor het inzicht in de ontwikkeling, resultaten en positie van de onderneming. Het is niet nodig om een aparte verklaring inzake corporate governance op te leggen aan ondernemingen die een geconsolideerd jaarverslag opstellen, maar er dient informatie inzake interne controle- en risicobeheerssystemen van de groep te worden verstrekt.

Daarbij dient de corporate governance verklaring, naast corporate governance aspecten, onder andere een toelichting te geven op de volgende risicomangement onderwerpen (Richtlijn 2004/39/EG):²¹

“Een beschrijving van de belangrijkste kenmerken van de interne controle- en risicobeheerssystemen van de vennootschap, in verband met het proces van financiële verslaggeving”.

De Europese Richtlijn moet vóór 5 september 2008 zijn geïmplementeerd in de Nederlandse wet- en regelgeving. Op het moment van afronden van dit onderzoek was nog geen wetsvoorstel bij de Tweede Kamer ingediend.

²¹ Zie bijlage B



3 Dataselectie en onderzoeksaanpak

3.1 Dataselectie en samenstelling onderzoekspopulatie

Het onderzoek richt zich op Nederlandse beursgenoteerde ondernemingen die hun statutaire zetel in Nederland houden. Deze ondernemingen zijn onderworpen aan de Code en worden derhalve in het empirisch onderzoek betrokken. Als peildatum is 1 januari 2008 gekozen. In de definitieve selectie is een aantal ondernemingen uitgesloten. Ondernemingen met een buitenlandse statutaire zetel worden niet meegenomen (zoals Shell en ArcelorMittal). Tevens is besloten om alle ondernemingen uit te sluiten waarvan de publicatie van het jaarverslag na 15 mei 2008 plaats heeft. Dit vanwege het feit dat het onderzoeksrapport eind mei beschikbaar moest zijn. Tevens is één onderneming uitgesloten vanwege het feit dat haar boekjaar eindigt op 30 juni. Derhalve is deze onderneming niet in staat geweest de laatste (december 2007) aanbevelingen van de Monitoring Commissie mee te nemen bij het opstellen van haar meest recente jaarverslag. Tenslotte is een onderneming uitgesloten waarvan de beursnotering begin dit jaar werd beëindigd in verband met een overname. De definitieve onderzoekspopulatie omvat 110 ondernemingen, allen genoteerd aan Euronext Amsterdam.

AEX	AMX	AScX	Overige	Overige
AEGON	Aalberts Industries	Ballast Nedam	Accell Group	Holland Colours
Ahold	AMG	Beter Bed	Acomo	ICT Automatisering
AkzoNobel	ARCADIS	Brunel	AMT	Jetix Europe
ASML	ASM International	ERIKS	AND International	KAS Bank
Corio	BAM	Exact	Publishers	Kendrion
Corporate Express	BinckBank	Grontmij	Batenburg Beheer	Reesink
DSM	Boskalis Westminster	Macintosh Retail Group	BE Semiconductor	Middle Europe Real
Fortis	Crucell	Nieuwe Steen Investments	Industries	Estate
Heineken	CSM	OPG Groep	Bever Holding	Neways Electronics
ING Groep	Draka	Pharming	Blue Fox Enterprises	International
KPN	Fugro	Qurius	Brill	Nyloplast
Philips Electronics	Heijmans	Sligro Food Group	Crown Van Gelder	Oranjewoud
Randstad	Imtech	Smit International	Ctac	Porceleyn Fles
Reed Elsevier	Nutreco	Super de Boer	DNC	Punch Graphix
SBM Offshore	Océ	Telegraaf Media Groep	DOCDATA	Rood Testhouse
Tele Atlas	Ordina	Ten Cate	DPA Flex	International
TNT	SNS Reaal	TKH Group	Econosto	RSDB
TomTom	USG People	Unit 4 Agresso	Exendis	Samas
Unilever	VastNed Retail	Van der Moolen	Fornix BioSciences	Schuitema
Vedior	Vopak	Van Lanschot	Gamma Holding	Simac
Wolters Kluwer	Wavin	VastNed Offices Industrial	Gouda Vuurvast	Spyker Cars
	Wessanen		Groothandelsgebouwen	Stern Groep
	Wereldhave		Hagemeyer	TIE Holding
			HES Beheer	TMC
			HITT	Wegener

Tabel 3.1 Definitieve onderzoekspopulatie

Van elk van deze 110 ondernemingen zijn de volgende publieke bronnen geraadpleegd:

- het jaarverslag over 2007;
- de website (corporate governance deel).



3.2 Onderzoeksaanpak

Dit onderzoek heeft als primaire doel te inventariseren hoe ondernemingen rapporteren over hun risico's en beheersingssystemen in het jaarverslag en - voor zover van toepassing - op hun website. Daartoe is met een meetinstrument gewerkt dat omschreven kan worden als een vragenlijst met specifieke vragen ten aanzien van risico's en beheersingssystemen (bijlage C). De vragenlijst dient ertoe om het onderzoeksteam in staat te stellen op een eenduidige manier de jaarverslagen (en websites) van ondernemingen te bestuderen en de relevante informatie op consistente wijze vast te leggen. De items in de vragenlijst zijn hoofdzakelijk samengesteld op basis van:

- de best practice bepalingen van de Code Tabaksblad
- de aanbevelingen van de Monitoring Commissie
- de speerpuntenbrief 2008 van Eumedion

voor zover deze betrekking hebben op risico's en beheersingssystemen.

Voor elke onderneming is aldus een dossier samengesteld met een ingevulde vragenlijst en een hardcopy van de desbetreffende pagina's uit het jaarverslag.

Het onderzoeksteam bestond uit zes personen: twee senior onderzoekers en vier junioren²². Om de consistentie en kwaliteit van het onderzoek te waarborgen is tevens een aantal controles ingebouwd. De individuele resultaten van de onderzoekers zijn onderling en tussentijds regelmatig op consistentie gecontroleerd.

De resultaten van alle vragenlijsten zijn ingevoerd in een database. Het merendeel van de vragen in de vragenlijst betreft gesloten vragen met een binair karakter (ja/nee; wel/niet). Op basis hiervan zijn gemiddelde percentages berekend voor de gehele onderzoekspopulatie en voor de subcategorieën. Daarnaast is ook een aantal open vragen beantwoord en beschreven in het empirische deel (hoofdstuk 4) van dit rapport. In het volgende hoofdstuk worden de resultaten van het onderzoek gepresenteerd.

²² De junior onderzoekers waren ten tijde van het onderzoek allen master studenten Financieel Management aan de Rotterdam School of Management, Erasmus Universiteit. Ze zijn tijdens het onderzoek begeleid door Prof. Dr. G.M.H. Mertens, die tevens de leiding had van het onderzoek gezamenlijk met drs. I.H.C Blij CFA.



4 Resultaten empirisch onderzoek

4.1 Inleiding

In dit hoofdstuk worden de resultaten gepresenteerd van het empirisch onderzoek aangaande de informatieverstrekking omtrent risico's en beheersingssystemen door Nederlandse beursgenoteerde ondernemingen. De opbouw van dit hoofdstuk is als volgt. In de eerste plaats wordt in paragraaf 4.2 aandacht besteed aan de informatie over risico's van de onderneming. De analyse wordt in 4.3 vervolgd met een inventarisatie van de informatie over risicobeheersings- en controlesystemen van de onderneming. Het empirisch onderzoek zal worden besloten in 4.4 met een uiteenzetting over de 'in control'-verklaring die door de ondernemingen is opgenomen in het jaarverslag.

De resultaten van het onderzoek zullen worden uitgesplitst naar AEX, AMX, AScX en Overigen. Op deze wijze wordt inzichtelijk wat de belangrijkste verschillen zijn tussen de verschillende categorieën. Daarnaast zal ook een (ongewogen) gemiddelde score worden weergegeven voor de gehele onderzoekspopulatie.

Voor zover van toepassing zal naast de bespreking van de resultaten tevens een aantal best practice voorbeelden worden toegevoegd. Deze best practices hebben tot doel als leidraad te fungeren voor zowel opstellers als gebruikers van informatie omtrent risico's en beheersingssystemen (in de jaarverslagen). Het belang van inzicht in de huidige verslaggevingspraktijk is groot, temeer daar de verslaggevingsvereisten ook op dit specifieke terrein continu aan verandering onderhevig zijn.²³ Op deze wijze willen wij bijdragen aan de verbetering van de kwaliteit van de verslaggeving op dit terrein.

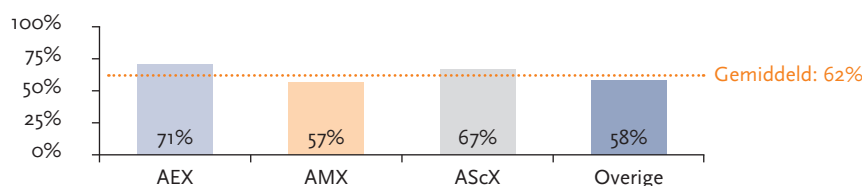
4.2 Informatie over risico's

In deze paragraaf wordt nader ingegaan op de informatie over risico's. Waar van toepassing wordt per vraag verwezen naar de achterliggende bron bijvoorbeeld de speerpuntenbrief van Eumedion of de Code Tabaksblad. De volgende vragen komen achtereenvolgens aan bod:

- Welke zijn de voornaamste risico's gerelateerd aan de strategische doelstellingen van de onderneming?
- Worden deze risico's nader uitgesplitst en zo ja, hoe vindt deze uitsplitsing plaats?
- Worden de belangrijkste (5) risico's geïdentificeerd?
- Is er sprake van een algemene beschrijving van de risico's of een risicobeschrijving toegespitst op de onderneming?
- Vindt er een nadere kwantificering van risico's plaats?
- Voor welke risico's vindt deze kwantificering plaats?
- Wordt informatie verstrekt over de omvang van de risico's in termen van impact op resultaat en eigen vermogen?
- Wordt informatie verstrekt over de kans dat deze risico's zich voordoen?
- Wordt informatie verstrekt over de risicobereidheid (*risk appetite*) van de onderneming?

- a) *Welke zijn de voornaamste risico's gerelateerd aan de strategische doelstellingen van de onderneming? (Monitoring Commissie aanbevelingen december 2007)*

In figuur 4.1 is weergegeven welk deel van de ondernemingen informatie verstrekt die is gerelateerd aan de door de onderneming gedefinieerde strategische doelstellingen. Hieruit blijkt dat het merendeel van de ondernemingen (gemiddeld 62%) aangeeft dat er risico's verbonden zijn aan de strategie. Bij de AEX-fondsen ligt dit percentage het hoogst (71%), gevolgd door de AScX (67%) en de AMX. Verder valt op dat de onderlinge verschillen tussen de groepen klein zijn.



Figuur 4.1 Informatie over risico's gerelateerd aan strategische doelstelling vennootschap

²³ Zoals besproken in hoofdstuk 2.



Het jaarverslag van Grontmij biedt ons inziens een goed voorbeeld van de wijze waarop de risico's worden besproken in relatie tot strategie van de onderneming. In bijlage D: 'Best Practices' is het desbetreffende deel van het jaarverslag opgenomen.

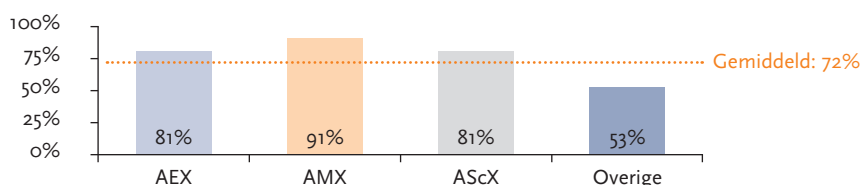
b) Worden deze risico's nader uitgesplitst en zo ja, hoe vindt deze uitsplitsing plaats? (Monitoring Commissie guidance 2005 en aanbevelingen 2007)

Zoals aangegeven in hoofdstuk 2 onderscheidt het COSO-raamwerk een aantal risicocategorieën. De Monitoring Commissie heeft in haar eerste rapport (december 2005) aanbevolen een overzicht te verstrekken van de belangrijkste strategische, operationele, financiële, wet- en regelgeving en financiële verslaggevingsrisico's. In tabel 4.1 staat in welke mate de ondernemingen in hun verslaggeving over de voornaamste risico's aansluiten bij deze categorieën. Opvallend is de hoge score voor operationele en financiële risico's, terwijl wet- en regelgeving en financiële verslaggevingsrisico's duidelijk achterblijven. Een verklaring voor de gevonden verschillen zou kunnen zijn dat ondernemingen van mening zijn dat compliance en verslaggevingsrisico's minder relevant zijn. De AEX-fondsen maken het vaakst melding van alle hier onderscheiden risicocategorieën; naarmate de ondernemingen afnemen in omvang neemt ook de informatieverstrekking af.

	Strategisch	Operationeel	Financieel	Compliance	Financiële Verslaggeving
AEX	57,1%	76,2%	71,4%	57,1%	38,1%
AMX	47,8%	65,2%	73,9%	47,8%	26,1%
AScX	28,6%	52,4%	66,7%	28,6%	23,8%
Overige	22,2%	40,0%	42,2%	8,9%	8,9%
Gemiddeld	35,5%	54,5%	59,1%	30,0%	20,9%

Tabel 4.1 Informatie over gehanteerde risicocategorieën

In figuur 4.2 is vervolgens aangegeven in hoeverre ondernemingen risico's verder uitsplitsen. Volstaan zij met aan te geven dat er sprake is van strategische risico's, of wordt eveneens een nadere onderverdeling daarbinnen aangebracht? Daarbij is als uitgangspunt voor de analyse gekozen voor de categorieën zoals onderscheiden door de Monitoring Commissie. Zoals uit figuur 4.2 blijkt, gaat gemiddeld 72% expliciet in op de hierboven vermelde risicocategorieën. Opvallend is dat de Overigen achterblijven bij het gemiddelde. Opmerkelijk is ook dat de AMX-ondernemingen beter scoren dan de AEX-fondsen. Een mogelijke verklaring kan zijn dat AEX-fondsen vanwege een Amerikaanse beursnotering vaker kiezen voor een uitgebreide beschrijving van alle risico's, waarbij ze geen onderscheid maken naar de verschillende risicocategorieën. Ook blijkt dat een deel van de onderzochte ondernemingen risico's niet nader uitsplitst. Zij volstaan met het beschrijven van enkel de categorieën van risico's die zich kunnen voordoen.



Figuur 4.2 Uitsplitsing van risico's

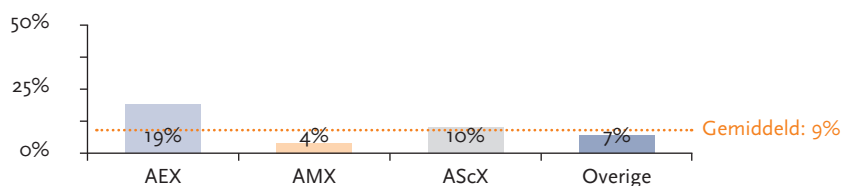
c) Worden de belangrijkste (5) risico's geïdentificeerd? (speerpuntenbrief Eumedion)

Als gevolg van de toegenomen hoeveelheid informatie over de verschillende risico's in de verslaggeving van ondernemingen ontstaat het gevaar dat de risicoparagraaf verwordt tot een opsomming van een lange lijst van risico's. Daardoor wordt het voor de gebruiker van een jaarverslag lastig om een inschatting te maken van de risico's die het meest bedreigend of belangrijk zijn voor een specifieke onderneming. In ons inventariserend onderzoek is daarom nagegaan of ondernemingen expliciet aangeven welke (5) risico's het belangrijkste zijn.²⁴ De resultaten zijn weergegeven in figuur 4.3. Hieruit blijkt dat slechts een beperkt aantal ondernemingen expliciet aangeeft welke risico's de belangrijkste zijn. Gemiddeld één op tien ondernemingen verschaft inzicht in de belangrijkste risico's, voor de AEX-fondsen is dit één op vijf (19%).

²⁴ Conform de oproep van Eumedion in haar speerpuntenbrief.



De Overigen blijven hier voornamelijk duidelijk bij achter. Samenvattend kan worden geconcludeerd dat ondernemingen vrij uitvoerig verslag doen van alle risico's die zijn verbonden aan de onderneming, maar een prioritering van deze risico's ontbreekt in de meeste gevallen.



Figuur 4.3 Uitsplitsing van risico's

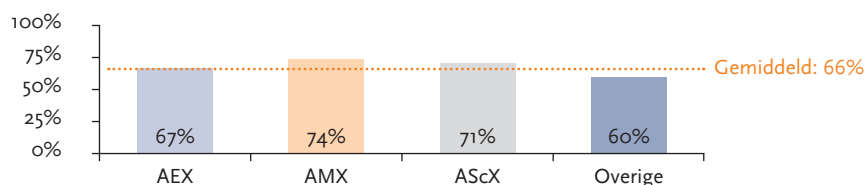
Uit het jaarverslag van Grontmij (pagina 42) is de volgende passage afkomstig:

De belangrijkste risico's die winst en groei kunnen bedreigen bij een advies- en ingenieursbureau zijn:

- looneisen die niet vertaald kunnen worden in hogere tarieven;
- beschikbaarheid van professionals;
- materiële koerswijzigingen met betrekking tot publieke investeringen op alle overheidsniveaus.

d) Is er sprake van een algemene beschrijving van de risico's of een risicobeschrijving toegespitst op de onderneming?

In figuur 4.4 wordt weergegeven in hoeverre de beschreven risico's algemeen worden weergegeven, dan wel de mate waarin bij de bespreking van risico's ingegaan wordt op het specifieke karakter van de onderneming. Een ruime meerderheid van de ondernemingen geeft een specifieke beschrijving, waarbij de risico's worden gekoppeld aan de ondernemingsspecifieke context. De beschrijving hiervan is overigens grotendeels kwalitatief. Daarnaast zien we geregeld een opsomming van een aantal risico's, zonder dat daarbij een relatie met de onderneming wordt gelegd. Dit soort opsommingen komt oblikaat over bij de lezer.

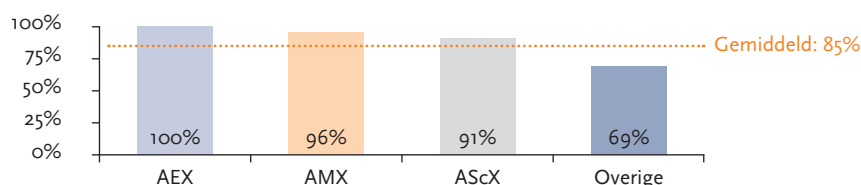


Figuur 4.4 Ondernemingspecifieke risicobeschrijving

Een best practice op dit gebied is te vinden in het jaarverslag van Océ op pagina 74-75. Wij verwijzen hiervoor naar bijlage D: 'Best Practices'.

e) Vindt er een nadere kwantificering van risico's plaats? (speerpuntenbrief Eumedion en Monitoring Commissie aanbevelingen december 2007)

Op basis van de informatie zoals weergegeven in figuur 4.5 kunnen we in de eerste plaats constateren dat 85% van de ondernemingen de (potentiële) effecten van één of meerdere risico's kwantificeert. Voor de AEX-fondsen geldt dit zonder uitzondering, de AMX en AScX volgen hier kort achter en voor de Overigen geldt dat 69% de risico's nader kwantificeert. Dat de scores hier hoog zijn is niet opvallend, indien we rekening houden met de verplichting volgens IFRS om de (met name financiële) risico's nader te kwantificeren (in de toelichting op de jaarrekening).



Figuur 4.5 Mate van kwantificeren van risico's



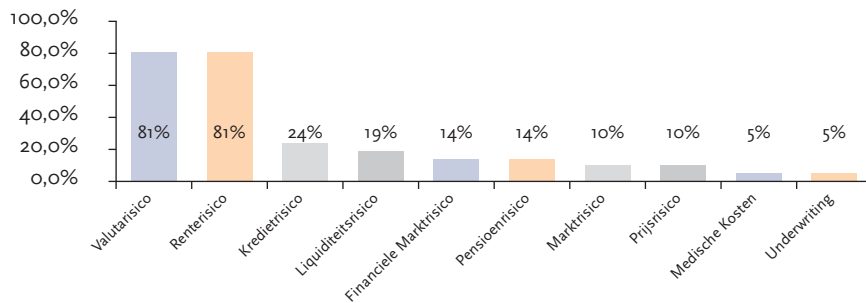
Ter illustratie volgt hieronder een best practice uit het jaarverslag van SNS Reaal (pagina 74) aangaande de kwantificering van risico's.

In miljoenen euro's	Reële waarde eigen vermogen		Resultaat		Eigen vermogen	
	2007	2006	2007	2006	2007	2006
Rente +1%	13	-95	42	-14	-118	-77
Rente -1%	-8	98	-42	14	118	77

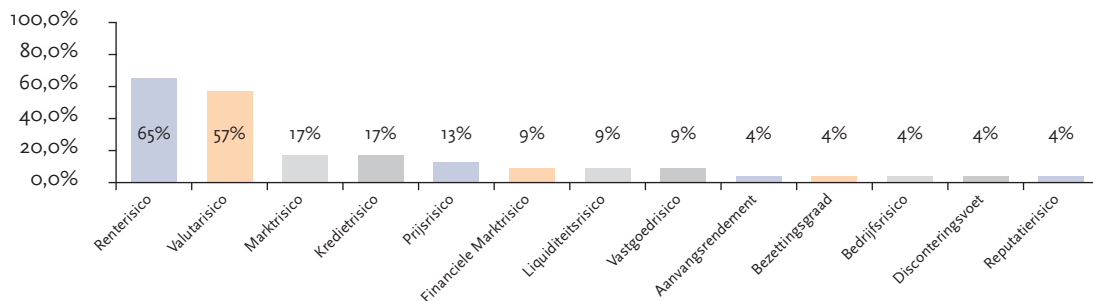
Tabel 19 Rentegevoeligheid SNS Bank

f) Voor welke risico's vindt deze kwantificering plaats?

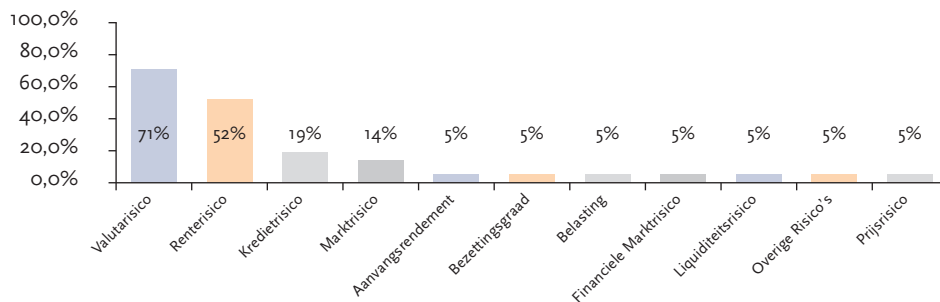
Tevens is het interessant om te inventariseren welke risico's door ondernemingen gekwantificeerd worden, uitgesplitst naar de verschillende categorieën. Figuur 4.6a t/m 4.6d presenteren een compleet overzicht van de belangrijkste soorten risico's die worden gekwantificeerd. Het valt op dat er sprake is van aanzienlijke verschillen in zowel de aantallen als de typen die door de verschillende ondernemingen gerapporteerd worden.



Figuur 4.6a Gekwantificeerde risico's door AEX-fondsen

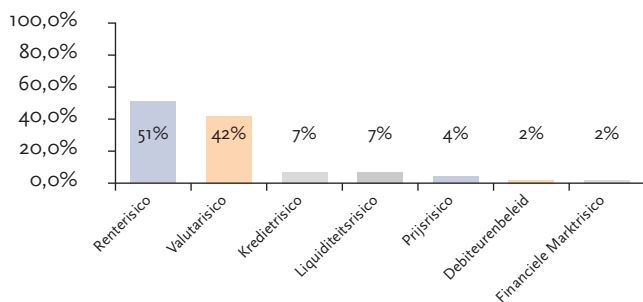


Figuur 4.6b Gekwantificeerde risico's door AMX-fondsen



Figuur 4.6c Gekwantificeerde risico's door AScX-fondsen

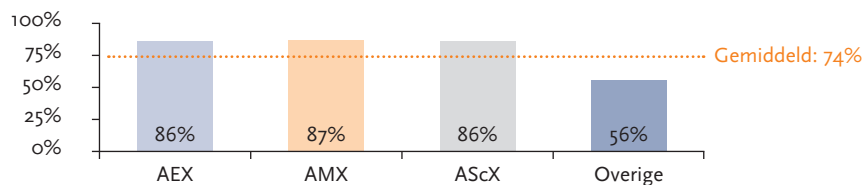




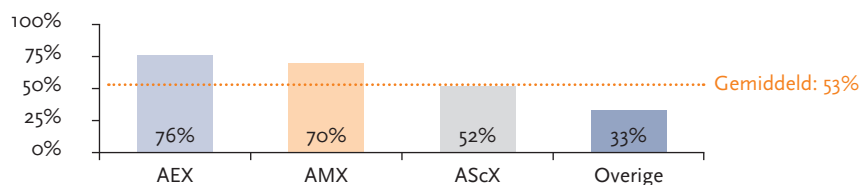
Figuur 4.6d Gekwantificeerde risico's door overige fondsen

g) Wordt informatie verstrekt over de omvang van de risico's in termen van impact op resultaat en op eigen vermogen? (speerpuntenbrief Eumedion)

Vervolgens is onderzocht of het effect van (bepaalde) risico's op het eigen vermogen en/of het resultaat is gekwantificeerd. Figuren 4.7a en 4.7b laten het volgende beeld zien. Bijna driekwart van de ondernemingen verstrekt informatie over het effect op het resultaat; ten aanzien van de impact op het eigen vermogen is dit gemiddelde duidelijk lager (53%). De informatieverstrekking neemt ook hier af naarmate ondernemingen kleiner zijn.



Figuur 4.7a Effect op resultaat



Figuur 4.7b Effect op vermogen

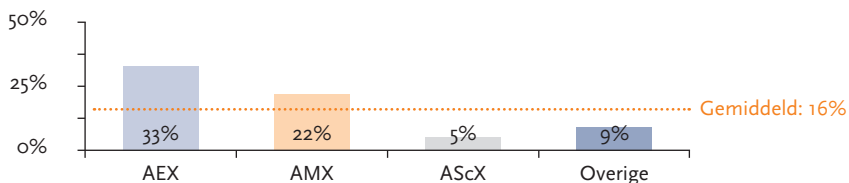
h) Wordt informatie verstrekt over de kans dat deze risico's zich voordoen? (speerpuntenbrief Eumedion)

Geen van de onderzochte ondernemingen heeft bij de gepresenteerde risico's aangegeven wat de kans is op een dergelijk risico. Een mogelijke verklaring hiervoor is dat het voor ondernemingen lastig is om een concrete inschatting te maken van de kans dat een bepaalde situatie zich daadwerkelijk zal voordoen. We constateren op dit punt wel een grote discrepantie ten opzichte van de informatie die wordt verstrekt over en de kwantificering van de risico's. Pas als ondernemingen overgaan tot het verstrekken van informatie over het effect van het risico en de kans dat dit risico optreedt, is het mogelijk om een impactanalyse op te stellen.



i) *Wordt informatie verstrekt over de risicobereidheid (risk appetite) van de onderneming?*
(Monitoring Commissie aanbevelingen december 2007)

Een informatie-element dat vorig jaar voor het eerst door de Monitoring Commissie naar voren werd gebracht in haar aanbevelingen heeft betrekking op de risicobereidheid van de onderneming. Uit de inventarisatie, waarvan de resultaten zijn weergegeven in figuur 4.8, blijkt dat het begrip *risk appetite* nog ingeburgerd dient te raken in de Nederlandse verslaggevingspraktijk. Slechts 16% van de onderzochte ondernemingen geeft een indicatie daarvan in haar risicoparagraaf. Wel zien we dat er sprake is van aanzienlijke verschillen tussen verschillende categorieën ondernemingen: waar een derde van de AEX-fondsen haar *risk appetite* aangeeft, beperkt zich dat tot slechts 5% van de AScX-fondsen.



Figuur 4.8 Vermelden van 'risk appetite'

Een in dit kader goede illustratie van de omschrijving van de *risk appetite* is de navolgende informatie, afkomstig uit het jaarverslag van ING (pagina 21-22):

Maatstaven voor risicotolerantie

De risicotolerantie wordt bij ING aan de hand van drie maatstaven uitgedrukt, namelijk *earnings-at-risk* (EaR), *capital-at-risk* (CaR) en economisch kapitaal. *Earnings-at-risk* is de maatstaf van de potentiële daling van de winst onder IFRS in vergelijking met de verwachte winst, bij een gematigd stress-scenario van 1 op 10 en bij uitblijven van risicoverminderend ingrijpen door het management. Intern wordt de uitkomst afgezet tegen de IFRS-winstprognose voor het komende jaar. De EaR geeft op die manier een indicatie van de kwaliteit van de winst. Het totale risicotolerantieniveau voor ING Groep daalde in 2007 naar 31% in vergelijking met 32% over 2006. Deze daling was het gevolg van een sterkere stijging van de winst dan de EaR. De EaR van ING Bank speelt een bepalende rol in de totale EaR van ING Groep, hoofdzakelijk vanwege het krediet- en transferrisico. Meer informatie over *earnings-at-risk* vindt u in de risicoparagraaf van de jaarrekening.

Capital-at-risk is de potentiële daling van de huidige nettovermogenswaarde (op basis van reële waarde) in de balans in het komende jaar in vergelijking met de verwachte waarde, bij een gematigd stress-scenario van 1 op 10 en bij uitblijven van risicoverminderend ingrijpen door het management. Het CaR-cijfer wordt doorgaans vooral overheerst door ING Verzekeringen en betreft met name het renterisico in verband met langlopende garanties aan klanten en het aandelenrisico. Het totale risicotolerantieniveau voor ING Groep, uitgedrukt in *capital-at-risk*/beschikbare financiële middelen, ging in 2007 omhoog naar 21% (17% in 2006) doordat het CaR sneller groeide dan de beschikbare financiële middelen. Meer informatie over *capital-at-risk* vindt u in de risicoparagraaf van de jaarrekening.

Economisch kapitaal betreft het kapitaal dat gezien de beoogde AA-kredietrating van ING Groep nodig is om onverwachte verliezen in ernstige stress-situaties op te vangen. Het economisch kapitaal van ING Groep steeg naar EUR 36,0 miljard in 2007 (2006: EUR 35,5 miljard), waarbij rekening wordt gehouden met het diversificatievoordeel van de combinatie bankieren en verzekeren en een aan de Groep toegerekend risicokapitaal boven op de gepubliceerde economisch kapitaal-cijfers voor het bank- en verzekeringsbedrijf. Het economisch kapitaal van ING Bank nam toe met 13% tot EUR 17,9 miljard als gevolg van de groei van de activiteiten en de overname van Oyak Bank. Bij ING Verzekeringen was er sprake van een meer bescheiden groei tot 23,2 miljard (2006: 22,4 miljard). De lichte stijging was vooral te danken aan modelaanpassingen en de overname van pensioenactiviteiten in Latijns-Amerika.

De risicomaatstaven van ING Groep betreffen de belangrijkste aspecten op basis van de ernst van de gebeurtenissen (normale versus extreme situaties) en van prestatie maatstaven waar risico kan optreden (waarde ten opzichte van winst). EaR en CaR zijn vanuit het perspectief van de aandeelhouder belangrijke maatstaven omdat zij inzicht bieden in het niveau van het risico dat ING op zich neemt. Vanuit het perspectief van de obligatiehouder is economisch kapitaal daarentegen belangrijker, omdat dit fungeert als het vermogen waarmee onder extreme omstandigheden verliezen moeten worden opgevangen.



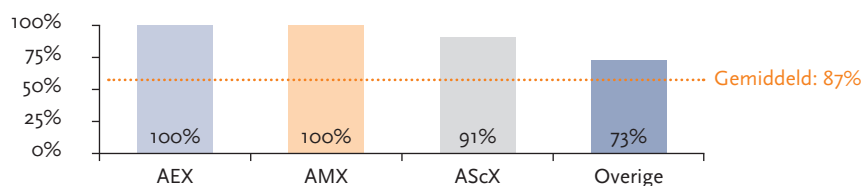
4.3 Informatie over risicobeheersings- en controlesystemen

Nadat in het voorgaande deel de informatie over risico's is geïnventariseerd, zal in deze paragraaf aandacht worden besteed aan de informatie over de risicobeheersings- en controlesystemen. De vragen die in dit kader van belang zijn, luiden als volgt:

- j) Wordt informatie verstrekt over de risicobeheersings- en controlesystemen (inclusief een beschrijving van de procedures)?
- k) Wordt in de beschrijving verwezen naar het werk c.q. de rapportages van de controlerende accountant dan wel de interne accountant/internal auditor of stafdiensten met een controlerende taak?
- l) Wordt de informatie over risico's en risicobeheersings- en controlesystemen op één plaats in het jaarverslag gepresenteerd?
- m) Wordt informatie verstrekt over de resultaten van de periodieke evaluatie van de opzet en werking van de interne risicobeheersings- en controlesystemen inclusief getroffen maatregelen?
- n) Zijn de evaluatie-uitkomsten besproken met de Raad van Commissarissen/Audit Commissie en zo ja, vinden de uitkomsten daarvan hun weerslag in de verslaggeving over de risicobeheersings- en controlesystemen?

j) Wordt informatie verstrekt over de risicobeheersings- en controlesystemen (inclusief een beschrijving van de procedures?) (speerpuntenbrief Eumedion en Monitoring Commissie guidance december 2005)

Ten aanzien van de informatie die wordt verstrekt over de systemen komt het volgende beeld naar voren (zie figuur 4.9). Alle AEX- en AMX-fondsen hebben informatie opgenomen over de systemen en de procedures, maar dat geldt niet voor de AScX en de Overigen (91% resp. 73%). Gemiddeld genomen is de score op dit informatie-element vrij hoog, te weten 87%.



Figuur 4.9 Informatie over systemen en beschrijving procedures

Daarbij dient te worden opgemerkt, dat de aard van de informatieverschaffing en de mate van diepgang van beschrijving van de procedures sterk verschilt. Met name voor de AScX en de Overigen geldt dat informatie over de procedures niet of slechts beperkt aanwezig is.²⁵ Omdat dikwijls wel sprake is van enige beschrijvende informatie over de (werking en aanwezigheid van) systemen, is de overall (gemiddelde) score op dit punt enigszins geflatteerd. Ook binnen de AEX en AMX zijn er echter aanzienlijke verschillen geconstateerd in de mate van informatieverstrekking. Een aantal ondernemingen binnen deze categorieën volstaat eveneens met een vrij summiere beschrijving. Daarentegen zijn er ook ondernemingen die een heldere uiteenzetting geven van hun risicomanagement en interne beheersing en de wijze waarop een en ander is georganiseerd (procedures).

Een best practice op dit gebied is de informatie hierover in het jaarverslag van Nutreco (pagina 68-72). Wij verwijzen hiervoor naar bijlage D: 'Best Practices'.

k) Wordt in de beschrijving verwezen naar het werk c.q. de rapportages van de controlerende accountant dan wel de interne accountant/internal auditor of stafdiensten met een controlerende taak?

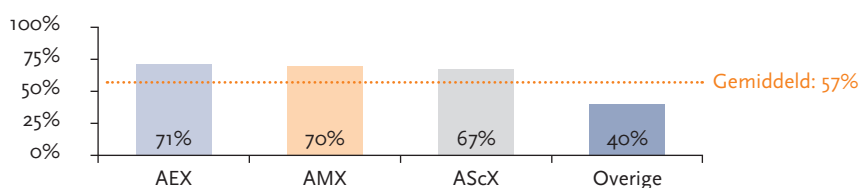
In de controle van de jaarrekeningen van grote ondernemingen betreft de controlerend accountant de kwaliteit van de risicobeheersings- en controlesystemen (met name gericht op financiële verslaggevings-risico's). Veel ondernemingen melden deze werkzaamheden in hun risicoparagraaf. Mede onder invloed van corporate governance ontwikkelingen besluiten beursgenoteerde ondernemingen in toenemende mate om een 'internal audit'-afdeling in te stellen. Deze afdelingen hebben vaak een bepaalde verantwoordelijkheid inzake de kwaliteit van de interne risicobeheersings- en controlesystemen.

²⁵ Zie hiervoor ook vraag (b) die aansluitend zal worden besproken inzake de verwijzing naar de controlerend accountant in de beschrijving.

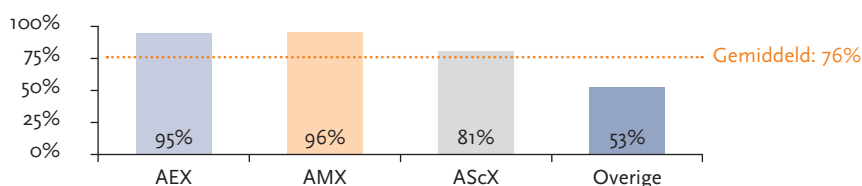


Figuur 4.10 laat zien dat iets meer dan de helft van alle ondernemingen (57%) in haar beschrijving verwijst naar het werk van de controlerende accountant. De scores van de AEX, AMX en AScX liggen niet ver uit elkaar, de overige ondernemingen scoren op dit aspect duidelijk lager. Wat wel opvalt, is dat de rol (en de verantwoordelijkheden) van de externe accountant dikwijls wordt genoemd in het hoofdstuk of onderdeel corporate governance van het jaarverslag. Bij de beschrijving van de procedures, die is opgenomen in de risicoparagraaf van het jaarverslag en onderdeel uitmaakt van de beschrijving van de interne risico- en controlesystemen, zien we een dergelijke verwijzing naar de controlerende accountant minder vaak.

Vervolgens is ook nagegaan bij hoeveel ondernemingen in het jaarverslag wordt verwezen naar de interne accountant/internal auditor of vergelijkbare stafdiensten. Uit figuur 4.11 kan worden afgeleid dat gemiddeld driekwart van alle ondernemingen een dergelijke verwijzing heeft opgenomen. Overigens verwijst het merendeel naar stafdiensten en slechts een beperkt aantal naar een (onafhankelijke) interne accountantsdienst. Ook hier blijven de overige fondsen duidelijk achter; iets meer dan de helft verwijst in de beschrijving van de procedures naar hoofdzakelijk stafdiensten met een controlerende taak.



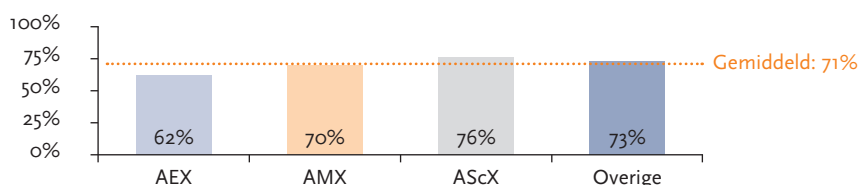
Figuur 4.10 Verwijzing naar controlerend accountant



Figuur 4.11 Verwijzing naar interne accountantsdienst/stafdiensten

l) Wordt de informatie over risico's en risicobeheersings- en controlesystemen op één plaats in het jaarverslag gepresenteerd? (speerpuntenbrief Eumedion en Monitoring Commissie aanbevelingen december 2007)

Omwille van de toegankelijkheid van de informatie is het wenselijk dat de informatie over risico's en risicobeheersings- en controlesystemen terug te vinden is op één plaats in het jaarverslag. Daarom is nagegaan in hoeverre ondernemingen hier gevolg aan geven. De resultaten in figuur 4.12 laten zien dat gemiddeld 71% van de ondernemingen de risico's en de beschrijving van de systemen in een hoofdstuk of onderdeel van hun jaarverslag presenteren.²⁶ Wat opvalt is dat de AScX en de Overigen hier hogere scores behalen dan de AEX- en AMX-ondernemingen. De verklaring is dat de informatie over risico's en de systemen bij grotere ondernemingen (AEX en AMX) uitgebreider en omvangrijker is; daarom wordt er bij deze ondernemingen vaker gekozen voor aparte hoofdstukken of secties in het jaarverslag.



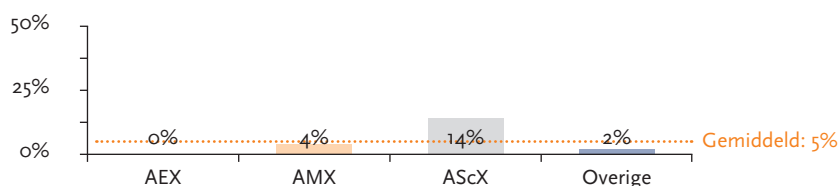
Figuur 4.12 Informatie over risico's en de systemen op een plaats

²⁶ Zoals in hoofdstuk 2 besproken, moeten beursgenoteerde ondernemingen met ingang van 2005 hun jaarrekening opstellen op basis van IFRS (International Financial Reporting Standards). De verplichting uit hoofde van IFRS 7 is in dit onderzoek niet geclassificeerd als een aparte plaats.



m) Wordt informatie verstrekt over de resultaten van de periodieke evaluatie van de opzet en werking van de interne risicobeheersings- en controlesystemen inclusief getroffen maatregelen? (Monitoring Commissie aanbevelingen december 2007)

Eén van de aanbevelingen van de Monitoring Commissie heeft betrekking op het verstrekken van informatie over de resultaten van de periodieke evaluatie van de opzet en werking van de systemen en, voor zover van toepassing, op de getroffen verbetermaatregelen. Zoals uit figuur 4.13 blijkt, resulteert de inventarisatie van dit punt in een lage score. Hoewel in vrijwel alle jaarverslagen melding wordt gemaakt van een periodieke evaluatie, treffen we bij iets minder dan 5% van de ondernemingen daadwerkelijk informatie over de uitkomsten van de evaluatie. Voorts valt op dat géén van de AEX-fondsen informatie over de resultaten heeft weergegeven. De meeste informatie wordt aangetroffen bij de AScX-fondsen; 14% van deze categorie vermeldt informatie in haar jaarverslag over de uitkomsten van de evaluatie en/of eventuele verbetermaatregelen.



Figuur 4.13 Informatie over resultaten en verbeterpunten op basis van periodieke evaluatie

Een voorbeeld van een onderneming die openheid betracht met betrekking tot de resultaten en de verbetermaatregelen is hieronder opgenomen en betreft CSM. In haar jaarverslag treffen we de volgende informatie aan (pagina 47):

Gedurende 2007 zijn diverse activiteiten gestart ter verdere verbetering van de bestaande interne risicobeheersings- en controlesystemen. Deze initiatieven zullen in 2008 worden voortgezet. De belangrijkste zijn:

- het houden van risk management workshops met de divisies en nagenoeg alle werkmaatschappijen, waarbij risico's worden gerangschikt op basis van impact op ons resultaat, de kans dat risico's voorkomen en de maatregelen die wij inmiddels hebben genomen ter beperking van het risico. Op basis hiervan wordt het risicoprofiel van CSM aangepast en waar van toepassing worden maatregelen genomen om de risico's te beperken;*
- het ontwikkelen en implementeren van CSM's "Generic Control Framework" om te komen tot een meer gestructureerde vastlegging van de "Internal Control Structure". In dit kader hebben de belangrijkste werkmaatschappijen de financiële verslaggevingsrisico's en controle activiteiten van de belangrijkste processen beschreven. Als gevolg van de verandering in organisatievorm heeft dit voor de Europese bakkerijdivisie slechts plaatsgevonden voor twee processen: omzet en inkoop. Deze beschrijvingen zijn door de interne accountant beoordeeld en het gedeelte dat betrekking heeft op de jaarrekeningcontrole is tevens door de externe accountant beoordeeld.*

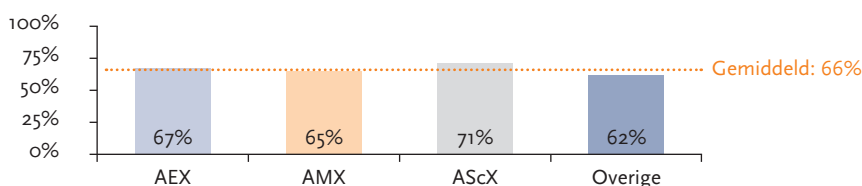
2007 was ook het eerste jaar dat onze interne accountantsdienst zich volledig kon richten op operationele audits en de controle op de jaarrekening volledig aan onze externe accountant werd overgelaten.

Het kwaliteitsniveau van interne beheersing wordt geëvalueerd op basis van de uitkomsten en rapportages van audits van de interne accountant en externe accountant alsmede de maandelijkse rapportages van de werkmaatschappijen en divisies omtrent de financiële en operationele ontwikkelingen en gang van zaken. Bevindingen worden gerapporteerd aan het Audit Committee. In 2007 hebben we in het kader van de financiële verslaggevingsrisico's geconstateerd, dat een aantal controlemaatregelen met betrekking tot onder andere het beheer van stamgegevens, de procedure rond voorraadopnames, de beveiliging van operationele systemen en de continuïteit van IT-systemen verder kunnen worden verbeterd.



n) *Zijn de evaluatie-uitkomsten besproken met de Raad van Commissarissen/Audit Commissie en, zo ja, vinden de uitkomsten daarvan hun weerslag in de verslaggeving over de risicobeheersings- en controlesystemen (Code Tabaksblat best practice bepaling III.1.8 en Monitoring Commissie aanbevelingen 2007)*

In het verlengde van de voorgaande vraag is nagegaan of de evaluatie-uitkomsten zijn besproken met de Raad van Commissarissen en meer specifiek de Audit Commissie. Figuur 4.14 geeft de uitkomsten weer. Gemiddeld 66% van de ondernemingen vermeldt dat de uitkomsten van de evaluaties zijn besproken met de Raad van Commissarissen en de Audit Commissie. Opvallend is dat deze score veel hoger is dan bij de vorige vraag. Met andere woorden, tweederde van alle ondernemingen vermeldt wel dat de evaluaties zijn besproken, maar vermeldt niet wat er is besproken. Deze resultaten duiden erop dat de informatie-verstrekking op dit punt vrij obliagaat is: inhoudelijk worden er weinig tot geen mededelingen gedaan. Tot slot blijkt ook dat de uitkomsten van de evaluatie van de systemen niet in de verslaggeving over risicobeheersings- en controlesystemen zijn opgenomen.



Figuur 4.14 Vindt bespreking van evaluatie-uitkomsten plaats met RvC/Audit Commissie

4.4 'In control'-verklaring

Als derde en laatste onderdeel van dit onderzoek zal worden ingegaan op de 'in control'-verklaring die door de ondernemingen wordt afgegeven. In eerste instantie zal worden aangesloten bij de geldende invulling van het begrip 'in control', dat als uitgangspunt best practice bepaling II.1.4 van de Code kent, aangevuld met de aanbevelingen van de Monitoring Commissie (*good practice*) omtrent de toepassing van dit principe. In paragraaf 4.4.1 worden aldus de volgende informatie-elementen nader onderzocht:

- o) Maakt de 'in control'-verklaring onderdeel uit van de risicoparagraaf? Zo nee, waar is deze verklaring dan wel in het jaarverslag opgenomen?
- p) Is er een verwijzing naar een referentiemodel opgenomen, en zo ja, welk model?
- q) Is er een verwijzing naar best practice bepaling II.1.4 en/of de aanbevelingen van de Monitoring Commissie?
- r) Is er een verwijzing naar SOX sectie 404 opgenomen?
- s) Is er een verwijzing opgenomen naar andere codes voor risicomanagement?

Daarna zal in paragraaf 4.4.2 worden onderzocht of Nederlandse beursgenoteerde ondernemingen een bestuursverklaring hebben opgenomen over de opzet en werking van de interne risicobeheersings- en controlesystemen in brede zin, waarbij die verklaring zich niet enkel beperkt tot risico's en beheersings-systemen met betrekking tot de financiële verslaggeving, maar ook betrekking heeft op strategische, operationele, wet- en regelgeving en financiële risico's. Deze verklaring sluit feitelijk aan bij de oorspronkelijke best practice bepaling II.1.4 van de Code. De volgende vragen zijn onderzocht:

- t) Rapporteert het bestuur over de werking van de risicobeheersings- en controlesystemen in het boekjaar?
- u) Wordt verklaard dat de interne risicobeheersings- en controlesystemen effectief en/of adequaat zijn?
- v) Wordt deze verklaring duidelijk onderbouwd?

Tenslotte worden in paragraaf 4.4.3 de financiële verslaggevingsrisico's nader belicht. De aspecten die hieronder vallen zijn gebaseerd op de aanbevelingen (*good practice*) van de Monitoring Commissie uit haar monitoring rapport van december 2005. Daarbij komen de volgende vragen aan bod:

- w) Wordt door het bestuur verklaard dat de risicobeheersings- en controlesystemen een redelijke mate van zekerheid geven dat de financiële verslaggeving geen onjuistheden van materieel belang bevat?
- x) Wordt verklaard dat de risicobeheersings- en controlesystemen in het verslagjaar naar behoren hebben gefunctioneerd?



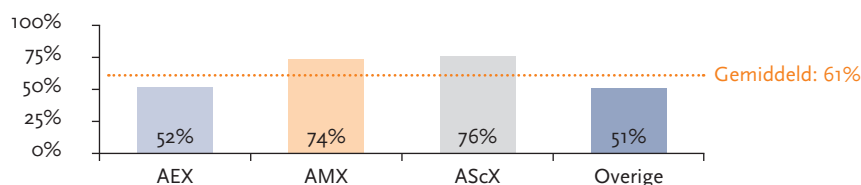
- y) Wordt verklaard dat er geen indicaties zijn dat de risicobeheersings- en controlesystemen in het lopende jaar niet naar behoren zullen werken (*forward looking statement*)?
- z) Worden eventuele tekortkomingen vermeld die materiële gevolgen kunnen hebben en in het verslagjaar respectievelijk het lopende jaar zijn geconstateerd en worden daarbij tevens aangebrachte of geplande verbeteringen aangegeven?

4.4.1 'In control'-verklaring

- o) *Maakt de 'in control'-verklaring onderdeel uit van de risicoparagraaf? Zo nee, waar is deze verklaring dan wel in het jaarverslag opgenomen? (speerpuntenbrief Eumedion en Monitoring Commissie aanbevelingen december 2007)*

Eumedion heeft in haar speerpuntenbrief 2008 aangegeven dat zij voorstander is van het centraal presenteren van alle risicomanagementinformatie in een risicoparagraaf.

In figuur 4.15 is aangegeven in hoeverre de door ondernemingen in het jaarverslag opgenomen 'in control'-verklaring deel uitmaakt van de risicoparagraaf. Gemiddeld 61% van de ondernemingen neemt de 'in control'-verklaring op als onderdeel van de risicoparagraaf, waarbij opvalt dat de score voor AEX-ondernemingen daar duidelijk bij achter blijft. Een mogelijke verklaring is dat we daar meer variatie in de wijze van presenteren zien.



Figuur 4.15 'In-control' verklaring opgenomen als onderdeel risicoparagraaf

In het jaarverslag van TNT (pagina 53) is de volgende verklaring opgenomen:

The Dutch corporate governance code under section 11.1.4 requires the Board of Management to examine strategic, operational, legal and regulatory, financial, and financial reporting risks.

The Board of Management confirms that it is responsible for TNT's risk management, internal control, integrity and compliance systems and has reviewed the operational effectiveness of these systems for the year ended 31 December 2007. The outcome of this review and analysis has been shared with the audit committee and the Supervisory Board and has been discussed with TNT's external auditors.

The Board of Management believes to the best of its knowledge based on the outcome of the TNT-specific approach to internal control over financial reporting, as outlined above, that TNT's risk management and internal control over financial reporting risks have worked effectively over the year ended 31 December 2007 and declares that there are no indications that they will not continue to do so in the coming year. The Board of Management also confirms with reasonable assurance that financial reporting is free from material inaccuracies or misstatement. The Financial Statements fairly represent the financial condition and results of operations of the company and provide the required disclosures.

The above however does not imply that TNT can provide certainty as to the realisation of business and financial strategic objectives, nor can TNT's approach to internal control over financial reporting be expected to prevent or detect all misstatements, errors, fraud or violation of law or regulations.

In view of the above, the Board of Management believes that it is in compliance with the requirements of 11.1.4 of the Dutch corporate governance code taking into account the recommendations of the Frijns Committee.



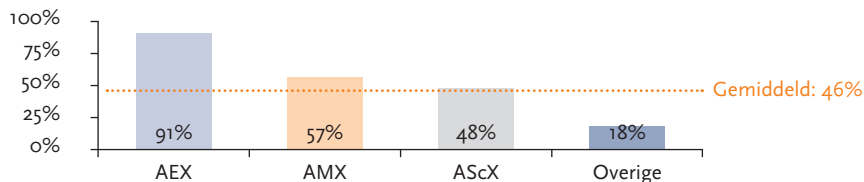
Uit Tabel 4.2 blijkt eveneens dat AEX-fondsen minder eenduidig zijn in het onderdeel van het jaarverslag waar zij de 'in control'-verklaring opnemen. Een kleine meerderheid van de onderzochte ondernemingen neemt deze verklaring op in de risicoparagraaf, maar ook zien we een aantal AEX-ondernemingen (24%) die de verklaring opnemen in de corporate governanceparagraaf of zelfs in het directieverslag (14%). Terwijl alle AEX- en AMX-fondsen een 'in control'-verklaring opnemen zijn er 3 AScX en 15 Overigen die dat niet hebben gedaan.

	AEX	AMX	AScX	Overige
Risicoparagraaf	52.4%	73.9%	76.2%	51.1%
Report of Executive Board	14.3%	8.7%	9.5%	4.4%
Corporate Governance	23.8%	13.0%	0.0%	11.1%
Aparte 'in control'-verklaring	4.8%	0.0%	0.0%	0.0%
Overige gegevens	0.0%	4.3%	0.0%	0.0%
Statement Regarding Administrative Organisation and Internal Control	0.0%	0.0%	0.0%	2.2%
Section 404 SOX	4.8%	0.0%	0.0%	0.0%
Ontbrekend	0.0%	0.0%	14.3%	31.2%
Totaal	100.0%	100.0%	100.0%	100.0%

Tabel 4.2 Onderdeel van het jaarverslag waar de 'in control'-verklaring is opgenomen.

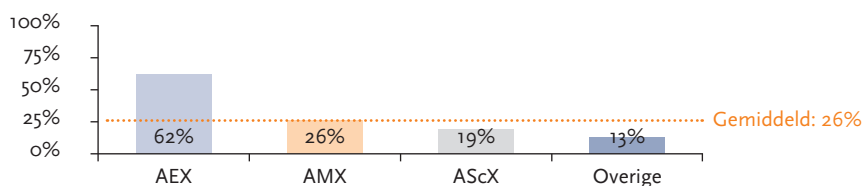
p) Is er een verwijzing naar een referentiemodel opgenomen, en zo ja, welk model? (Code Tabaksblat toelichting op best practice bepaling II.1.4 en Monitoring Commissie aanbevelingen 2007)

In onderstaande figuur (4.16) wordt aangegeven in hoeverre de onderzochte ondernemingen melding maken van het gebruik van een referentiemodel. Slechts indien er sprake is geweest van een expliciete vermelding van een referentiemodel, is daar bij de beoordeling rekening mee gehouden. Uit de figuur blijkt dat 46% van de ondernemingen verwijst naar een gehanteerd referentiemodel, waarbij de score voor AEX-fondsen duidelijk daarboven uitkomt, met ruim 90%.



Figuur 4.16 Ondernemingen die verwijzen naar een referentiemodel

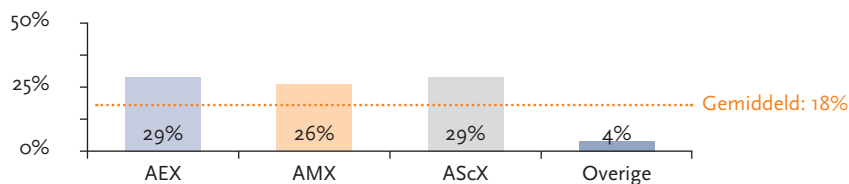
Als we vervolgens inzoomen op de gehanteerde modellen, dan valt op dat vrijwel uitsluitend COSO-IC²⁷ en COSO-ERM modellen genoemd worden. Daarbij wordt vaker verwezen naar het oudere COSO-IC model dan naar zijn opvolger, het COSO-ERM raamwerk. Gemiddeld verwijst 26% van de ondernemingen naar COSO-IC, 18% verwijst naar COSO-ERM. Opvallend is vooral de verwijzing naar het oorspronkelijke COSO-raamwerk bij de categorie AEX. Bij de Overigen wordt duidelijk minder verwezen naar dit model. Voor COSO-ERM geldt een dergelijk verschil tussen de categorieën overigens niet, uitgezonderd de Overigen die laag scoren.



Figuur 4.17a COSO-IC als referentie

²⁷ Dikwijls wordt COSO-IC ook aangeduid als COSO of COSO I.





Figuur 4.17b COSO-ERM als referentie

Een goede illustratie van een dergelijke verwijzing is te vinden in het jaarverslag van Océ (pagina 70):

Het systeem van risicomanagement en interne beheersing

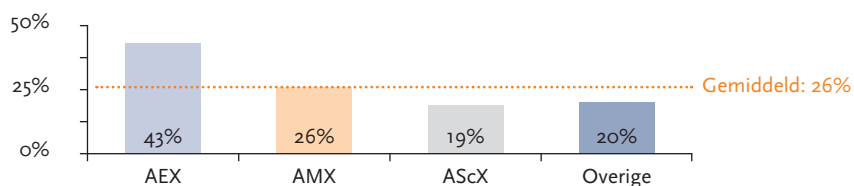
De Raad van Bestuur is verantwoordelijk voor het ontwerp en de werking van het systeem voor risico management en interne beheersing van Océ. Dit systeem is gericht op het onderkennen en beheersen van strategische, operationele, financiële en wet- en regelgeving-risico's teneinde het bereiken van de doelstellingen van de onderneming mogelijk te maken. Het systeem is gebaseerd op het eerste referentiemodel van de Committee of Sponsoring Organizations of the Treadway Commission [COSO]. Voor wat betreft informatie-technologie is het referentiemodel van het Information Technology Governance Institute gevolgd [CobIT, Control objectives for Information and related Technology].

Océ volgt de opzet van deze modellen in de maatregelen die zijn getroffen om bovengenoemde risico's in de bedrijfsprocessen en in de financieringsrapportages te beheersen. De modellen zijn centraal uitgewerkt en zoveel mogelijk op eenduidige wijze toegepast in de verschillende organisatie-onderdelen en juridische entiteiten. Een algemene risico-analyse is ingebed in de strategische bedrijfsplannen. Om inzicht te geven in de manier waarop Océ relevante risico's beheerst, wordt hieronder een overzicht gegeven van de opzet van de interne structuur voor risicobeheersing en de relatie met de verschillende risicocategorieën.

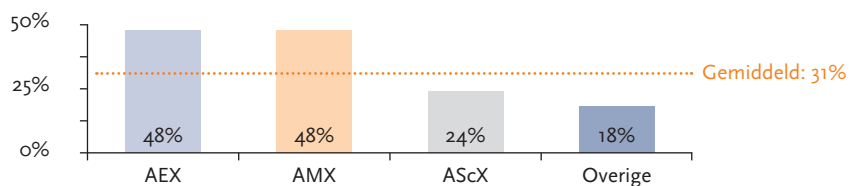
Gedurende het verslagjaar zijn geen belangrijke tekortkomingen geconstateerd in de interne structuur voor risicobeheersing. Voor de belangrijkste onderdelen hiervan wordt ter verduidelijking een korte beschrijving gegeven.

q) Is er een verwijzing naar best practice bepaling II.1.4 en/of de aanbevelingen van de Monitoring Commissie?

In figuur 4.18 is nader ingegaan op de vraag of ondernemingen in de risicoparagraaf verwijzen naar best practice bepaling II.1.4 van de Code of de aanbevelingen van de Monitoring Commissie. Alleen de ondernemingen die een expliciete verwijzing opnemen, zijn op dit onderdeel beoordeeld. Dit kan een verklaring zijn voor de lage gemiddelde scores die wij voor dit onderwerp aantreffen.



Figuur 4.18a bpb II.1.4 verwijzing

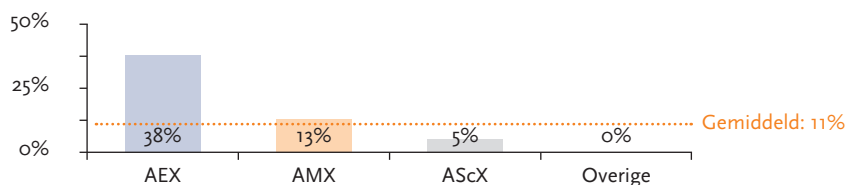


Figuur 4.18b Aanbevelingen Monitoring Commissie



r) *Is er een verwijzing naar SOX sectie 404 opgenomen?*

Vanwege een beursnotering in de Verenigde Staten moet een aantal Nederlandse beursfondsen voldoen aan de SOX-wetgeving. In figuur 4.19 is weergegeven hoe vaak Nederlandse ondernemingen verwijzen naar SOX. Ruim een derde van de AEX-fondsen verwijst naar SOX. Voor enkele ondernemingen is door het beëindigen van de Amerikaanse beursnotering inmiddels een einde gekomen aan de verplichting om aan de SOX-wetgeving te voldoen. Opvallend is dat wij bij deze ondernemingen enkele malen konden lezen dat het risicomanagement nog steeds volgens de SOX-voorschriften is vormgegeven en voldoet aan de eisen conform SOX, maar men niet langer verklaart dat de risicobeheersings- en controlesystemen *compliant* zijn met SOX.



Figuur 4.19 Verwijzing naar SOX

Ten aanzien van dit punt verwijzen wij naar de volgende verklaring die afkomstig is uit het jaarverslag van Ahold (pagina 32):

Annual declaration on risk management and control systems

Ahold supports the Dutch Corporate Governance Code and makes the following declaration in accordance with best practice provision II.1.4:

The Corporate Executive Board is responsible for establishing and maintaining adequate internal risk management and control systems. Such systems are designed to manage rather than eliminate the risk of failure to achieve objectives, and can only provide reasonable and not absolute assurance against material misstatement or loss.

With respect to financial reporting, management has assessed whether the risk management and control systems provide reasonable assurance that the 2007 financial statements do not contain any material inaccuracies. This assessment was based on the criteria set forth in COSO: Internal Control – Integrated Framework. It included tests of the design and operating effectiveness of entity-level controls, transactional controls at significant locations, and relevant general computer controls. Any deficiencies not fully remediated at year-end were evaluated. Based on this assessment, management determined that the Company's financial reporting systems are adequately designed and operated properly in 2007. Additionally, management did not become aware of any indications that they will not operate properly in 2008. This should not be construed as a statement in accordance with Section 404 of the US Sarbanes-Oxley Act, which is no longer applicable to Ahold.

With respect to strategy, operations and compliance, the risk factors that may impede the achievement of Ahold's objectives in these areas are described below. The ABC Framework and monitoring systems described above are the principal means used within Ahold to manage these risks. Management did not become aware of any important failings in these systems in 2007.

There were no significant changes in the Company's risk management and control systems during 2007 and no significant changes are presently planned for 2008. Management has discussed these results with the Audit Committee, the Supervisory Board and the external auditor.



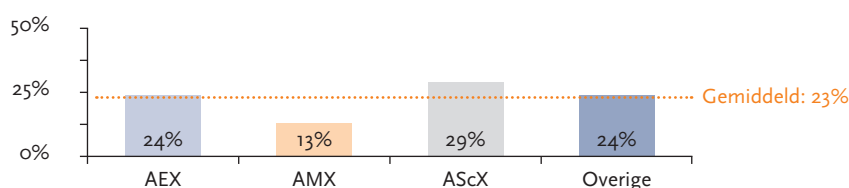
s) *Is er een verwijzing opgenomen naar andere codes voor risicomanagement?*

Naast verwijzingen naar best practice bepaling II.1.4 van de Code Tabaksblat is eveneens onderzocht of er door ondernemingen is verwezen naar andere corporate governance codes. Bij een tweetal AEX-ondernemingen werd een verwijzing naar een andere code gemaakt, te weten de Code Lippens (België) en de Combined Code (UK).

4.4.2 'In control'-verklaring met brede scope

t) *Rapporteert het bestuur over de werking van risicobeheersings- en controlesystemen in het boekjaar?*
(best practice bepaling II.1.4 Code Tabaksblat)

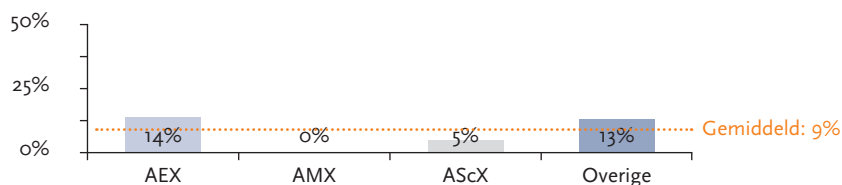
Minder dan een kwart van alle ondernemingen rapporteert over de werking van de risicobeheersings- en controlesystemen in het boekjaar. De resultaten in figuur 4.20 bevestigen het beeld dat de verslaggeving over de werking van de systemen voor het merendeel van de ondernemingen betrekking heeft op de financiële verslaggeving en beduidend minder op de andere risico's. Dit geldt voor alle categorieën, hetgeen erop duidt dat er geen opmerkelijke verschillen bestaan tussen de grotere en de lokale fondsen op dit gebied.



Figuur 4.20 Rapportage bestuur over werking van de systemen

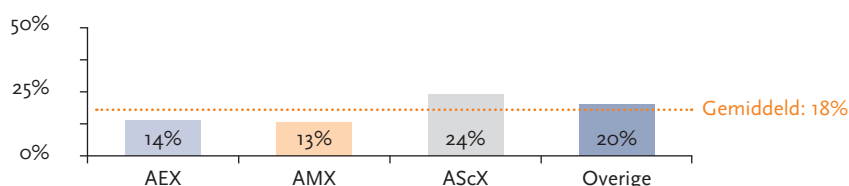
u) *Wordt verklaard dat de interne risicobeheersings- en controlesystemen effectief en/of adequaat zijn?*
(best practice bepaling II.1.4 Code Tabaksblat)

Naast de rapportering over de systemen is ook nagegaan of het bestuur verklaard heeft dat de interne risicobeheersings- en controlesystemen effectief en adequaat zijn. De uitkomsten zijn weergegeven in figuur 4.21. Iets minder dan één op de tien ondernemingen verklaart dat de systemen effectief zijn. Vergeleken met de vorige vraag betekent dit dat minder dan de helft van de ondernemingen die rapporteren over de systemen, aangeven dat deze effectief zijn.



Figuur 4.21 Verklaring dat de systemen effectief zijn

Op de vraag of het bestuur heeft verklaard dat de interne risicobeheersings- en controlesystemen adequaat zijn, luidt het antwoord als volgt (figuur 4.22). Gemiddeld werd bij 18% van alle jaarverslagen een dergelijke verklaring aangetroffen. In vergelijking met figuur 4.20 valt op dat dit percentage lager is. Tenslotte blijkt uit de analyse dat zeven ondernemingen verklaren dat de systemen effectief en adequaat zijn. Het betreft twee AEX, één AScX en vier Overigen. Het overall beeld dat hierbij naar voren komt is, dat de afgegeven verklaringen niet volledig aansluiten bij best practice bepaling II.1.4 van de Code.



Figuur 4.22 Verklaring dat de systemen adequaat zijn



v) *Wordt deze verklaring duidelijk onderbouwd? (best practice bepaling II.1.4 Code Tabaksblat)*

Tot slot is nagegaan of de verklaring omtrent de effectiviteit en adequaatheid van de interne risicobeheersings- en controlesystemen wordt onderbouwd in het jaarverslag. De conclusie luidt dat bij vrijwel alle ondernemingen een onderbouwing ontbreekt. Één onderneming (TIE Holding) vormt naar onze mening hierop een uitzondering. Zij heeft hierover in haar jaarverslag de volgende informatie opgenomen (pagina 22):

In order to assure adequate and effective internal risk management and control systems, all internal business processes are aligned according to the internal instrument called My-TIE. This system gives the Management Board complete visibility on all transactions that have taken place anywhere within the Company and provides detailed reports on revenue and costs. It also provides for strong procedures to control purchasing, order fulfillment and support. For all TIE employees world wide, it provides information on policies and procedures, customers and prospects, human resources, assets, documentation and pricing of products and services and it is the platform to collaborate with other employees, customers and resellers. The system has been outsourced in order to ensure 24/7 global availability and to free up internal resources.

The My-TIE system has been in operation since 2004 and functionality and design are developed continuously to further improve supporting business processes. My-TIE has also proven to be a very effective instrument of the internal risk management and control system. Any shortcomings that come to light as management continues to evaluate processes and procedures, also in light of changing circumstances and business processes, are addressed and resolved as soon as possible.

In view of the above, the Management Board believes that with the implementation of My-TIE as system of monitoring and reporting, it has taken adequate steps to implement an appropriate risk management and internal control system. This system provides, with reasonable certainty, reliable internal and external reports, adequate information to determine in how far the Company is achieving the strategic goals it has set and assurance that the Company is operating within the boundaries of the law. My-TIE significantly reduces, but cannot fully eliminate the possibility of poor judgment in decision-making, human errors, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of other unforeseeable circumstances. Another limiting factor is the need to consider the relative costs and benefits of risk responses. A properly designed and implemented risk management and internal control system will therefore provide reasonable but not absolute assurance that a company will not be hindered in achieving its business objectives, or in orderly and legitimate conduct of its business. In this context reasonable certainty refers to a degree of assurance that would be satisfactory for a prudent manager in the management of his affairs in the given circumstances.

Notwithstanding the forgoing and in view of the above, the Management Board is of the opinion that it has implemented a system that is adequate and effective, suitable for the Company's business and in compliance with the requirements of provision II.1.4 of the Dutch Corporate Governance Code. The Management Board has discussed the internal risk management and control systems with the Supervisory Board.

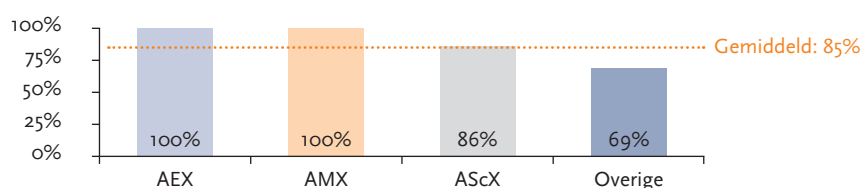


4.4.3 'In control'-verklaring met betrekking tot financiële verslaggevingsrisico's

In deze paragraaf wordt ingegaan op de verklaring van het bestuur over de financiële verslaggevingsrisico's. Dit in tegenstelling tot de voorgaande vragen, waarin is nagegaan of ondernemingen een 'in control' verklaring afleggen over de werking van de risicobeheersings- en controlesystemen met betrekking tot alle categorieën van risico's (zoals strategisch, operationeel, financieel en wet- en regelgeving).

w) *Wordt door het bestuur verklaard dat de risicobeheersings- en controlesystemen een redelijke mate van zekerheid geven dat de financiële verslaggeving geen onjuistheden van materieel belang bevat? (Monitoring Commissie guidance 2005)*

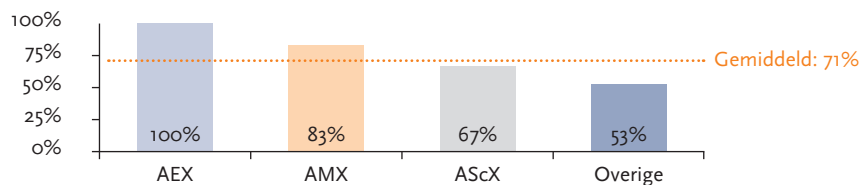
Ruim viervijfde van de ondernemingen verklaart dat de systemen een redelijke mate van zekerheid geven dat de financiële verslaggeving geen onjuistheden van materieel belang bevat, conform de aanbeveling van de Monitoring Commissie. De AEX- en AMX-ondernemingen die werden onderzocht, hebben allen een dergelijke verklaring opgenomen in hun jaarverslag. Bij de AScX en de Overigen doet 86% respectievelijk 69% dat.



Figuur 4.23 'In control'-verklaring betreffende financiële verslaggeving

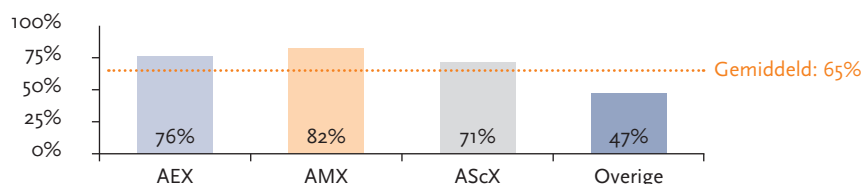
x) *Wordt verklaard dat de risicobeheersings- en controlesystemen in het verslagjaar naar behoren hebben gefunctioneerd? (Monitoring Commissie guidance 2005)*

Figuur 4.24 laat zien dat de gemiddelde score op deze vraag op 71% uitkomt; dit is lager dan het gemiddelde bij de voorgaande vraag. Ook hier scoren de AEX-fondsen maximaal; bij de AMX-fondsen werd bij 83% een dergelijke verklaring aangetroffen. De AScX en de Overigen scoren, in lijn met het voorgaande, lager. Bij de Overigen is een dergelijke verklaring in iets meer dan de helft van de gevallen opgenomen.



Figuur 4.24 Verklaring dat systemen in verslagjaar naar behoren functioneerden

y) *Wordt verklaard dat er geen indicaties zijn dat de risicobeheersings- en controlesystemen in het lopende jaar niet naar behoren zullen werken (forward looking statement)? (Monitoring Commissie guidance 2005)*



Figuur 4.25 Forward looking statement

Een andere aanbeveling van de Monitoring Commissie in haar guidance uit december 2005 betreft het *forward looking statement*. Hier ontstaat een ietwat afwijkend beeld in vergelijking met de beide voorgaande vragen. Uit figuur 4.25 valt af te leiden dat gemiddeld 65% van de ondernemingen een dergelijke verklaring heeft opgenomen. Wat met name opvalt is de lagere score van de AEX-fondsen: 76% van de ondernemingen verklaart dat er geen indicaties zijn dat de systemen in het lopende jaar niet naar behoren zullen werken. Een reden hiervoor is dat een aantal van de fondsen een beursnotering in de Verenigde Staten heeft

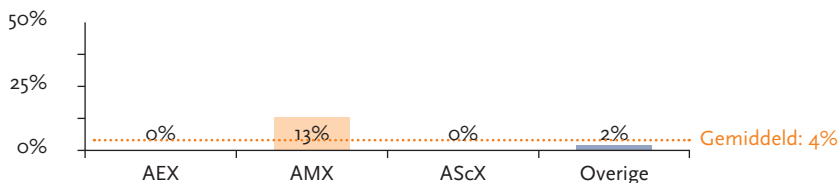


en derhalve verplicht is om aan de bepalingen van SOX te voldoen. De verklaring in het Nederlandse jaarverslag sluit hier nauw bij aan, met als gevolg dat er geen uitspraak is opgenomen over de situatie in het lopende jaar. Bij de AMX-fondsen is de score ten opzichte van de vorige vraag gelijk. Verder merken wij op dat de score van de AScX-fondsen vergelijkbaar is met de grotere AEX-ondernemingen. Bij de Overigen blijkt iets minder dan de helft een *forward looking statement* te hebben.

z) Worden eventuele tekortkomingen vermeld die materiële gevolgen kunnen hebben en in het verslagjaar respectievelijk het lopende jaar zijn geconstateerd en worden daarbij tevens aangebrachte of geplande verbeteringen aangegeven? (Monitoring Commissie guidance 2005)

Tenslotte is nagegaan of de risicoparagraaf van het jaarverslag informatie bevat over eventuele tekortkomingen en tevens of doorgevoerde of geplande verbeteringen worden aangegeven. Deze aspecten zijn beide afzonderlijk onderzocht en gescoord.

Figuur 4.26 laat zien dat gemiddeld genomen slechts 4% van alle ondernemingen eventuele materiële tekortkomingen vermeldt die zijn geconstateerd. De AMX-fondsen betrachten hierbij de meeste openheid, we hebben bij 4 ondernemingen (13%) informatie aangetroffen over tekortkomingen. Bij de Overigen is dergelijke informatie eenmaal aangetroffen.

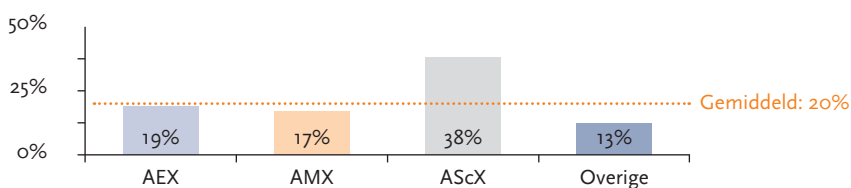


Figuur 4.26 Vermelding van tekortkomingen met materiële gevolgen

In dit kader van door ondernemingen betrachtte transparantie is het volgende voorbeeld opgenomen, afkomstig uit het jaarverslag van Binckbank (pagina 52):

In 2007 zijn een aantal interne audit onderzoeken uitgevoerd met als algemeen oordeel een adequate beoordeling van de interne beheersmaatregelen en opzet van de organisatie op de onderzochte risicogebieden binnen BinckBank. Openstaande punten zijn algemeen gezien tekortkomingen op het gebied van beleidsdocumenten en soms het naleven hiervan. Daarnaast zijn er een aantal tekortkomingen gesignaleerd in het journaliserings- en reconciliatieproces, welke op afzienbare termijn weer opgelost zullen worden. In het algemeen is het bijhouden van de groei voor de organisatie een grote uitdaging met daarbijbehorende risico's op het gebied van operationele processen en systeemondersteuning. Een aantal belangrijke systeem aanpassingsprojecten zijn gaande om de verwachte groei in goede banen te leiden.

Een duidelijk ander beeld ontstaat als wordt gekeken naar de informatie omtrent reeds doorgevoerde of geplande verbeteringen. Deze resultaten zijn gepresenteerd in figuur 4.27. Eén op de vijf ondernemingen (20%) vermeldt informatie over verbeteringen. Wat in eerste instantie opvalt, is de relatief hoge score van de AScX (38%). Dit kan onder meer worden verklaard doordat deze ondernemingen vaker aangeven dat zij ten aanzien van de implementatie van de best practices en aanbevelingen achterlopen op de grote ondernemingen. Een aantal malen is gebleken dat verbeteringen verband houden met de implementatie van de aanbevelingen van de Monitoring Commissie.



Figuur 4.27 Vermelding van aangebrachte of geplande verbeteringen



Tot slot volgt een best practice voorbeeld waarbij de materiële tekortkomingen als uitgangspunt worden genomen teneinde concrete verbeteringen van het systeem te presenteren. Uit het jaarverslag van Heijmans is het volgende afkomstig (pagina 62):

In het afgelopen jaar is nadere invulling gegeven aan het risicomanagementsysteem.

In dit kader zijn onder meer de volgende initiatieven ten uitvoer gebracht:

- *nulmeting van de beheersing van de financiële rapporteringsrisico's door een externe partij bij de divisie Infrastructuur;*
- *toepassing van Six Sigma bij Burgers Ergon, en*
- *invoering van centrale aansturing van grote projecten bij de divisie Infrastructuur.*

Daarnaast zijn als gevolg van de negatieve resultaatsontwikkelingen bij de divisie Bouw de binnen deze divisie reeds eerder ingezette maatregelen ter beheersing van de operationele processen verder aangescherpt.

De implementatie ervan is door de nieuwe divisiedirectie met een sterkere prioriteit voortgezet. De volgende maatregelen maken daar onderdeel van uit:

- *periodieke financiële review van omvangrijke en complexe projecten;*
- *toepassing van methodiek gebaseerd op Risico Management Overzichten (RMO) voor ieder project voor de start van de bouw en ook tijdens de uitvoering;*
- *10-punten systematiek voor projectmanagement;*
- *bedrijfs specifieke cursus in risicoanalyse en risicomangement, en*
- *invoering van centrale aansturing van grote projecten.*

Tevens heeft de raad van bestuur een onafhankelijke, externe partij gevraagd een onderzoek uit te voeren naar de voortgang van de implementatie van deze maatregelen. Hiermee is eind 2007 een aanvang gemaakt.

Afronding van dit onderzoek geschiedt naar verwachting in de loop van het eerste kwartaal 2008.

Het risicomanagementsysteem omvat zowel specifieke als algemene maatregelen en behelst de risico's die moeten worden beheerst op holding-, divisie- en werkmaatschappijniveau.

In 2008 zal het risicomanagementsysteem verder geoptimaliseerd worden, met name door het structureren van de vele initiatieven die thans lopen, binnen één Heijmans breed risicomangementraamwerk.





5 Samenvatting en conclusies

Inleiding en doelstelling onderzoek

In dit rapport staat de informatieverstrekking over risicomanagement door Nederlandse beursgenoteerde ondernemingen centraal. Risicomanagement wordt omschreven als het geheel van activiteiten en maatregelen die gericht zijn op het beheersen van risico's.

Het beheersen van risico's en een transparante verslaggeving over risicomanagement zijn onderdelen van een goed functionerende corporate governance. Bij ondernemingen groeit het besef dat goede beheersing van risico's een belangrijke bijdrage kan leveren aan de performance. Ook institutionele factoren, zoals wet- en regelgeving, dwingen ondernemingen om risicomanagement meer aandacht te geven. Tezamen heeft dit geleid tot meer aandacht voor de risico's en beheersingssystemen, zowel bij de ondernemingsleiding als haar stakeholders. NIVRA en Eumedion zijn hierbij actief betrokken.

Dit onderzoeksrapport heeft als doel inzicht te verschaffen in de verslaggeving omtrent risico's en beheersingsmaatregelen van beursgenoteerde ondernemingen op basis van een inventarisatie van de jaarverslagen over het boekjaar 2007. Daarnaast tracht het rapport aan de hand van de verkregen inzichten bij te dragen aan de verbetering van verslaggeving en transparantie op het gebied van risicomanagement.

Stand van zaken institutionele kader

In hoofdstuk 2 is het institutionele kader geschetst waarbinnen Nederlandse beursfondsen momenteel opereren. Op basis hiervan zijn specifieke aspecten van risico's en beheersingssystemen geïdentificeerd, die in het empirisch onderzoek nader zijn onderzocht. In de eerste plaats is aandacht besteed aan het risicoraamwerk van COSO. Het COSO-raamwerk is het belangrijkste raamwerk voor interne beheersing en risicobeheersing. Vervolgens is stilgestaan bij de gevolgen van de invoering van SOX. Nederlandse ondernemingen met een beursnotering in de Verenigde Staten moeten voldoen aan de bepalingen van deze wet. Ook is kort aandacht besteed aan de *Turnbull Guidance*, de conclusie is dat de uitgangspunten van de *Turnbull Guidance* sterke gelijkenis vertonen met het COSO-raamwerk. Als derde zijn de bepalingen van de Code Tabaksblat en de aanbevelingen van de Monitoring Commissie besproken. Best practice bepaling II.1.4 en de aanbevelingen (good practices) van de Monitoring Commissie tezamen bepalen dat de scope van de 'in control'-verklaring in Nederland is toegespitst op de risico's met betrekking tot de financiële verslaggeving. Voor overige risico's kan worden volstaan met een beschrijving. In het rapport van de Monitoring Commissie van 2007 worden aanvullende aanbevelingen gedaan voor de beschrijving van het risicoprofiel en het interne risicobeheersings- en controlesysteem. Ook is aandacht besteed aan de voorstellen (juni 2008) van de Monitoring Commissie tot aanpassing van de Code voor zover deze betrekking hebben op de interne risicobeheersing.

Tevens is de speerpuntenbrief 2008 van Eumedion besproken, hierin wordt specifiek informatie gevraagd over de bedrijfsstrategie in relatie tot het risicomanagement van de beursgenoteerde ondernemingen. Tot slot is in hoofdstuk 2 kort ingegaan op enkele relevante bepalingen van de Europese Richtlijn (2006/46/EG), deze zal naar verwachting in september 2008 worden geïmplementeerd.

Aanpak empirisch onderzoek en dataselectie

In hoofdstuk 3 is de opzet van het empirisch onderzoek en de dataselectie beschreven. Het empirisch onderzoek heeft als primaire doel in kaart te brengen hoe ondernemingen rapporteren over hun risico's en beheersingssystemen in het jaarverslag en hun website. Dit is uitgevoerd met behulp van een vragenlijst met specifieke vragen ten aanzien van risico's en beheersingssystemen. De items in de vragenlijst zijn hoofdzakelijk samengesteld op basis van (i) de best practice bepalingen van de Code Tabaksblat, (ii) de aanbevelingen van de Monitoring Commissie en (iii) de speerpuntenbrief 2008 van Eumedion. Het onderzoek is uitgevoerd op Nederlandse beursgenoteerde ondernemingen die moeten voldoen aan de bepalingen van de Code. Als peildatum is 1 januari 2008 gekozen. De definitieve onderzoekspopulatie omvat 110 ondernemingen met een notering aan Euronext Amsterdam.

Resultaten empirisch onderzoek

In hoofdstuk 4 zijn de resultaten gepresenteerd van het empirisch onderzoek naar de informatieverstrekking over risico's en beheersingssystemen. Achtereenvolgens is aandacht besteed aan:

1. de informatie over risico's van de onderneming
2. de informatie over risicobeheersings- en controlesystemen van de onderneming



3. de 'in control' verklaring.

Op basis van deze resultaten zullen in het resterende deel van dit hoofdstuk de belangrijkste resultaten en de daaruit af te leiden conclusies worden gepresenteerd.

• *Informatie over risico's*

Ten aanzien van het door de Monitoring Commissie aanbevolen overzicht van de belangrijkste risico's die zijn verbonden aan de strategie blijkt dat 62% van de ondernemingen deze risico's aangeeft. Kijken we naar de verschillende categorieën risico's, dan valt op dat veelvuldig operationele en financiële risico's worden genoemd, terwijl wet- en regelgeving en financiële verslaggevingsrisico's duidelijk minder vaak worden vermeld.

Een beperkt aantal ondernemingen geeft expliciet aan welke risico's de belangrijkste zijn: één op tien ondernemingen verschaft inzicht in de belangrijkste risico's. Uit onze analyse blijkt dat ondernemingen vrij uitvoerig verslag doen van alle risico's die zijn verbonden aan de onderneming, maar een prioritering van deze risico's ontbreekt in de meeste gevallen. Ook treffen we regelmatig uitvoerige opsommingen van risico's aan in het jaarverslag, zonder dat deze worden gekwantificeerd of dat er een relatie met de onderneming wordt gelegd. Dit soort opsommingen komt obligaats over bij een lezer en draagt weinig bij aan het inzicht.

Ten aanzien van de kwantificering van risico's kan uit het onderzoek worden afgeleid dat er sprake is van aanzienlijke verschillen tussen de categorieën ondernemingen. De AEX-fondsen rapporteren frequenter, maar ook is het aantal onderscheiden risico's, die gekwantificeerd worden meer divers. Gekwantificeerde risico's zijn vaak 'hard' en financieel van aard. In de verslaggeving over risico's is geen informatie aangetroffen over de samenhang tussen het voordoen van bepaalde risico's. Bijna driekwart van de ondernemingen verstrekt informatie over het effect op het resultaat, iets meer dan de helft rapporteert de impact op het eigen vermogen. De informatieverstrekking neemt af naarmate ondernemingen kleiner zijn. Geen van de onderzochte ondernemingen heeft bij de gepresenteerde risico's aangegeven wat de kans is op het zich voordoen van een dergelijk risico.

Het begrip '*risk appetite*' dient nog verder ingeburgerd te raken in de Nederlandse verslaggevingspraktijk. Slechts 15% van de onderzochte ondernemingen geeft een indicatie daarvan in haar risicoparagraaf. Bij een derde van de AEX-fondsen wordt gerefereerd aan de risicobereidheid, bij de anderen is dit aantal nog kleiner. Onze conclusie luidt dat er op dit punt nog veel ruimte voor verbetering is.

• *Informatie over risicobeheersings- en controlesystemen*

Ten aanzien van de informatie die wordt verstrekt over de systemen komt het volgende beeld naar voren. Alle AEX- en AMX-fondsen hebben informatie opgenomen over de systemen en de procedures, maar dat geldt niet voor alle AScX en de Overigen (91% resp. 73%). Tevens hebben we geconstateerd dat de kwaliteit van de informatie sterk verschilt. Met name voor de AScX en de Overigen geldt dat informatie over de procedures niet of slechts beperkt aanwezig is. Ruim de helft van alle ondernemingen verwijst in haar beschrijving van de systemen naar het werk van de controlerende accountant. Driekwart verwijst naar de interne accountant en/of stafdiensten met een controlerende taak.

Een opvallende conclusie uit het onderzoek is dat in vrijwel alle jaarverslagen melding wordt gemaakt van een periodieke evaluatie, maar dat in minder dan 5% daadwerkelijk informatie over de uitkomsten van de evaluatie wordt verstrekt. De AScX-ondernemingen zijn relatief het meest transparant (14%), tegen 0% voor de AEX-ondernemingen. Wij concluderen dat het met name de AEX-ondernemingen zijn die geen inhoudelijk inzicht wensen te geven in mogelijke tekortkomingen van de risicobeheersings- en controlesystemen.

Gemiddeld 71% beschrijft de risico's en de systemen in één hoofdstuk of een apart onderdeel van het jaarverslag. Ook hier scoren de AScX, evenals de Overigen, hoger dan de AEX- en AMX-ondernemingen. Ruim een derde van de ondernemingen heeft de 'in control'-verklaring niet opgenomen in de risicoparagraaf, maar elders in het jaarverslag (vooral de AEX).

Het meest gebruikte risicoraamwerk is nog steeds het COSO-raamwerk; iets minder dan de helft van de ondernemingen verwijst hiernaar. Voor de AEX ligt dit percentage boven de 90%. Opvallend is wel dat vaker wordt verwezen naar het oudere COSO-IC-model dan naar zijn opvolger, het COSO-ERM-raamwerk. Twee derde van de AEX-fondsen verwijst naar het oorspronkelijke COSO-raamwerk, bij de AMX en AScX wordt relatief vaker verwezen naar COSO-ERM.



Van de AEX-ondernemingen verwijst 38% naar SOX en van de AMX 13%. Voor een aantal is door het beëindigen van de Amerikaanse beursnotering inmiddels een einde gekomen aan de verplichting om aan de SOX-wetgeving te voldoen. Bij een aantal van deze ondernemingen lezen we dat het risicomanagement nog steeds voldoet aan SOX, maar een verklaring dat de risicobeheersings- en controlesystemen *compliant* zijn met SOX ontbreekt.

- *'In control'-verklaring*

Slechts een kwart van de ondernemingen verwijst bij de 'in control'-verklaring expliciet naar best practice bepaling II.1.4, eenderde verwijst naar de aanbevelingen van de Monitoring Commissie.

Eveneens minder dan een kwart van alle ondernemingen rapporteert over de werking van de risicobeheersings- en controlesystemen in het boekjaar. De resultaten uit het onderzoek laten zien dat de verslaggeving over de werking van de systemen voor het merendeel van de ondernemingen betrekking heeft op de financiële verslaggeving en beduidend minder op de andere risico's. Iets minder dan één op de tien ondernemingen verklaart in brede zin dat de systemen effectief zijn, zeven ondernemingen verklaren dat de systemen effectief en adequaat zijn. Op één onderneming na ontbreekt bij allen een onderbouwing van de verklaring omtrent de effectiviteit en adequaatheid van de interne risicobeheersings- en controlesystemen. Uit de analyse van de informatie over de werking van risicobeheersings- en controlesystemen blijken de op dit punt afgegeven verklaringen niet goed aan te sluiten bij best practice bepaling II.1.4 van de Code.

Ten aanzien van de 'in control'-verklaring die betrekking heeft op de risico's met betrekking tot de financiële verslaggeving ontstaat een heel ander beeld: 85% van de ondernemingen verklaart 'in control' te zijn conform de aanbeveling van de Monitoring Commissie. De AEX- en AMX-ondernemingen scoren 100%, bij de AScX en de Overigen is dit 86% respectievelijk 69%. Voorts heeft 65% van de ondernemingen een *forward looking statement* opgenomen. Wat hier opvalt is de relatief lagere score van de AEX-fondsen (76%).

Tenslotte is nagegaan of de risicoparagraaf, voor zover betrekking hebbend op de financiële verslaggevingsrisico's, informatie bevat over eventuele tekortkomingen en/of doorgevoerde dan wel geplande verbeteringen. De resultaten wijzen uit dat slechts 4% van de ondernemingen eventuele materiële tekortkomingen vermeldt die zijn geconstateerd, terwijl één op de vijf ondernemingen wel melding maakt van doorgevoerde of geplande verbeteringen. Dit bevestigt onze eerdere conclusie dat ondernemingen liever geen inzicht wensen te geven in mogelijke tekortkomingen van de risicobeheersings- en controlesystemen. Dit geldt ook weer het sterkst voor de grotere ondernemingen.

- *Overall beeld ten aanzien van de informatie over risicomanagement*

Risicomanagement is een onderwerp dat volop in de belangstelling staat. Het is positief om te constateren dat de aandacht voor dit onderwerp in de jaarverslaggeving van ondernemingen duidelijk is toegenomen. Informatieverschaffing over risicomanagement is onmiskenbaar in ontwikkeling. Geconstateerd wordt dat het onderwerp ook in het jaarverslag aan belang wint, maar daarbij dient te worden opgemerkt dat er nog geen onderneming is die alle onderzochte onderdelen in haar jaarverslag heeft opgenomen.

Tevens komt uit het onderzoek naar voren dat er in de verslaggeving sprake is van grote diversiteit: de mate van diepgang, beschrijving van systemen, risico's en de kwaliteit van de 'in control'-verklaring tonen een grote variëteit tussen ondernemingen.

Opvallend is daarbij dat de verschillen in transparantie tussen AEX, AMX en AScX op een aantal aspecten afwijkend is van de algemene beeldvorming: uit het onderzoek komt naar voren dat de AMX- en AScX-ondernemingen soms meer transparant zijn dan de AEX-ondernemingen.

Op basis van de uitkomsten van dit onderzoek hebben wij de volgende aandachtspunten geïdentificeerd:

a) *De toegankelijkheid van de verschaft informatie*

Het volume van de informatieverschaffing laat grote verschillen zien. We treffen ondernemingen aan die ruim 10 pagina's besteden aan het onderwerp, maar ook veel ondernemingen die zich beperken tot 1 pagina. De omvang is niet noodzakelijkerwijs indicatief voor de informatiedichtheid. We zien een scheiding tussen beschrijven en informeren; dat laatste heeft duidelijk de voorkeur. Dit kan treffend worden geïllustreerd aan de hand van de antwoorden op de vraag over het verschaffen van informatie over periodieke evaluatie. Terwijl een groot aantal ondernemingen aangeeft dat zij een periodieke evaluatie uitvoeren is er slechts een klein percentage van de ondernemingen dat de uitkomsten van deze evaluatie opneemt.



b) De voorzichtigheid bij ondernemingen aangaande de 'in control'-verklaring

Bij beëindiging van hun Amerikaanse beursnotering geven ondernemingen aan dat zij niet langer in overeenstemming met SOX hoeven te rapporteren en dat opgenomen verklaringen derhalve ook niet als zodanig geïnterpreteerd mogen worden. Ook hebben wij enkele malen 'onthoudingen' met betrekking tot 'in control'-verklaringen geconstateerd voor gedurende het boekjaar overgenomen ondernemingen. Daarnaast zijn er aanzienlijke verschillen geconstateerd in de gekozen bewoordingen van de opgenomen verklaringen, waardoor twijfels over de reikwijdte van deze verklaring kunnen ontstaan.

c) De presentatie van de informatie over risicomanagement

Ondernemingen worden opgeroepen om de informatie over risicomanagement zo veel mogelijk te centraliseren in een apart hoofdstuk van het jaarverslag, omdat dit de toegankelijkheid voor de gebruikers bevordert. We zien echter dat hier nog aanzienlijke ruimte voor verbetering aanwezig is.

d) De informatie over risico's

Er is een grote verscheidenheid aan risico's in de jaarverslagen, dit bemoeilijkt onderlinge vergelijkbaarheid. Het gebruik van risicocategorieën is nog geen gemeengoed. Meer consistentie in het definiëren en categoriseren van risico's zou het inzicht aanzienlijk kunnen verbeteren. Wij zouden ondernemingen voorts willen oproepen aandacht te besteden aan de risico's die verbonden zijn aan het beloningsbeleid. De crisis in de financiële sector toont aan dat hier sprake is van significante risico's, die tot op heden grotendeels onderbelicht zijn gebleven. Kwantificering van risico's wordt door ondernemingen veelvuldig toegepast, maar beperkt zich voornamelijk tot harde, financiële gegevens waarop een gevoeligheidsanalyse is uitgevoerd. Het is niet mogelijk om een goed beeld te vormen van de omvang van de aanwezige risico's, omdat de volgende informatie ontbreekt:

- De geschatte kans op het zich voordoen van bepaalde risico's.
- Correlatie tussen het optreden van verschillende risico's.
- Scenarioanalyses voor uitzonderlijke gebeurtenissen zoals de huidige kredietcrisis of een pandemie, die effect hebben op meerdere risicoparameters van een onderneming.

e) De informatie over risk appetite

De *risk appetite* staat nog in de kinderschoenen, de informatie opgenomen in de jaarverslagen hierover is onvoldoende. Informatie over de risicobereidheid van ondernemingen zou concreter moeten zijn en beter moeten aansluiten op de strategie van de onderneming en de daaraan verbonden specifieke risico's. Deze elementen tezamen vormen een belangrijke input voor een goede investeringsanalyse. Vandaar dat dit een wezenlijk onderdeel zou moeten vormen van de risicoparagraaf.



Bijlage A: Speerpuntenbrief Eumedion



Raad van Bestuur en Raad van Commissarissen

Betreft: Speerpunten 2008
Ons kenmerk: 2007.98
Schiphol, 8 november, 2007

Geacht bestuur en raad van commissarissen,

Eumedion, het corporate governance platform voor institutionele beleggers, verstuurt jaarlijks haar zogenoemde speerpuntenbrief voor het volgende jaarverslagen- en aandeelhoudersvergaderingenseizoen naar de 75 grootste Nederlandse beursgenoteerde ondernemingen. Deze speerpuntenbrief bevat belangrijke onderwerpen die de bij Eumedion aangesloten deelnemers graag onder uw aandacht willen brengen en die zij in hun bijdragen op de verschillende aandeelhoudersvergaderingen aan de orde kunnen stellen. Ten behoeve van een betere stroomlijning van de dialoog tijdens de aandeelhoudersvergadering, verzoeken wij u uw eventuele commentaar op deze punten zo spoedig mogelijk, doch uiterlijk 1 maart 2008 aan ons kenbaar te maken.

In de afgelopen twee jaar heeft Eumedion aandacht gevraagd voor de organisatie van de algemene vergadering van aandeelhouders. Als onderdeel daarvan heeft Eumedion de beursgenoteerde ondernemingen gevraagd om eerder (minimaal vier weken voor de datum van de aandeelhoudersvergadering) de agenda en de vergaderstukken uit te sturen, de registratiedatum te vervroegen, duidelijker aan te geven of agendapunten ter stemming worden gebracht en spelregels te formuleren t.a.v. de spreektijd van individuele aandeelhouders. Eumedion constateert tot haar tevredenheid dat op al deze terreinen wezenlijke vooruitgang is geboekt waardoor de organisatie van de algemene vergadering van aandeelhouders in 2008 geen speerpunt meer is.

Eumedion heeft voor het seizoen 2008 één speerpunt en één aandachtspunt geformuleerd. Het speerpunt en het aandachtspunt bouwen voort op de evaluatie van Eumedion van het afgelopen



jaarverslagen- en aandeelhoudersvergaderingenseizoen¹. Het speerpunt heeft betrekking op de bedrijfsstrategie en het risicomanagement van de beursgenoteerde ondernemingen. Het aandachtspunt heeft betrekking op de structuur van het bezoldigingsbeleid. Deze onderwerpen worden hieronder nader toegelicht.

1. Speerpunt: bedrijfsstrategie en risicomanagement

Ondernemers moeten ondernemingskansen blijven nemen. Onlosmakelijk hoort het nemen van ondernemingsrisico's daarbij. Aandeelhouders vragen om een heldere en overtuigende strategie, waarbij naast de strategische kansen de aan deze strategie verbonden risico's inzichtelijk worden gemaakt en de beheersmaatregelen die daarop van toepassing zijn. Aandeelhouders willen kortom graag antwoord op de vragen:

- i) wat is de middellange en lange termijn strategie?;
- ii) op welke kansen zet de onderneming bewust in?;
- iii) welke risico's zijn aan de strategie verbonden, wat is de kans dat deze risico's zich voordoen en wat is de omvang daarvan in termen van impact op resultaat en eigen vermogen? Institutionele beleggers hebben behoefte aan een overzicht van de, zeg vijf, belangrijkste risico's in plaats van een vermelding van alle denkbare risico's;
- iv) hoe zien de interne risicobeheersings- en controlesystemen er uit en welke procedures zijn er?;
- v) welke aanpassingen en verbeteringen zijn in het afgelopen boekjaar in deze systemen doorgevoerd en worden in het lopende boekjaar nog doorgevoerd? Waar zitten nog tekortkomingen en wat heeft prioriteit in aanpak?

Aandeelhouders hebben vanuit dit oogpunt meer behoefte aan een "brede risicoparagraaf" dan aan een algemene bestuursverklaring over de beheersing van de financiële verslaggevingsrisico's, zoals deze zich in de afgelopen jaren heeft ontwikkeld. Eumedion constateert dat de beschrijving van de interne risicobeheersings- en controlesystemen ten aanzien van de belangrijkste (strategische en operationele) risico's weinig informatief is of dat een beschrijving in haar geheel ontbreekt. De ervaring leert echter dat juist de strategische en operationele risico's debet waren aan deconfitures, bijna deconfitures of strategisch falen van ondernemingen in de afgelopen decennia hetgeen het belang van inzicht in deze risico's onderstreept. Daarnaast constateert Eumedion dat de risico's, ook de financiële, slechts in een beperkt aantal gevallen worden gekwantificeerd en dat de rapportages over de risico's en het risicobeheer verspreid zijn opgenomen in het jaarverslag en in de jaarrekening.

¹ Te downloaden via de website van Eumedion: www.eumedion.nl.



Eumedion zou graag zien dat in het jaarverslag over boekjaar 2007 een informatieve en inzichtelijke brede risicoparagraaf in het jaarverslag wordt opgenomen, waarin *alle* gegevens ten aanzien van risico's en risicobeheer geconcentreerd op die plek in het jaarverslag zijn opgenomen.

Voor alle duidelijkheid: de deelnemers van Eumedion vinden deze informatie van een groter belang dan de verklaring die het bestuur opstelt over de effectiviteit en adequaatheid van de interne risicobeheersings- en controlesystemen ten aanzien van de financiële verslaggevingsrisico's.

2. Aandachtspunt: structuur van het bezoldigingsbeleid

Eind 2006 heeft Eumedion een set aanbevelingen voor een goede structuur van het bezoldigingsbeleid gepubliceerd ("Aanbevelingen betreffende bestuurdersbezoldiging", gedateerd 25 oktober 2006)². Eumedion kan zich voorstellen dat het gedachteproces over de vormgeving van het bezoldigingsbeleid niet in één jaar is voltooid. Eumedion heeft daarom gemeend de aanbevelingen voor een goede structuur van het bezoldigingsbeleid nogmaals onder uw aandacht te brengen.

Voor de goede orde merkt Eumedion op dat de aanbevelingen niet zien op de hoogte van de bezoldiging van bestuurders maar op het bewerkstelligen van een goede structuur van het bezoldigingsbeleid voor het bestuur. Daarbij gaat het de deelnemers van Eumedion met name om de belangrijkste principes van de aanbevelingen, te weten:

1. Aansluiting van het bezoldigingsbeleid aan de lange termijn doelstellingen van de vennootschap.
2. In normale omstandigheden zou de lange termijn bonus een groter deel van de totale bezoldiging moeten uitmaken dan de jaarlijkse (korte termijn) bonus.
3. Beleggers hebben een voorkeur voor (relatieve) *total shareholder return* (TSR) als prestatie maatstaf voor de lange termijn bonus. Indien TSR als prestatie maatstaf wordt gehanteerd, dan wil Eumedion de beursgenoteerde ondernemingen de suggestie meegeven de uitkomst binnen de *peer group* te meten aan de hand van de gemiddelde beurskoersen in ten minste een aantal verslagjaren. Eventuele "koerspieken", bijvoorbeeld als gevolg van een openbaar bod, worden op deze wijze "weggemiddeld".
4. Indien de relatieve TSR als prestatie maatstaf bij aandelen- en/of optieregelingen wordt gehanteerd, dient naar de mening van Eumedion de voorwaardelijke aandelen- en/of optietoekenning te komen vervallen wanneer de vennootschap beneden de mediaan van de *peer group* presteert.

² Te vinden op de website van Eumedion: www.eumedion.nl



5. Indien de hoogte en samenstelling van de bezoldiging van de bestuurders mede wordt bepaald door het bezoldigingsbeleid van een bepaalde groep vennootschappen (de zogenoemde *arbeidsmarkt peer group*; te onderscheiden van de zogenoemde TSR (of: prestatie) *peer group*), dan is de samenstelling van deze *peer group* van groot belang voor de uiteindelijke uitkomsten. Voorzichtigheid is geboden met het gebruik van Amerikaanse vennootschappen in deze *peer group*, in verband met de totaal verschillende "bezoldigingscultuur" aldaar³. Daarnaast is behoedzaamheid op zijn plaats bij de opname van vennootschappen die in *financial distress* zijn. Vennootschappen wier continuïteit niet ter discussie staat, zouden idealiter alleen "*going concern* vennootschappen" in hun arbeidsmarkt *peer group* mogen opnemen.
6. In het afgelopen jaar is het een aantal malen voorgekomen dat aan bestuurders discretionaire bonussen werden toegekend op basis van onderhandelingsprestaties bij een grote afsplitsing of overname. Eumedion is hiervan geen voorstander. Een "uitzonderlijke" korte termijnprestatie hoort naar onze mening te "lopen" via de korte termijn bonus regeling. Denkbaar is dat in een dergelijk geval de korte termijn bonus boven *target* is, maar binnen de range zoals door de algemene vergadering is vastgesteld.

Indien het huidige bezoldigingsbeleid van uw vennootschap deze kernprincipes nog niet reflecteert, dan zou Eumedion u willen vragen de hierboven genoemde kernprincipes te betrekken bij een eventuele evaluatie van het bezoldigingsbeleid.

Mocht u behoefte hebben aan een nadere toelichting op deze brief, dan zijn wij daarvoor uiteraard beschikbaar. De Engelstalige versie van deze brief is ter informatie bijgesloten.

Hoogachtend,



Drs. Rients Abma

Directeur

³ De TSR peer group bestaat uit de directe concurrenten van de vennootschap. In de TSR peer group kunnen uitdrukkelijk wel de concurrerende vennootschappen uit de Verenigde Staten zijn opgenomen.



Bijlage B: Europese Richtlijn 2006/46/EG

RICHTLIJN 2006/46/EG VAN HET EUROPEES PARLEMENT EN DE RAAD van 14 juni 2006 tot wijziging van de Richtlijnen 78/660/EEG van de Raad betreffende de jaarrekening van bepaalde vennootschapsvormen, 83/349/EEG van de Raad betreffende de geconsolideerde jaarrekening, 86/635/EEG van de Raad betreffende de jaarrekening en de geconsolideerde jaarrekening van banken en andere financiële instellingen en 91/674/EEG van de Raad betreffende de jaarrekening en de geconsolideerde jaarrekening van verzekeringsondernemingen.

Overwegingen

(10) Vennootschappen waarvan de effecten tot de handel op een gereguleerde markt zijn toegelaten en die hun statutaire zetel in de Gemeenschap hebben, dienen te worden verplicht om een jaarlijkse verklaring inzake corporate governance openbaar te maken als een specifiek en duidelijk herkenbaar onderdeel van het jaarverslag. Deze verklaring dient de aandeelhouders op zijn minst belangrijke, gemakkelijk toegankelijke informatie te verstrekken over de feitelijk toegepaste corporategovernancepraktijken, met inbegrip van een beschrijving van de belangrijkste kenmerken van eventuele bestaande risicobeheersystemen en interne controles met betrekking tot het proces van financiële verslaggeving. In de verklaring inzake corporate governance moet duidelijk worden gemaakt of de vennootschap andere corporategovernancebepalingen toepast dan voorzien in het nationale recht, ongeacht de vraag of deze bepalingen rechtstreeks zijn vastgelegd in een corporategovernancecode waaraan een vennootschap is onderworpen of in ongeacht welke corporategovernancecode die de vennootschap eventueel heeft besloten toe te passen.

Bovendien kunnen vennootschappen een analyse van sociale en milieuaspecten verschaffen als dat nodig is voor het inzicht in de ontwikkeling, resultaten en positie van de vennootschap. Het is niet nodig om een aparte verklaring inzake corporate governance op te leggen aan ondernemingen die een geconsolideerd jaarverslag opstellen, maar er dient informatie inzake het risicobeheer en interne-controlesysteem van de groep te worden verstrekt.

Wijziging van Richtlijn 78/660/EEG

7) Het volgende artikel wordt ingevoegd:

„Artikel 46 bis

1. Een vennootschap waarvan de effecten worden toegelaten tot de handel op een gereguleerde markt in de zin van artikel 4, lid 1, punt 14, van Richtlijn 2004/39/EG van het Europees Parlement en de Raad van 21 april 2004 betreffende markten voor financiële instrumenten (*), neemt in haar jaarverslag een verklaring inzake corporate governance op. Deze verklaring vormt een specifiek deel van het jaarverslag en bevat ten minste de volgende informatie:

- a) een verwijzing naar:
 - i) de corporate-governancecode waaraan de vennootschap is onderworpen, en/of
 - ii) de corporate-governancecode die de vennootschap heeft besloten vrijwillig toe te passen, en/of
 - iii) alle relevante informatie over de corporategovernancepraktijken die worden toegepast naast de nationale wettelijke vereisten.

Indien het bepaalde onder i) en ii) van toepassing is, vermeldt de vennootschap tevens waar de desbetreffende teksten voor het publiek beschikbaar zijn; indien het bepaalde onder iii) van toepassing is, maakt de vennootschap haar corporate-governancepraktijken beschikbaar voor het publiek;

- b) voor zover een vennootschap, in overeenstemming met de nationale wetgeving, van de onder a), i) en ii), bedoelde corporate-governancecode afwijkt, een vermelding van de delen van de corporate-governancecode waarvan zij afwijkt en van de redenen daarvoor. In gevallen waarin de vennootschap heeft besloten geen enkele bepaling van een onder a), i) en ii), bedoelde corporate-governancecode toe te passen, dient zij aan te geven om welke redenen zij daartoe heeft besloten;
- c) een beschrijving van de belangrijkste kenmerken van de interne controle- en risicobeheersystemen van de vennootschap, in verband met het proces van financiële verslaggeving;
- d) de informatie die verlangd wordt in artikel 10, lid 1, onder c), d), f), h) en i), van Richtlijn 2004/25/EG van het Europees Parlement en de Raad van 21 april 2004 betreffende het openbaar overnamebod (**), voor zover de vennootschap onder deze richtlijn valt;



- e) tenzij de desbetreffende informatie reeds volledig in nationale wetgeving of regelgeving wordt verstrekt, de werking van de aandeelhoudersvergadering en haar voornaamste bevoegdheden en een beschrijving van de rechten van de aandeelhouders en hoe deze kunnen worden uitgeoefend;
 - f) de samenstelling en de werking van de bestuurs-, leidinggevende en toezichthoudende organen en hun comités.
2. De lidstaten kunnen toestaan dat de krachtens dit artikel vereiste informatie wordt openbaar gemaakt in een afzonderlijk verslag dat samen met het jaarverslag wordt gepubliceerd op de wijze die is uiteengezet in artikel 47 of door middel van een verwijzing in het jaarverslag naar de plaats waar het desbetreffende document voor het publiek beschikbaar is op de website van de vennootschap. In het geval van een afzonderlijk verslag kan de corporategovernanceverklaring een verwijzing bevatten naar het jaarverslag waar de krachtens lid 1, onder d), vereiste informatie beschikbaar is. Artikel 51, lid 1, tweede alinea, is van toepassing op het bepaalde in lid 1, onder c) en d), van dit artikel. Voor de overige informatie dient de wettelijke auditor na te gaan of de corporate-governanceverklaring is verstrekt.

Wijziging van Richtlijn 83/349/EEG

2) In artikel 36, lid 2, wordt het volgende punt toegevoegd:

- „f) een beschrijving van de belangrijkste kenmerken van de interne controle- en risicobeheersystemen van de groep met betrekking tot het proces van de opstelling van de geconsolideerde jaarrekening, indien de effecten van een onderneming worden toegelaten tot de handel op een gereguleerde markt in de zin van artikel 4, lid 1, punt 14, van Richtlijn 2004/39/EG van het Europees Parlement en de Raad van 21 april 2004 betreffende markten voor financiële instrumenten (*). Indien de geconsolideerde jaarrekening en het jaarverslag als één enkel verslag worden ingediend, moet deze informatie worden opgenomen in het deel van het verslag dat de verklaring inzake corporate governance bevat, zoals bepaald in artikel 46 bis van Richtlijn 78/660/EEG.



Bijlage C: Vragenlijst

Vragenlijst Risicoparagraaf en in control statement

1. Algemeen

- 1.1 Maakt het in-control statement onderdeel uit van de risicoparagraaf (oftewel het risicomanagement hoofdstuk)
- 1.2 Indien nee, wat is de naam van het onderdeel van het jaarverslag waarin het in-control statement dan is opgenomen
- 1.3 Is er een verwijzing naar referentiemodel opgenomen?
- 1.4 Indien ja, welk model (bijv. COSO 1992; COSO-ERM 2004)
- 1.5 Is er een expliciete verwijzing naar BPB II.1.4 opgenomen van de code Tabaksblad?
- 1.6 Is er een expliciete verwijzing opgenomen naar de aanbevelingen van de Monitoring Commissie?
- 1.7 Is er een verwijzing naar SOX section 404 opgenomen?
- 1.8 Is er een verwijzing naar een andere Code opgenomen v.w.b. risicomanagement?

Opmerking	Blz.

2. Financiële verslaggeving risico's: (Cie Frijns)

- 2.1 Wordt door het bestuur verklaard dat de risicobeheersings- en controlesystemen een redelijke mate van zekerheid geven dat de financiële verslaggeving geen onjuistheden van materieel belang bevat? (dit gaat over de opzet)
- 2.2 Wordt verklaard dat de risicobeheersings- en controlesystemen in het verslagjaar naar behoren hebben gewerkt? (dit gaat over de werking)
- 2.3 Wordt verklaard dat er geen indicaties zijn dat de risicobeheersings- en controlesystemen in het lopende jaar niet naar behoren zullen werken? (forward looking statement)
- 2.4 Worden eventuele tekortkomingen die mogelijkterwijs materiële gevolgen kunnen hebben en in het verslagjaar respectievelijk het lopende jaar zijn geconstateerd gemeld?
- 2.5 Worden daarbij tevens aangebrachte of geplande verbeteringen aangegeven?

Ja	Nee	Blz.

3. Overige risico's: (Cie Frijns)

- 3.1a Wordt er een overzicht gegeven van de risico's welke aan de strategie van de onderneming zijn verbonden?
- 3.1.b Vindt er een uitsplitsing van risico's plaats?
- 3.1.c Indien ja, in welke categorieën worden risico's uitgesplitst (zie categorieën zoals vermeld in rapport Monitoring Commissie 2007)?
- 3.1.d Wordt een overzicht verstrekt van de belangrijkste risico's?
 - Strategisch
 - Operationeel
 - Financieel
 - Compliance
 - Financiële verslaggeving
 - Overige, te weten...
- 3.1.e Is er sprake van een algemene beschrijving van de risico's of wordt de risicobeschrijving toegespitst op de onderneming?
- 3.2.a Worden de risico's gekwantificeerd (al dan niet via een gevoeligheidsanalyse)?
- 3.2.b Indien ja, welke risico's worden gekwantificeerd?
- 3.3 Wordt informatie verstrekt over de kans dat deze risico's zich voor doen?
- 3.4a Wordt informatie verstrekt over de omvang van de risico's in termen van impact op resultaat?
- 3.4.b Wordt informatie verstrekt over de omvang van de risico's in termen van impact op eigen vermogen?

Ja	Nee	Blz.



- 3.5 Wordt informatie verstrekt over de interne risicobeheersings- en controlesystemen inclusief een beschrijving van de procedures?
- 3.6 Wordt in de beschrijving van de systemen ook verwezen naar het werk/rapportages van de controlerend accountant?
- 3.7 Wordt in de beschrijving van de systemen ook verwezen naar het werk/rapportages van de intern accountant/internal auditor of andere stafdiensten met een controlerende taak?
- 3.8 Wordt de informatie over risico's en interne risicobeheersings- en controlesystemen op één plaats in het jaarverslag gepresenteerd?
- 3.9 Wordt informatie verstrekt over de risicohouding (risk appetite) van de onderneming?
- 3.10 Wordt informatie verstrekt over de resultaten van de periodiek te verrichten evaluatie van de opzet en werking van het interne risicobeheersings- en controlesysteem inclusief de naar aanleiding daarvan getroffen maatregelen?
- 3.11 Zijn de evaluatie-uitkomsten besproken met de RvC/Audit Cie?
- 3.12 Zo ja, vinden de uitkomsten van deze besprekingen hun weerslag in de verslaggeving over risicobeheersings- en controlesystemen?

	Ja	Nee	Blz.
3.5			
3.6			
3.7			
3.8			
3.9			
3.10			
3.11			
3.12			

4 Ten aanzien van alle risico's (conform Code Tabaksblat)

- 4.1 Rapporteert het bestuur over de werking van de risicobeheersings- en coontrolesystemen in het boekjaar?
- 4.2 Wordt verklaard dat de interne risicobeheersings- en controlesystemen effectief zijn?
- 4.3 Worden deze verklaringen van het bestuur duidelijk onderbouwd?
- 4.4 Wordt verklaard dat de interne risicobeheersings- en controlesystemen adequaat zijn?

	Ja	Nee	Blz.
4.1			
4.2			
4.3			
4.4			



Bijlage D: Best Practices

Uit Jaarverslag Grontmij (pagina 43-45):

Strategie

De kernactiviteiten vertonen weliswaar een sterke samenhang, maar ze zijn ook verbonden met diverse markten, klanten en regio's. Een groot deel van de diensten die worden geleverd, is direct en indirect verbonden met de overheidsmarkt. Grontmij's afhankelijkheid van voornamelijk de Nederlandse markt is afgenomen ten gunste van een geografische spreiding over zes stabiele economieën. De activiteiten zijn afhankelijk van de ontwikkelingen in de markten van onder andere bouw, infrastructuur, milieu, water, energie en industrie. De invloed van positieve en negatieve cyclische effecten wordt gedempt door:

- de cohesie tussen de activiteiten;
- de brede geografische spreiding;
- de verscheidenheid van klanten;
- sterke marktposities en de omvang van de vennootschap.

Opdrachten

Sommige opdrachten worden aan Grontmij toegekend op basis van langlopende overeenkomsten met Grontmij als voorkeursleverancier. Het grote aantal klanten maakt Grontmij onafhankelijk en verbetert de stabiliteit van het bedrijf. De projecten die voor een individuele klant worden uitgevoerd, nemen echter niet meer dan circa 2% van de totale omzet voor hun rekening. Dankzij ons gedecentraliseerde kantorennetwerk wordt een groot deel van onze bedrijfsopbrengsten gerealiseerd door een groot aantal betrekkelijk kleine contracten, met navenant beperkte risico's. Daar waar risico's worden vermoed, zijn deze zoveel mogelijk door gepaste (project)verzekeringen afgedekt. Grontmij is tot op zekere hoogte gevoelig voor prijsveranderingen en plotselinge veranderingen in het overheidsbeleid. Wij kunnen ons hieraan snel aanpassen. De budgetten van Grontmij zijn grotendeels gebaseerd op de verwachte investeringen van de overheden van Europese landen en een aantal grote industrieën.

Grote schommelingen in prijs, energie of loonkosten (naar boven of naar beneden) hebben geen snelle veranderingen in deze investeringen tot gevolg tenzij een structurele economische daling plaatsvindt in alle landen en bij alle sectoren. De groeipercentages van het BNP van elk land zijn dan ook belangrijke bedrijfsindicatoren voor Grontmij.

Grontmij is continue alert op signalen die duiden op veranderingen in de marktomstandigheden. Het blijft echter altijd mogelijk dat zich onverwachte veranderingen in de marktomstandigheden voordoen. Uitstel en stagnatie van de opdrachtenstroom kunnen leiden tot tijdelijke onderbezettingsverliezen. Bijna alle projecten worden uitgevoerd door Grontmij-bedrijven als hoofdopdrachtnemer voor de klanten voor veelal een vaste opdrachtsom.

Projecten

Gezien de aard van de bouwsector als geheel heeft Grontmij voor haar bedrijfsactiviteiten een robuust risicobeheersingsbeleid ontwikkeld: een afwisselend contractenportfolio geeft de noodzakelijke bescherming tegen contractverliezen, een grondige disciplinaire controle is verankerd en het geld wordt actief (dagelijks) gemanaged.

Grontmij richt zich in haar bedrijfsactiviteiten systematisch (ISO-9001, ISO-14001) op een bottomup benadering. Risico's worden geïdentificeerd op projectniveau, vanaf het projectniveau kan het risicoprofiel van alle projecten verzameld worden tot marktsectoren en/of tot klantgroepen per regio. Dit stelt de onderneming in staat om de condities en risico's van individuele projecten te evalueren. In figuur op pagina 56 kunt u het soort risico in projectrealisatie zien.

De projectopbrengst is voortgekomen uit gebudgetteerde projectinkomsten.

De gebudgetteerde inkomsten zijn aangepast aan de bruto en netto risicopercentages.

Gebaseerd op de potentiële risico/opbrengst van individuele projecten, is de organisatie in staat zich te richten op de meest aantrekkelijke projecten. Sinds de organisatie haar kapitaal heeft gelimiteerd, probeert de organisatie binnen een raamwerk van risicomanagement op basis van haar kennis deel te nemen aan geselecteerde joint venture bedrijven. Voor een beperkte periode van bijvoorbeeld drie tot vier jaar, kan Grontmij de tijd die door specialisten is ingezet omzetten in een minderheidsbelang in een joint venture

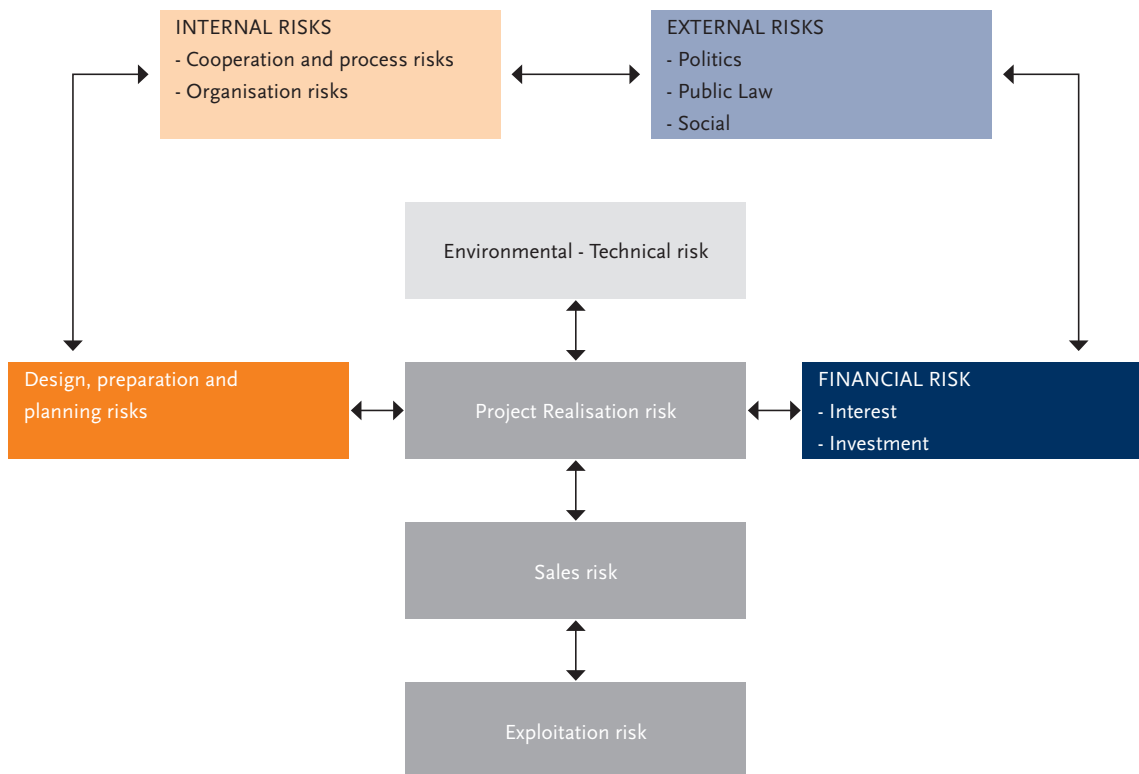


bedrijf om zo extra dividend en cashflow te investeren in haar kernactiviteiten. Het aantal joint venture projecten kan van jaar tot jaar verschillen. In bepaalde PFI (Private Finance Initiatives) investeert Grontmij op kleine schaal (€ 1-2 miljoen). De ROI van de geselecteerde joint ventures is minimaal 20%.

Grontmij neemt deel aan verschillende joint ventures:

- glastuinbouwontwikkeling in Nederland;
- recreatiegebieden en golfbanen in Nederland;
- milieu- en waterprojecten in Nederland;
- project joint ventures in België, Duitsland, Verenigd Koninkrijk en Zweden op het gebied van transport en water.

Risk types in project realisation



Arbeidsmarkt

Voor de uitvoering van opdrachten heeft Grontmij hoogopgeleide medewerkers ter beschikking. Onze positie in de arbeidsmarkt is van wezenlijk belang voor onze bedrijfsvoering. Omzetgroei is mede begrensd door het aantal gekwalificeerde medewerkers dat we kunnen aantrekken en behouden.

De beschikbaarheid van de juiste medewerkers is van cruciaal belang voor diensten en activiteiten. Weersinvloeden zijn van gering belang. Ze worden in de budgetten doorberekend en gemiddeld over het jaar en de regio's waarin Grontmij werkzaam is. Wat het personeel betreft: voor projectmanagementdiensten en de hieraan gerelateerde bouw- en infrastructuurprojecten wil Grontmij over een evenwichtige bezetting beschikken waarbij rond 85% van de medewerkers een langlopend arbeidscontract heeft en de overige 15% is aangesteld op projectbasis of op flexibele basis. De uitwisseling van mankracht tussen de verschillende bedrijfsonderdelen leidt tot een hogere bezettingsgraad.



Jaarverslag Océ

	Risk	Control measures/actions
<i>Lack of sufficient distribution power:</i>	<ul style="list-style-type: none"> • Number of sales staff (FTE) too low • Inadequate market coverage in the office segment • Productivity per sales employee too low • Number of indirect sales channels too low 	<ul style="list-style-type: none"> • In Europe: organic increase sales staff and acquisition of distributors • Implementation of office model in Europe, where possible by means of acquisition • Intensive training programmes [E-learning] further expanded • Partnerships with distributors in countries where Océ does not have sufficient presence
<i>No full-line competitive product and services portfolio:</i>	<ul style="list-style-type: none"> • Gaps in full-line product portfolio • Delay in introduction of products • Insufficiently competitive cost level • Competitive offerings by Océ Business Services • Insufficient access to OEM products 	<ul style="list-style-type: none"> • Steering of own technology and product development by Executive Board • Increase interest OEM in product portfolio • Sharper R&D focus on own unique strengths • Combine development activities with partners that add scale and innovation strength • Outsourcing of manufacturing and assembly next to more OEM systems in product portfolio • Start Document Services Valley: dedicated R&D for Océ Business Services • Tactical and strategic alliances with OEM suppliers
<i>Failure to implement corporate operational excellence programs successfully:</i>	<ul style="list-style-type: none"> • Lower net benefits • Delayed implementation • Cost overruns in implementation of process of harmonization and system support ["Spine project"] 	<ul style="list-style-type: none"> • Direct steering by members of Executive Board of individual projects • In view of the significance of the programs, specific commitment to realize cost savings of € 50 million in 2008 • Implementation support from external experts
<i>Business interruption resulting from implementation of corporate operational excellence programs and ICT projects:</i>		<ul style="list-style-type: none"> • Support from external experts including the execution of risk analyses before and during implementation • Set up and implement safety measures such as buffer stocks and operational back-up of critical processes
<i>Insufficient cash flow to finance the growth of the business and repay debt:</i>		<ul style="list-style-type: none"> • Sharp focus on realization of the strategic plan ['Growth creates Value'] • Cash Conversion Cycle management [working capital reduction] • Divestment of non-core assets and businesses • Continue to outsource leasing in Europe to vendor lease partners and expand the activities of the lease captive in the United States
<i>Financial risks impacting on value creation and continuity:</i>	<ul style="list-style-type: none"> • Foreign exchange risk exposure • Interest related exposure 	<ul style="list-style-type: none"> • Short term: use financial instruments to hedge transaction exposure in main currencies [12-months' forward position]. Foreign exchange risk on loans are 100% hedged. Currency translation risks are not hedged. • Medium and long term: natural hedges, including outsourcing of production and assembly of machines and modules to Asia. • Actively implement Interest Rate policy through interest Rate Swaps



Risk management and internal control

The risk management and control systems present within Nutreco are structured in such a way that the achievement of the targets set by the Company is optimally guaranteed. Nutreco complies with the governance requirements in respect of these responsibilities and seeks to satisfy the best practice provisions of the Tabaksblad Code. Nutreco is not obliged to meet specific requirements as stated in section 404 of the Sarbanes-Oxley Act.

The presence and efficacy of the implemented systems do not guarantee that the Company's objectives are achieved. Nor do the implemented systems warrant that human error, unforeseen circumstances, materially incorrect statements, loss, fraud and violation of laws and regulations can be fully prevented.

During the year under review, the existing framework for risk management was further implemented. Cornerstones of this framework are the Risk Management Advisory Board, the Nutreco Risk Management Model for strategic and operational risks and the management and control systems already applied in the areas of financial accounting, HSEQ (Health, Safety, Environment and Quality), feed and food safety, reporting, information security and compliance and corporate governance. Nutreco has laid down its policy measures and instructions in the Nutreco Policy House. The various control measures are explained in the following paragraphs.

Organisation of risk management

Risk Management Advisory Board

During the year under review, the Executive Board was assisted by a Risk Management Advisory Board, which evaluates risk exposure and advises both the Executive Board and the management of the operating companies on risk exposure as well as on the set-up and effect of the control measures taken. The Risk Management Advisory Board met four times during the year under review. A report of these meetings has been presented to the Executive Board and the Audit Committee. The Risk Management Advisory Board is always constituted as follows: the CFO, the Group Controller, the Group Treasurer, the Corporate Secretary and the Group Audit Manager. Specific business know-how is provided by corporate staff or business management, depending on the subjects to be assessed and evaluated at the meetings of the Advisory Board. During the year under review, the Risk Management Advisory Board focused specific attention on Nutreco's main risk areas and management processes relating thereto, such as the purchase of raw materials, information security, the treasury policy, insurance policies and the integration of newly acquired companies. The latter topic, in particular, was given much attention during the year under review in view of Nutreco's earliermentioned growth strategy; based on an in-depth analysis and evaluation of recent acquisitions, further control measures have been worked out for future integrations.

Risk Management Model

Developed in 2005, the renewed Risk Management Model was further implemented during 2007. The model provides the management of the operating companies with tools for the identification, classification and monitoring of risks, and is used for rendering account of risk management at business level. It has been found in actual practice that risk reporting tends to focus in particular on market and organisation risks. The risk monitoring results to be reported are part of the business review meetings and are presented to the Management Advisory Board for evaluation. The model has been integrated into the existing planning and control cycle.

Risk management and internal control measures

Generic management & control cycle

Strategic plans, budgets and forecasts are prepared at fixed times during the year for all operational and nonoperational units of the Nutreco organisation. The current results are evaluated monthly by the management of the operating companies and the Executive Board. The Company's performance is compared to that of the previous year and tested against the budgeted results. Forecasts are assessed for feasibility. This management and control cycle, which is based on financial and non-financial reports, enables the senior management to direct and control the operational activities in an efficient manner.



Management of raw materials risk exposure

The specific market risks arising from the volatility of raw materials markets are actively managed, among other things, by means of financial instruments (such as options and futures) and commodity forward contracts. Purchasing management keeps within the bounds of the centrally set policy and guidelines and must act in conformity with the required internal control measures. Within the framework of the Nutreco Sourcing Initiative, purchasing management as a whole was given much attention during the year under review.

Management of credit risks

Management of credit risks arising from deliveries to customers is the primary responsibility of the operating companies. The control of credit risks arising from financial counterparties is the responsibility of Group Treasury. Credit management keeps within the bounds of the centrally set policy and must act in conformity with the internal control measures. Credit risks are the specific area of attention of the senior corporate management. The Risk Management Advisory Board evaluates the quality of the control measures taken in respect of these risks. In order to further streamline different control measures, a new credit policy was developed that became effective at the beginning of 2007 and provides for clear authorisation limits and means for testing creditworthiness.

Management of interest and currency risks

In 2007 the treasury policy was reviewed under the supervision of the Risk Management Advisory Board, with, in particular, risks and limits being quantified and reporting formats and frequency being revised. Interest rate and currency risk control is part of the treasury policy.

Currency risks arising from concluded transactions must be fully covered. Risks of expected transactions are covered on the basis of probability of realisation. The operating companies cover their transaction risks through Group Treasury. Risks arising from concluded and expected transactions are reported on a monthly basis. Group Treasury chiefly uses currency forward transactions and swap transactions to hedge transaction risk exposure, which is reported on a daily basis.

Nutreco controls the consolidated translation risk by financing investments abroad in local currencies, by swapping part of the private loan, which is stated in US dollars, with another currency and by entering into cross-currency swaps. As a result of this hedge, movements caused by foreign exchange effects are partly set off in respect of both assets and cash flow. Translation risks are reported on a quarterly basis.

Management of the interest risk is the responsibility of Group Treasury. Trading is carried on within the confines of strict regulations, which are supervised by means of quarterly reporting.

Management of Health, Safety, Environment and Quality

Nutreco has a clearly defined HSEQ policy, which is applicable to all Nutreco companies. The HSEQ policy is important for product quality, process security and environmental impact. Nutreco has an HSEQ audit system in place, which covers both organisational and procedural matters. The standards observed by Nutreco are often stricter than national and international standards and are well in excess of the statutory minimum requirements. The HSEQ audit team operates according to a programme approved by the Executive Board. For further information on the HSEQ policy and the audits, please refer to the 2007 Corporate Social Responsibility Report and the Nutreco website (www.nutreco.com).

Management of food and feed safety

Prior to being processed, raw materials are thoroughly checked against specifications and for purity. Most of these checks are executed by Nutreco's own laboratories, which are well known for their know-how, expertise and quality. Nutreco's production processes meet strict standards and requirements and are in full compliance with GMP standards (Good Manufacturing Practices). Nutreco's operating companies use recognised quality systems, are almost all ISO-certified and meet HACCP guidelines. Audits are regularly performed by internationally recognised research agencies, such as Bureau Veritas and SGS, as well as by buyers and Nutreco's own HSEQ team. In respect of the risk of bacterial contamination of meat products during the production process, a policy has been drafted and procedures have been prescribed that are aimed at preventing such contaminations. An absolute guarantee that no contamination will ever occur cannot be given. As a result, the Company has developed systems and procedures with chain partners to spot contamination at an early stage and to limit the consequences. If any contamination should occur, Nutreco is able, through the Nutrace® system, to quickly trace the problem, thus reducing the risk to consumers.



Internal control measures

The Nutreco IAC framework (Internal Accounting Control) is based on different policy documents, manuals and procedures, such as the Raw Material Risk Management Policy, the Foreign Currency Policy, the Accounting Manual, the Internal Control Manual, the Treasury Manual and the Capital Expenditure Procedure. These set out guidelines, procedures and instructions in the area of financial accounting and reporting.

The managements of the operating companies are responsible for the quality of the control processes. The Internal Audit department, supported by the external auditor, handles verification of this: it assesses the developments and tests the efficacy of the implemented processes. Any inadequacies are recorded, followed up and corrected. Selection of these reviews is done partly by rotation, partly by individual selection. During the year under review, 38 IAC reviews were carried out, representing the evaluation of a total of 300 administrative processes. Furthermore, during the year under review the previously developed self-assessment process, by means of which the set-up and effect of locally implemented control measures can be assessed, was used by all Nutreco companies. This self-assessment process and related documentation also support the work of the other corporate departments and the external accountant.

The improvement in the quality of the administrative processes, already noted in 2006, continued during the year under review, with non-compliance with internal quality requirements in 2007 (6%) being mainly caused by integration activities still to be implemented within recent acquisitions and by shortcomings arising from ERP implementations. Action has since been taken to redress the identified shortcomings, none of which had materially affected the quality of the reporting. The results of the reviews were shared with the Executive Board, the Audit Committee and the external auditor.

Information security measures

The Nutreco Baseline Information Security provides the control framework for risks in the area of information technology and security. This document sets out policy, rules of conduct, procedures and instructions in the area of the control of automated systems and is managed by the Information Security Manager, who is also responsible for the focus on policy implementation and implementation monitoring.

The efficacy of the information technology and security policy is further assured through a process of self-assessment (of generic control measures) and verification processes. As well as a further improvement in control measures at all operating companies, the self-assessment during the year under review also brought to light the need for supplementary actions from the Corporate Information Technology department (clarification of responsibilities, adjustment of procedures etc.). The required control measures have since been implemented. The verification processes are performed by the Internal Audit department, which partly relies on external expertise. The results of the self-assessment and verification processes are shared with the Executive Board, the Audit Committee and the external auditor.

During the year under review, the focus on application- and implementation-related risks was increased considerably, particularly with regard to the risk arising from the situation where implementation of an ERP application coincides with a significant organisational change. Currently, such strategic implementations always go hand in hand with both pre- and post-implementation assessments in order to identify risks and take timely measures.

Management of compliance risks

The Company has a Legal Affairs department for managing risks arising from the requirements to comply with the applicable legislation and regulation in all jurisdictions where it is active, as well as to meet good practices in the area of corporate governance. Based on internal policy and procedures, the Legal Affairs department is involved, either directly or through its network, in mergers and acquisitions, share transactions, finance activities and major business transactions and/or legal conflicts.

The Risk Management Advisory Board has assessed the efficacy of the control measures. This has not given rise to any significant changes in processes. The increased takeover activity necessitated a more project-like approach of these activities. Nutreco is taking an increasingly multidisciplinary approach to such projects, with internal and external specialists working together. The involvement of the Internal Audit department warrants the quality of these processes.



Insurance

As well as taking risk control measures, Nutreco has also underwritten a general insurance programme. Nutreco has an in-house insurance company for this purpose, Nutreco Insurance, established on the Netherlands Antilles, which partly reinsures operating risks with independent insurance companies. Nutreco works worldwide with Aon as a broker and provider of insurance-related services. The policies cover loss resulting from, among other things, loss of assets and/or business interruption due to fire, explosion or natural disaster, third-party liability including product liability, transport-related damage and a number of other specific risks.

Tax

In January 2006 Nutreco Holding N.V. concluded an enforcement covenant with the Dutch tax authorities as part of the 'horizontal supervision' project initiated by the Dutch Ministry of Finance on the basis of which existing cooperation was further enhanced. The starting points of the covenant are openness and transparency, based on mutual respect and trust, resulting in an intensive exchange of information and preliminary consultations on matters with potentially material tax consequences. During 2007, under the covenant, agreement was reached on the Dutch tax position up to and including the fiscal year 2006 and the final tax assessments up to and including 2006 were imposed accordingly. With regard to 2007, any relevant tax matters were raised – and agreement was reached – at pre-consultation sessions. As a result, any uncertainties concerning the Dutch tax position have been reduced to a minimum.

This form of collaboration fits within Nutreco's policy on risk management in respect of taxation and is partly made possible by a constant focus on the level and quality of the internal control framework in the area of taxation, which is also included in the collaboration under the covenant.

In the other jurisdictions where Nutreco is operating, the Company is, where possible, pursuing a proactive policy in order to minimise any uncertainties regarding the tax positions. The internal control framework for taxation is used in most other countries as well and will be further implemented in 2008.

Measures to guarantee corporate governance

The main lines of Nutreco's corporate governance policy, which is based on the guidelines laid down in the Dutch Corporate Governance Code (page 50 of this annual report), set out to what extent the guidelines are followed. Besides general corporate governance requirements, Nutreco's governance framework also contains a number of specific components.

Nutreco Code of Ethical Conduct

The Nutreco Code of Ethical Conduct sets out a number of moral values to which Nutreco subscribes. It is not all-encompassing but instead formulates minimum ethical standards which are to be interpreted within the framework of local laws and customs. All employees with managerial responsibilities in respect of operating companies, as well as intermediate managerial levels and corporate staff, are expected to confirm in writing that they will comply with this Code. The Company Secretary is in charge of supervising compliance with the Code of Ethical Conduct. The text of the Code of Ethical Conduct is available on the Company's website.

Whistleblowing procedure

Since 2004 Nutreco has implemented a whistleblowing procedure as part of its Code of Ethical Conduct. The procedure serves to ensure that any alleged infringement of the existing policy and procedures may be reported without the person making the report suffering any negative consequences of his action. The text of the whistleblowing procedure is available on the Company's website.

Disclosure Committee (DC)

All public financial disclosures made by Nutreco should be accurate, complete and timely, fairly present, in all material respects, the Company's financial condition, results of operations and cash flows, and meet any other legal, regulatory or stock exchange requirements.

The Disclosure Committee assists the Chief Executive Officer and the Chief Financial Officer in fulfilling the Company's and their responsibilities regarding the identification and disclosure of material information about the Company and the accuracy, completeness and timeliness of the Company's financial statements.



The membership of the Disclosure Committee consists of the Company Secretary, the Director Investor Relations, the Group Audit Manager, the Group Treasurer, the Group Tax Manager and the Group Controller.

Letter of Representation (LoR)

All managing directors and controllers of the group companies shall annually sign a detailed statement with respect to financial reporting, internal controls and ethical principles. The LoR also includes activities in the field of information security, internal control, risk management and HSEQ. Any observations made in this statement shall be reported to and discussed with the Executive Board and the Audit Committee.

Role of the external auditor

The external auditor carries out the requisite activities for the issuance of an auditor's report accompanying the annual accounts. The external auditor focuses on the financial reporting and also assesses the accounting principles that have been applied to ensure that the report is free of material misstatement. Where possible, the external auditor relies on the work of the Internal Audit department, which focuses on the quality of the accounting process and the efficacy of the internal control measures. The combined activities of the Internal Audit department and the external auditor also involve an evaluation of the internal control system.









De agenda van het NIVRA in het maatschappelijk debat (2008) is te vinden op www.nivra.nl.

Antonio Vivaldistraat 2-8
Postbus 7984
1008 AD Amsterdam
Telefoon (020) 301 04 01
Fax (020) 301 03 02
E-mail: debat@nivra.nl
Internet: www.nivra.nl

