De inzichtelijkheid van de rapportage over interne risicobeheersing: Een kwantitatieve analyse voor de AEX fondsen, boekjaar 2008

November 2009

Corporate Governance Insights Centre
Rijksuniversiteit Groningen
Faculteit Economie en Bedrijfskunde
www.rug.nl/feb/onderzoek/onderzoekscentra/cgic

Contactpersoon voor dit rapport:
Niels Hermes
c.l.m.hermes@rug.nl

1. Samenvatting van de belangrijkste bevindingen

De Monitoring Commissie Corporate Governance Code heeft de Rijks*universiteit* Groningen verzocht onderzoek te verrichten naar de inzichtelijkheid van de rapportage over interne risicobeheersing van AEX vennootschappen over het boekjaar 2008 ter ondersteuning van het werk van de Commissie. Het voorliggende rapport bevat de resultaten van dit onderzoek.

Het onderzoek naar de inzichtelijkheid van de rapportage over interne risicobeheersing door de AEX fondsen in het boekjaar 2008 bestaat uit twee onderdelen. In het eerste deel van het onderzoek wordt onderzocht in hoeverre deze fondsen de Nederlandse corporate governance code naleven met betrekking tot best practice bepalingen II.1.3 tot en met II.1.6. Deze best practice bepalingen gaan in op de risicobeheersing en risicobeheersingsmaatregelen en -systemen van een onderneming. In het tweede onderdeel van het onderzoek wordt een inventarisatie gemaakt van de informatie die de ondernemingen in het jaarverslag vrijwillig verschaffen met betrekking tot de relevante risicocategorieën en de aanwezigheid en werking van de interne risicobeheersings- en controlesystemen.

In het onderzoek zijn in totaal 21 AEX fondsen onderzocht.

De belangrijkste bevindingen van dit rapport zijn als volgt samen te vatten:

(1) Met betrekking tot de naleving van de Nederlandse corporate governance code blijkt dat de 21 AEX fondsen, op een enkele uitzondering na, de best practice bepalingen betreffende de interne risicobeheersings- en controlesystemen in hoge mate naleven. Voor de vier betrokken bepalingen ligt de naleving ruim boven de 90 procent.

(2) Wat betreft de informatieverschaffing betreffende verschillende risicocategorieën en de aanwezigheid en werking van de interne risicobeheersings- en controlesystemen blijkt uit het onderzoek dat de 21 AEX fondsen in het jaarverslag over een relatief groot aantal aspecten vrijwillig informatie verstrekken.

(3) Met betrekking tot verschillende voor de onderneming belangrijke risicocategorieën blijkt dat het merendeel van de AEX fondsen over een groot aantal categorieën informatie in het jaarverslag opneemt. Voor vijf van de zeven onderscheiden risicocategorieën verschaft meer dan de helft van de 21 AEX fondsen informatie in het jaarverslag.

(4) Met betrekking tot de financiële, strategische en operationele risico's wordt door vrijwel alle fondsen vrijwillig informatie in het jaarverslag opgenomen. Risico's betreffende de integriteit van de onderneming en de zogenaamde "empowerment" risico's worden minder vaak besproken, al geldt voor deze beide categorieën nog steeds de meerderheid van de fondsen vrijwillig informatie opneemt in het jaarverslag. Informatieverschaffing betreffende risico's gerelateerd aan informatietechnologie en risico's betreffende de financiële rapportage komt het minst vaak voor.

(5) Met betrekking tot de aanwezigheid en werking van de interne risicobeheersings- en controlesystemen wordt door de 21 AEX fondsen in bijna alle gevallen vrijwillig informatie in het jaarverslag opgenomen over het raamwerk dat is gebruikt om de interne systemen op te zetten. Bovendien vermelden de meeste ondernemingen expliciet in het jaarverslag dat het bestuur de verantwoordelijkheid neemt voor de opzet en het functioneren van het interne risicobeheersings- en controlesysteem.

2. Beschrijving methode van onderzoek

Algemeen
Het onderzoek naar de inzichtelijkheid van de rapportage over interne risicobeheersing door de AEX fondsen in het boekjaar 2008 bestaat uit twee onderdelen. In het eerste deel van het onderzoek wordt onderzocht in hoeverre deze fondsen de Nederlandse corporate governance code naleven met betrekking tot best practice bepalingen II.1.3 tot en met II.1.6. Deze best practice bepalingen gaan in op de risicobeheersing en risicobeheersingsmaatregelen en -systemen van een onderneming. In het tweede onderdeel van het onderzoek wordt een inventarisatie gemaakt van de informatie die de ondernemingen in het jaarverslag vrijwillig verschaffen met betrekking tot de verschillende relevante risicocategorieën en de aanwezigheid en werking van de interne risicobeheersings- en controlesystemen.

Onderzochte ondernemingen
In het onderzoek zijn alle ondernemingen meegenomen die per 31 december 2008 deel uitmaakten van de AEX index van de Euronext Amsterdam en die binnen het bereik van de Nederlandse corporate governance code vallen. Voor het onderzoek zijn de jaarverslagen van 21 beursgenoteerde ondernemingen onderzocht.[1]

Nalevingsonderzoek
Voor het onderzoek betreffende de naleving van de Nederlandse corporate governance code door de AEX fondsen met betrekking tot best practice bepalingen II.1.3 tot en met II.1.6 (risicobeheersing en risicobeheersingsmaatregelen en systemen) is dezelfde methode gehanteerd zoals die in de nalevingsrapporten van voorgaande jaren is gebruikt. Deze methode wordt hieronder daarom slechts kort uiteengezet; voor een uitgebreidere beschrijving van de methode wordt verwezen naar het nalevingsrapport van de Monitoring Commissie Corporate Governance over het boekjaar 2007.[2]

Als bronnen voor het onderzoek zijn de inhoud van verslagen en de jaarrekening over het boekjaar 2008, evenals de informatie op de websites van de vennootschappen, gebruikt. Teneinde de best practice bepalingen II.1.3 tot en met II.1.6 van de code op een adequate wijze in het onderzoek te kunnen verwerken, zijn zij omgevormd tot één of meerdere stellingen.

De methode van het inventariseren van de naleving van de best practice bepalingen II.1.3 tot en met II.1.6 kan als volgt worden beschreven. Met een *enkelvoudige* codering (0 of 1) wordt de aan- (code 1) of afwezigheid (code 0) van een feit aangeduid. Indien (het desbetreffende onderdeel van) de best practice bepaling wordt nageleefd, zijn er twee opties:

---

[1] Royal Dutch Shell is buiten beschouwing gelaten, omdat deze onderneming vanwege de notering aan de London Stock Exchange de Combined Code naleeft.
[2] Zie: Monitoring Commissie Corporate Governance, Vierde rapport over de naleving van de Nederlandse corporate governance code, Den Haag, december 2008. Dit rapport is te downloaden via de link: http://www.commissiecorporategovernance.nl/page/downloads/DEC_2008_NL_Nalevingsrapport_2008_DEF____.pdf

- De naleving kan feitelijk aan de hand van informatie in het jaarverslag of op de website worden vastgesteld (code 1,1).
- De naleving kan niet feitelijk worden vastgesteld, maar er wordt ook geen informatie gevonden die op het tegendeel wijst. In deze situatie wordt, conform het 'pas toe of leg uit'-beginsel, naleving verondersteld (code 1,0).

Indien is vastgesteld dat de best practice bepaling niet wordt nageleefd, kan één van de volgende twee opties opgeld doen:
- Er wordt uitgelegd waarom niet wordt nageleefd (code: 0,1).
- Er wordt niet uitgelegd waarom niet wordt nageleefd (code: 0,0). In dit geval wordt de code niet toegepast.

Tabel 2.1 geeft de vertaling van de in het onderzoek gehanteerde codes naar de interpretatie van het 'pas toe of leg uit'-beginsel.

Tabel 2.1
Relatie scores en 'pas-toe-of-leg-uit'-beginsel

Score	*Aanduiding*	*Pas toe of leg uit*
0,0	Best practice bepaling wordt niet nageleefd en er is evenmin uitleg aangetroffen	Niet toegepast
0,1	Best practice bepaling wordt niet nageleefd maar er wordt wél uitleg gegeven	Toegepast, met uitleg
1,0	Impliciete naleving best practice bepaling (er kan geen informatie worden gevonden die duidt op het tegendeel)	Toegepast
1,1	Expliciete naleving best practice bepaling	Toegepast

Vrijwillige informatieverschaffing inzake risicocategorieën en aanwezigheid en werking van interne risicobeheersings- en controlesystemen
In het tweede deel van het onderzoek wordt nagegaan in hoeverre ondernemingen additionele informatie verschaffen over de aanwezigheid en werking van de interne risicobeheersings- en controlesystemen. Met additioneel wordt hier bedoeld de informatie over deze systemen die ondernemingen verschaffen in aanvulling op de informatie die zij volgens best practice bepalingen II.1.3 tot en met II.1.6 in het kader van de naleving van de Nederlandse corporate governance code dienen te verstrekken. Deze informatie wordt aldus vrijwillig door ondernemingen in het jaarverslag opgenomen.

Een onderzoek naar de vrijwillige informatieverschaffing inzake risicocategorieën en aanwezigheid en werking van de interne risicobeheersings- en controlesystemen is interessant, mede in het licht van het feit dat de Nederlandse corporate governance code in december 2008 door de Monitoring Commissie is geactualiseerd. In de nieuwe code wordt met betrekking tot de interne risicobeheersings- en controlesystemen gesteld dat ondernemingen een beschrijving dienen te geven van de voornaamste risico's gerelateerd aan de strategie van de vennootschap, alsmede een beschrijving van de opzet en werking van de interne risicobeheersings- en controlesystemen met betrekking tot de voornaamste

risico's in het boekjaar. De nieuwe code is op 1 januari 2009 in werking en dient daarom pas te worden toegepast over het boekjaar 2009. Desalniettemin is het interessant om te evalueren in hoeverre de AEX fondsen reeds in het jaarverslag van 2008 op vrijwillige basis informatie verschaffen over verschillende risicocategorieën en de aanwezigheid en werking van het interne risicobeheersings- en controlesysteem.

Voor het in kaart brengen van de vrijwillige informatieverschaffing inzake belangrijke risicocategorieën en de aanwezigheid en werking van de interne risicobeheersings- en controlesystemen is een onderzoeksinstrument ontwikkeld op basis waarvan een tekstanalyse kan worden gemaakt van de jaarverslagen van de 21 onderzochte AEX fondsen. Het onderzoeksinstrument bevat een lijst van elf elementen, "*items*" genoemd, waarover met behulp van het jaarverslag informatie is verzameld. Deze items zijn onderverdeeld in twee groepen: 7 items met betrekking tot de informatieverschaffing inzake specifieke risico's en 4 items met betrekking tot de informatieverschaffing over risicobeheersing en controle. De keuze voor deze 11 items is gebaseerd op onderzoek in de wetenschappelijke literatuur naar de mate waarin ondernemingen vrijwillig informatie verschaffen over hun interne risicobeheersings- en controlesystemen. De items met betrekking tot de specifieke risico's zijn ontleend aan een onderzoek naar de vrijwillige informatieverschaffing inzake risicomanagement door Britse beursgenoteerde ondernemingen.[3] Een deel van de items betreffende de informatieverschaffing inzake risicobeheersing en controle zijn afkomstig uit een recent onderzoek naar de mate waarin Nederlandse ondernemingen vrijwillig informatie over risicomanagement verschaffen.[4] De tekstanalyse richt op de informatieverschaffing over risicobeheersing en controle in het verhalende deel van het jaarverslag (dat wil zeggen exclusief de jaarrekening). Informatie over risicomanagement en internal control die elders op de website te vinden is, is niet meegenomen.

Naast de itemlijst wordt de omvang van de informatieverschaffing inzake risicobeheersing en controle gemeten als het aandeel dat de tekst van de risicoparagraaf inneemt in de totale tekst van het verhalende deel van het jaarverslag (dat wil zeggen, exclusief de jaarrekening).

Tabel 2.2 toont een overzicht van de gebruikte items. In bijlage I is een gedetailleerde beschrijving te vinden van de 11 items die in het onderzoeksinstrument zijn gebruikt. De tabel laat zien dat met behulp van de tekstanalyse informatie is verzameld betreffende de vraag of ondernemingen in hun jaarverslag informatie opnemen over de volgende risicocategorieën: strategische risico's, operationele risico's, financiële risico's, risico's betreffende de informatietechnologie, risico's betreffende de integriteit van de onderneming, "empowerment" risico's en risico's betreffende de financiële verslaggeving. Elke risicocategorie bestaat uit een aantal specifieke risico's. Voor een

[3] Zie: Philip M. Linsley en Philip J. Shrives, "Risk reporting : A study of risk disclosures in the annual reports of UK companies", *British Accounting Review*, 2006, volume 38, pp.387-404.
[4] Zie: Rogier Deumes en W. Robert Knechel, "Economic incentives for voluntary reporting on internal risk management and control systems", *Auditing: A Journal of Practice and Theory*, 2008, volume 27, pp. 35-66. Het onderzoek naar de mate waarin Nederlandse ondernemingen vrijwillig informatie over risicomanagement verschaffen beslaat de jaren 1997-1999.

overzicht van de specifieke risico's per categorie wordt verwezen naar bijlage II.[5] Voor elk van deze risicocategorieën wordt beoordeeld of de onderneming de betreffende specifieke risico's benoemt en/of bespreekt.[6] Indien een specifiek risico door de onderneming wordt benoemd/besproken, wordt voor de risicocategorie waartoe dit specifieke risico behoort de code "ja" ingevuld.

Tabel 2.2 laat tevens zien dat aan de hand van de tekstanalyse informatie is verzameld over de vraag of een onderneming inzage verschaft over de aanwezigheid en werking van de risicomaatregelen en het gehanteerde raamwerk op basis waarvan het risicobeheersings- en controlesysteem is ingericht. Daarnaast is onderzocht of de onderneming in het jaarverslag een oordeel van de accountant heeft opgenomen betreffende de verklaring van het bestuur omtrent de effectiviteit van het interne risicobeheersings- en controlesysteem.[7] Tenslotte is onderzocht of de onderneming in het jaarverslag een verklaring heeft opgenomen waarin het bestuur expliciet de verantwoordelijkheid voor het interne risicobeheersings- en controlesysteem neemt. De wijze van codering voor deze vier items is dezelfde als die voor bovengenoemde risicocategorieën.

Tabel 2.2
Items betreffende de vrijwillige informatieverschaffing inzake risicocategorieën en aanwezigheid en werking van het interne risicobeheersings- en controlesysteem

Informatie inzake risicocategorieën
- strategische risico's
- operationele risico's
- financiële risico's
- risico's betreffende de informatietechnologie
- risico's betreffende de integriteit van de onderneming
- "empowerment" risico
- risico's betreffende de financiële rapportage

Informatie inzake aanwezigheid/werking interne risico-beheersings- en controlesysteem
- informatie over de risicobeheersingsmaatregelen
- informatie over het gehanteerde raamwerk
- verklaring van de accountant
- expliciete verklaring bestuur inzake verantwoordelijkheid voor het interne risicobeheersings- en controlesysteem

[5] De indeling van risico's per categorie is gebaseerd op het risicomodel van het Institute of Chartered Accountants of England and Wales (ICAEW) en is ontleend aan het artikel van Linsley en Shrives, *op. cit.*

[6] Indien een onderneming een specifiek risico benoemt/bespreekt als onderdeel van een andere categorie dan die in het onderzoek wordt gehanteerd, dan wordt het betreffende risicio ingedeeld volgens de in het onderzoek gedefinieerde categorisering. Met andere woorden, indien een onderneming bijvoorbeeld specifieke risico's betreffende de informatietechnologie benoemt/bespreekt als onderdeel van de operationele risico's, dan worden deze specifieke risico's in het onderzoek ondergebracht in de categorie risico's betreffende de informatietechnologie.

[7] Een dergelijke verklaring is verplicht voor ondernemingen die een beursnotering in de Verenigde Staten hebben. Zij dienen conform de regels van de Amerikaanse beursautoriteit, de SEC (Securities and Exchange Commission) een zogeheten Form 20-F te publiceren, waarin deze verklaring moet zijn opgenomen. Voor dit item is daarom, naast het jaarverslag, ook Form 20-F meegenomen in de analyse.

3. Resultaten

3.1 Inleiding

In dit hoofdstuk worden de resultaten van het onderzoek beschreven. In paragraaf 3.2 worden de resultaten voor het nalevingsonderzoek betreffende de best practice bepalingen II.1.3 tot en met II.1.6 voor boekjaar 2008 gepresenteerd. In paragraaf 3.3 worden vervolgens de bevindingen gepresenteerd ten aanzien van de vrijwillige informatieverschaffing door ondernemingen in het jaarverslag over boekjaar 2008 inzake de aanwezigheid en werking van de interne risicobeheersings- en controlesystemen.

3.2 De naleving van de Code met betrekking tot de interne risicobeheersings- en controlesystemen

De resultaten van het onderzoek betreffende de naleving van de Nederlandse corporate governance code door de AEX fondsen met betrekking tot best practice bepalingen II.1.3 tot en met II.1.6 zijn terug te vinden in de tabellen 3.1 tot en met 3.3. Alvorens de resultaten van het onderzoek te bespreken dient het volgende te worden opgemerkt. Zoals hierboven reeds vermeld werd, is de Nederlandse corporate governance code in december 2008 door de Monitoring Commissie geactualiseerd. Met betrekking tot de best practice bepalingen betreffende de interne risicobeheersings- en controlesystemen is bepaling II.1.4 in de Code van 2003 inhoudelijk veranderd en uitgebreid en in twee nieuwe bepalingen (II.1.4 en II.1.5) uitgesplitst. De belangrijkste verandering is dat volgens de nieuwe Code ondernemingen een beschrijving dienen te geven van de voornaamste risico's gerelateerd aan de strategie van de vennootschap, alsmede een beschrijving van de opzet en werking van de interne risicobeheersings- en controlesystemen met betrekking tot de voornaamste risico's in het boekjaar. Omdat de geactualiseerde Code op 1 januari 2009 in werking is getreden dienen ondernemingen deze Code voor het eerst te hanteren over het boekjaar 2009, al zijn zij vrij om de nieuwe Code toe te passen over het boekjaar 2008. Hoewel in sommige jaarverslagen wel verwezen wordt naar de nieuwe Code en de gevolgen die de nieuwe Code heeft voor de rapportage over de interne risicobeheersings- en controlesystemen, geldt voor alle ondernemingen dat zij de Code van 2003 naleven.

Allereerst wordt specifiek aandacht geschonken aan de toepassing van best practice bepaling II.1.3 met betrekking tot de aanwezigheid van interne risicobeheersings- en controlesystemen. Volgens deze bepaling dient een onderneming als onderdeel van deze systemen risicoanalyses van de operationele en financiële doelstellingen te maken, dient er een gedragscode op de website van de onderneming te worden geplaatst, moeten er handleidingen beschikbaar zij voor de inrichting van de financiële verslaggeving en de voor de opstelling daarvan te volgen procedures en is er een systeem aanwezig van monitoring en rapportage. De interne risicobeheersings- en controlesystemen vervullen een zeer belangrijke rol met betrekking tot het bereiken van de strategische doelstellingen, het vergroten van de betrouwbaarheid van de financiële informatieverzorging en de naleving van relevante wet- en regelgeving. De resultaten in

tabel 3.1 laten zien dat de AEX fondsen best practice bepaling II.1.3 en de verschillende specifieke onderdelen daarvan vrijwel zonder uitzondering in hoge mate naleven.

Tabel 3.1
Naleving Best Practice Bepalingen II.1.3 door AEX fondsen

Best practice bepaling 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 rapportage

	Naleven	Uitleg	Niet Toepassen	n
- **Systeem is aanwezig**	**21**	**0**	**0**	**21**
- **Risicoanalyses**	**21**	**0**	**0**	**21**
- **Gedragscode in publieke bronnen**	**19**	**0**	**2**	**21**
- **Handleiding aanwezig**	**21**	**0**	**0**	**21**
- **Systeem van monitoring en rapportage**	**20**	**0**	**1**	**21**

In tabel 3.2 wordt de naleving van best practice bepaling II.1.4 beschreven. In 2004 heeft de Monitoring Commissie naar aanleiding van de toepassing van de code in 2004 een aanbeveling[8] gedaan over wanneer van toepassing van deze bepaling sprake is. Het gaat daarbij hoofdzakelijk om de verklaring betreffende de adequaatheid en effectiviteit van de interne risicobeheersings- en controlesystemen. Deze aanbeveling is ook geldig voor de evaluatie van de toepassing van deze bepaling in 2008.

In de aanbeveling stelt de Monitoring Commissie dat er een onderscheid gemaakt moet worden tussen de financiële verslaggevingrisico's en de overige bedrijfsrisico's. Vervolgens beveelt de Monitoring Commissie aan dat het bestuur van een beursgenoteerde vennootschap ten aanzien van de financiële verslaggevingrisico's verklaart dat de risicobeheersings- en controlesystemen in het verslagjaar naar behoren hebben gewerkt en dat er geen indicaties zijn dat deze systemen in het lopende jaar niet naar behoren zullen werken. Voorts dient het bestuur eventuele tekortkomingen die geconstateerd zijn in het verslagjaar en die materiële gevolgen kunnen hebben voor het verslagjaar en/of het lopende jaar te melden, waarbij zij tevens dient aan te geven welke verbeteringen in de systemen zijn aangebracht, dan wel zijn gepland.

De resultaten in tabel 3.2 laten zien dat de AEX fondsen de adviezen van de Monitoring Commissie op vrijwel alle onderdelen in hoge mate naleven. Hierop zijn slechts twee uitzonderingen. Allereerst geldt voor 8 van de 21 fondsen dat zij ten aanzien van de financiële verslaggeving geen verklaring geven voor het verwacht functioneren van de interne risicobeheersings- en controlesystemen in het lopende boekjaar. Een mogelijke verklaring hiervoor kan zijn dat ondernemingen die in 2008 verklaren dat de systemen gefunctioneerd hebben, niet nog eens expliciet in 2009 verklaren dat ze verwachten dat

[8] Zie: http://www.corpgov.nl/Aanbeveling_interne_risicobeheersings-_en_controlesystemen

een en ander ook in 2009 (het lopende jaar) ook adequaat zal functioneren. Ten tweede valt op dat 8 van de 21 ondernemingen geen beschrijving geven van de wet- en regelgevingsrisico's waarmee de onderneming mogelijk kan worden geconfronteerd.

Tabel 3.2
Naleving Best Practice Bepaling II.1.4 door AEX fondsen

Best practice bepaling II.1.4: In het jaarverslag verklaart het bestuur dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn en geeft 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.

	Naleven	Uitleg	Niet Toepassen	n
Ten aanzien van de financiële verslaggeving				
- Redelijke mate van zekerheid	**21**	**0**	**0**	**21**
- Verklaring functioneren in 2007	**20**	**0**	**1**	**21**
- Onderbouwing van de verklaring	**19**	**0**	**2**	**21**
- Verklaring verwacht functioneren	**13**	**0**	**8**	**21**
- Tekortkomingen genoemd	**21**	**0**	**0**	**21**
- Aangebrachte verbeteringen	**21**	**0**	**0**	**21**
- Geplande verbeteringen	**21**	**0**	**0**	**21**
Ten aanzien van operationeel/strategische risico's				
- Beschrijving	**20**	**0**	**1**	**21**
- Tekortkomingen genoemd	**21**	**0**	**0**	**21**
- Aangebrachte verbeteringen	**21**	**0**	**0**	**21**
- Geplande verbeteringen	**21**	**0**	**0**	**21**
Ten aanzien van Wet- en Regelgeving Risico's				
- Beschrijving	**13**	**0**	**8**	**21**
- Tekortkomingen genoemd	**21**	**0**	**0**	**21**
- Aangebrachte verbeteringen	**21**	**0**	**0**	**21**
- Geplande verbeteringen	**21**	**0**	**0**	**21**

Tabel 3.3 toont de naleving van best practice bepalingen II.1.5 en II.1.6. Volgens bepaling II.1.5 dienen ondernemingen in het jaarverslag te rapporteren over de gevoeligheid van de resultaten van de onderneming ten aanzien van externe omstandigheden en variabelen. Uit de tabel blijkt dat alle 21 AEX fondsen deze bepaling naleven. Dit betekent dat alle fondsen expliciete informatie opnemen over de risico's die de bedrijfsvoering loopt aangaande processen en ontwikkelingen die de onderneming zelf niet in de hand heeft.

Best practice bepaling II.1.6 stelt dat een onderneming een klokkenluidersregeling moet hebben, die werknemers in staat stelt om onregelmatigheden betreffende het functioneren van de onderneming en haar bestuurders te melden aan de voorzitter van de raad van commissarissen. Deze regeling dient voorts te worden gepubliceerd op de website van de

onderneming. Uit tabel 3.3 blijkt dat deze bepaling door de overgrote meerderheid van de AEX fondsen wordt nageleefd. Opvallend is wel dat toch nog drie van de 21 fondsen de klokkenluidersregeling niet op de website heeft geplaatst

Tabel 3.3
Naleving Best Practice Bepalingen II.1.5 en II.1.6 door AEX fondsen

Best practice bepaling II.1.5: Het bestuur rapporteert in het jaarverslag over de gevoeligheid van de resultaten van de vennootschap ten aanzien van externe omstandigheden en variabelen.
Best practice bepaling II.1.6: Het bestuur draagt er zorg voor dat werknemers zonder gevaar voor hun rechtspositie de mogelijkheid hebben te rapporteren over vermeende onregelmatigheden van algemene, operationele en financiële aard binnen de vennootschap aan de voorzitter van het bestuur of aan een door hem aangewezen functionaris. Vermeende onregelmatigheden die het functioneren van bestuurders betreffen worden gerapporteerd aan de voorzitter van de raad van commissarissen. De klokkenluidersregeling wordt in ieder geval op de website van de vennootschap geplaatst.

	Naleven	**Uitleg**	**Niet Toepassen**	**n**
Ten aanzien van best practice bepaling II.1.5				
- Rapportage gevoeligheid resultaten	**21**	**0**	**0**	**21**
Ten aanzien van best practice bepaling II.1.6				
- Er is een klokkenluidersregeling	**20**	**0**	**1**	**21**
- Mogelijkheid melding bij RvC	**21**	**0**	**0**	**21**
- Regeling vindbaar in publieke bronnen	**18**	**0**	**3**	**21**

Concluderend kan worden gesteld dat het nalevingsonderzoek laat zien dat de 21 AEX fondsen de best practice bepalingen betreffende de risicobeheersings- en controlesystemen, op een enkele uitzondering na, in hoge mate naleven. Tabel 3.4 geeft een overzicht van het percentage van de AEX fondsen dat de bepalingen II.1.3 tot en met II.1.6 naleeft. De getoonde percentages zijn ongewogen, dat wil zeggen, bij het berekenen van de naleving van een best practice bepaling is aan elk onderdeel van de bepaling eenzelfde gewicht toegekend. Uit de tabel blijkt dat de nalevingspercentages steeds ruim boven de 90 procent liggen. Het beeld dat uit tabel 3.4 naar voren komt in hoge mate overeen met de bevindingen ten aanzien van de naleving van de bepalingen II.1.3 tot en met II.1.6 zoals deze voor het boekjaar 2007 werden gevonden.[9]

Tabel 3.4
Nalevingspercentages best practice bepalingen II.1.3 tot en met II.1.6 (ongewogen)

- Best practice bepaling II.1.3	97%
- Best practice bepaling II.1.4	93%
- Best practice bepaling II.1.5	100%
- Best practice bepaling II.1.6	94%

[9] Zie: Monitoring Commissie Corporate Governance, Vierde rapport over de naleving van de Nederlandse corporate governance code, Den Haag, december 2008. Dit rapport is te downloaden via de link: http://www.commissiecorporategovernance.nl/page/downloads/DEC_2008_NL_Nalevingsrapport_2008_DEF____.pdf

3.3 Vrijwillige informatieverschaffing betreffende risicocategorieën en de aanwezigheid en werking van interne risicobeheersings- en controlesystemen

In deze paragraaf worden de bevindingen gepresenteerd ten aanzien van de vrijwillige informatieverschaffing door ondernemingen in het jaarverslag over boekjaar 2008 inzake de verschillende voor de onderneming belangrijke risicocategorieën en de aanwezigheid en werking van de interne risicobeheersings- en controlesystemen. Zoals hierboven reeds werd vermeld is de Code in december 2008 door de Monitoring Commissie geactualiseerd. In de nieuwe Code wordt met betrekking tot de interne risicobeheersings- en controlesystemen gesteld dat ondernemingen een beschrijving dienen te geven van de voornaamste risico's gerelateerd aan de strategie van de vennootschap, alsmede een beschrijving van de opzet en werking van de interne risicobeheersings- en controlesystemen met betrekking tot de voornaamste risico's in het boekjaar. De nieuwe code is op 1 januari 2009 in werking en dient daarom pas te worden toegepast over het boekjaar 2009. Desalniettemin is het interessant om te evalueren in hoeverre de AEX fondsen reeds in het jaarverslag van 2008 op vrijwillige basis informatie verschaffen over verschillende risicocategorieën en over de aanwezigheid en de werking van het interne risicobeheersings- en controlesysteem.

Tabel 3.5 laat zien in hoeverre ondernemingen in hun jaarverslag op vrijwillige basis informatie verschaffen over de verschillende risicocategorieën zoals deze in hoofdstuk 2 van dit rapport werden onderscheiden. De eerste conclusie die kan worden getrokken op basis van de in de tabel gepresenteerde resultaten is dat het merendeel van de ondernemingen over een groot aantal risicocategorieën informatie in het jaarverslag opneemt. Voor vijf van de zeven risicocategorieën verschaft meer dan de helft van de 21 AEX fondsen informatie in het jaarverslag.

Met betrekking tot de financiële, strategische en operationele risico's wordt door vrijwel alle fondsen informatie opgenomen. Dit is wellicht niet geheel verrassend. Het gaat hier immers om risico's als marktontwikkeling, productontwikkeling, prijs- en concurrentiebeleid, wisselkoerseffecten, leencapaciteit, renteontwikkeling, et cetera. De effecten van dergelijke risico's op de bedrijfsvoering zijn relatief duidelijk aan te geven.

Risico's betreffende de integriteit van de onderneming (zoals fraude en illegale praktijken) en de zogenaamde "empowerment" risico's (dat wil zeggen: risico's gekoppeld aan het delegeren van besluitvorming, zoals outsourcing) worden minder vaak besproken, al geldt voor deze beide categorieën nog steeds de meerderheid van de fondsen vrijwillig informatie opneemt in het jaarverslag.

Informatieverschaffing betreffende risico's gerelateerd aan informatietechnologie en risico's betreffende de financiële rapportage komt het minst vaak voor: slechts 8 respectievelijk 5 van de 21 fondsen geeft over deze beide categorieën enig inzicht in het jaarverslag. Mogelijkerwijs worden deze risico's door veel ondernemingen niet als afzonderlijke categorieën beschouwd en aldus beschreven, maar worden zij als onderdeel gezien van operationele dan wel financiële risico's.

Tabel 3.5
Informatieverschaffing inzake verschillende risicocategorieën in het jaarverslag door AEX fondsen

	Ja	Nee
- strategische risico's	**20**	**1**
- operationele risico's	**20**	**1**
- financiële risico's	**21**	**0**
- risico's betreffende de informatietechnologie	**8**	**13**
- risico's betreffende de integriteit van de onderneming	**15**	**6**
- "empowerment" risico's	**13**	**8**
- risico's betreffende de financiële rapportage	**5**	**16**

Voetnoot: zie bijlage II voor een beschrijving van de specifieke risico's per risicocategorie

Overigens komen de resultaten van dit onderzoek overeen met de bevindingen in een vergelijkbaar onderzoek van Linsley en Shrives uit 2006.[10] In hun onderzoek naar de informatieverschaffing over verschillende risicocategorieën in de jaarverslagen van 79 Britse beursgenoteerde ondernemingen komt naar voren dat de meeste informatie wordt gegeven over financiële en strategische risico's. Ook informatie omtrent risico's betreffende de integriteit van de onderneming komt vaak voor, op enige afstand gevolgd door informatie over operationele risico's. Informatie over empowerment risico's en risico's betreffende de informatietechnologie wordt nauwelijks verstrekt.

In tabel 3.6 wordt een overzicht gegeven van de vrijwillige informatieverschaffing door ondernemingen betreffende de aanwezigheid en werking van de interne risicobeheersings- en controlesystemen. Uit de tabel blijkt allereerst dat een overgrote meerderheid van de ondernemingen informatie verschaft over het raamwerk dat is gebruikt om de interne systemen op te zetten. Daarbij wordt veelal verwezen naar raamwerken als COSO I of COSO II (beter bekend als COSO Enterprise Risk Management).

Daarnaast blijkt dat de meeste ondernemingen (18 van de 21) in het jaarverslag expliciet vermelden dat het bestuur de verantwoordelijkheid neemt voor de opzet en het functioneren van het interne risicobeheersings- en controlesysteem. In het onderzoek van Deumes en Knechel uit 2008 komt naar voren dat deze informatie tien jaar geleden nauwelijks in de jaarverslagen van Nederlandse beursgenoteerde ondernemingen was terug te vinden.[11] Hun onderzoek laat zien dat slechts 6 procent van de door hen onderzochte ondernemingen deze informatie in het jaarverslag van 1998 opnam.

Veel minder vaak bevat het jaarverslag een beschrijving van de risicobeheersingsmaatregelen die de onderneming hanteert. Slechts 8 van de 21 AEX fondsen verschaft een algemene beschrijving van deze maatregelen, dan wel een beschrijving van specifieke maatregelen, zoals het gebruik van valutacontracten om de

[10] Linsley en Shrives, *op. cit.*
[11] Deumes en Knechel, *op. cit.*

effecten van wisselkoersschommelingen te mitigeren, het afsluiten van verzekeringen, het doorlopen van specifieke procedures, et cetera. Opvallend is dat uit het onderzoek van Deumes en Knechel blijkt dat ondernemingen in 1998 relatief vaker informatie in het jaarverslag opnamen betreffende de maatregelen die worden getroffen om risico's te beheersen. Uit hun onderzoek komt naar voren dat deze informatie was terug te vinden in de jaarverslagen van 60 procent van de door hen onderzochte ondernemingen.

Ten slotte is er voor 8 van de 21 fondsen een verklaring van de accountant gevonden die betrekking heeft op de verklaring van het bestuur dat het interne risicobeheersings- en controlesysteem effectief is. Een dergelijke verklaring is verplicht voor ondernemingen die een beursnotering in de Verenigde Staten hebben. Zij dienen conform de regels van de Amerikaanse beursautoriteit, de SEC (Securities and Exchange Commission) een zogeheten Form 20-F te publiceren, waarin deze verklaring moet zijn opgenomen. Voor dit item is daarom, naast het jaarverslag, ook Form 20-F meegenomen in de analyse. De 8 fondsen die een verklaring van de accountant hebben opgenomen hebben een beursnotering in Verenigde Staten en vermelden de accountantsverklaring in Form 20-F. Twee fondsen nemen de verklaring ook op in het jaarverslag. Voor de overige 13 fondsen is een dergelijke verklaring niet verplicht. Vanwege de kosten, alsmede de mogelijk verstrekkende gevolgen in termen van aansprakelijkheid, wordt een dergelijke verklaring door deze fondsen daarom ook niet opgenomen.

De totale hoeveelheid informatie over risico's en risicobeheersing dat in het jaarverslag te vinden, uitgedrukt als percentage van de totale hoeveelheid tekst die het jaarverslag beslaat (exclusief de jaarrekening), bedraagt ruim 8 procent.

Tabel 3.6
Informatieverschaffing inzake de aanwezigheid en werking van het interne risicobeheersings- en controlesysteem in het jaarverslag door AEX fondsen

In deze tabel wordt weergegeven: (1) hoeveel van de AEX fondsen in het jaarverslag informatie verschaft over risicobeheersingmaatregelen; (2) hoeveel fondsen een verwijzing geven naar het raamwerk dat is gebruikt om interne risicobeheersings- en controlesysteem op te zetten; (3) hoeveel fondsen aangeven dat er een verklaring van de accountant is gevoegd bij het zogenaamde internal control statement van het bestuur; en (4) hoeveel besturen van AEX fondsen expliciet de verantwoordelijkheid neemt voor het interne risicobeheersings- en controlesysteem.

	Ja	**Nee**
Informatie over de risicobeheersingsmaatregelen	**8**	**13**
Informatie over het raamwerk dat is gebruikt om interne risicobeheersings- en controlesysteem op te zetten	**17**	**4**
Informatie over de verklaring van de accountant die is gevoegd bij het internal control statement van het bestuur	**8**	**13**
Informatie over de verantwoordelijkheid van het bestuur voor het interne risicobeheersings- en controlesysteem	**18**	**3**

4. Bijlagen

Bijlage I: Beschrijving van de items gebruikt voor het onderzoek naar de vrijwillige informatieverschaffing betreffende de risicocategorieën en de aanwezigheid en werking van het interne risicobeheersings- en controlesysteem.

1. *Strategische risico's.* Aan de hand van het jaarverslag wordt vastgesteld of de onderneming informatie opneemt over strategische risico's. Deze risico's houden verband met onder andere: marktontwikkeling, prijs- en concurrentiebeleid, sectorinvloeden (bijvoorbeeld de effecten van invoering van regulering op een sector), et cetera.[12]

	Strategische risico's
0	Er wordt **geen** informatie verschaft over strategische risico's in het jaarverslag
1	Er wordt **wel** informatie verschaft over strategische risico's in het jaarverslag

2. *Operationele risico's.* Aan de hand van het jaarverslag wordt vastgesteld of de onderneming informatie opneemt over operationele risico's. Deze risico's houden verband met onder andere: productontwikkeling, voorraadbeheer, reputatie en merken, klanttevredenheid, efficiëntie van het productieproces, milieuaspecten, et cetera.

	Operationele risico's
0	Er wordt **geen** informatie verschaft over operationele risico's in het jaarverslag
1	Er wordt **wel** informatie verschaft over operationele risico's in het jaarverslag

3. *Financiële risico's*. Deze risico's houden verband met onder andere: rentepercentages, wisselkoerseffecten, liquiditeitseffecten, leencapaciteiten (bijvoorbeeld als gevolg verandering in credit rating), et cetera.

	Financiële risico's
0	Er wordt **geen** informatie verschaft over financiële risico's in het jaarverslag
1	Er wordt **wel** informatie verschaft over financiële risico's in het jaarverslag

4. *Risico's betreffende de informatietechnologie.* Aan de hand van het jaarverslag wordt vastgesteld of de onderneming informatie opneemt over risico's betreffende de informatietechnologie. Deze risico's houden verband met onder andere de beschikbaarheid en de veiligheid van de aanwezige informatietechnologie.

	Risico's betreffende de informatietechnologie
0	Er wordt **geen** informatie verschaft over risico's betreffende informatietechnologie in het jaarverslag
1	Er wordt **wel** informatie verschaft over risico's betreffende informatietechnologie in het jaarverslag

[12] Anders gezegd: het opnemen van informatie over één type strategisch risico leidt al tot het scoren van een één (1). Hetzelfde geldt voor vele van de hierna genoemde verslaggevingsitems. Voor de tabellen in de hoofdtekst worden de scores omgezet: de score 1 wordt omgezet in "ja"; de score 0 wordt omgezet in "nee".

5. *Risico's betreffende de integriteit van de onderneming*. Aan de hand van het jaarverslag wordt vastgesteld of de onderneming informatie opneemt over risico's betreffende de integriteit van de onderneming. Deze risico's houden verband met gevallen van fraude van het bestuur en de werknemers, reputatieschade voor de onderneming en illegale praktijken.

	Risico's betreffende de integriteit van de onderneming
0	Er wordt **geen** informatie verschaft over risico's betreffende de integriteit van de onderneming in het jaarverslag
1	Er wordt **wel** informatie verschaft over risico's betreffende de integriteit van de onderneming in het jaarverslag

6. *Empowerment risico's.* Aan de hand van het jaarverslag wordt vastgesteld of de onderneming informatie opneemt over empowerment risico's. Deze risico's houden verband met onder andere: outsourcing, het gebruik van prestatiebeloning, communicatie, et cetera.

	Empowerment risico's
0	Er wordt **geen** informatie verschaft over empowerment risico's in het jaarverslag
1	Er wordt **wel** informatie verschaft over empowerment risico's in het jaarverslag

7. Financiële rapportage risico's. Aan de hand van het jaarverslag wordt vastgesteld of de onderneming informatie opneemt over financiële rapportage risico's. Deze risico's houden verband met onder andere: de opzet en werking van de financiele rapportage processen en systemen (ook wel Accounting Information System, of bestuurlijke informatieverzorging), de aanwezigheid van functiescheidingen, opzet van interne controle maatregelen, specifieke problemen rond waardering van activa en passiva (bijvoorbeeld: schatting van oliereserves, impairment, et cetera).

	Risico's betreffende de financiële rapportage
0	Er wordt **geen** informatie verschaft over risico's betreffende de financiële rapportage in het jaarverslag
1	Er wordt **wel** informatie verschaft over risico's betreffende de financiële rapportage in het jaarverslag

8. *Risicobeheersingmaatregelen.* Een onderneming kan in meer of mindere mate uitgebreid rapporteren over de maatregelen die zij heeft getroffen in het kader van risicomanagement en internal control. Allereerst is het mogelijk dat een onderneming überhaupt geen informatie over het risicomanagement en internal control systeem opneemt. Voorts is het mogelijk dat er een beschrijving wordt gegeven van het risicomanagement en internal control systeem in algemene bewoordingen. In dit geval wordt er in vele gevallen volstaan met de melding dat er een risicomanagementsysteem is. Tot slot, is het mogelijk dat een onderneming concreet, al dan niet per risico (gebied), aangeeft op welke wijze de risico's worden beheerst (bijvoorbeeld valutacontracten om wisselkoerseffecten te mitigeren, het afsluiten van verzekeringen, het testen van interne controle maatregelen en het doorlopen van specifieke procedures, et cetera).

	Risicobeheersingsmaatregelen
0	Er wordt **geen** informatie verschaft over de risicobeheersingmaatregelen in het jaarverslag
1	Er wordt in het jaarverslag een **algemene** beschrijving gegeven van de getroffen risicobeheersingmaatregelen, dan wel aandacht besteed aan **specifieke** risicobeheersingmaatregelen.

9. *Raamwerk.* Bij het inrichten van het risicomanagement en internal control systeem kunnen ondernemingen gebruik maken van diverse *best practices* c.q. richtlijnen. Het meest bekende

voorbeeld daarvan zijn de raamwerken die door COSO zijn ontwikkeld in 1992 en laatstelijk in 2004 is gewijzigd. In het jaarverslag kan de onderneming al dan niet expliciet verwijzen naar het raamwerk dat als uitgangspunt heeft gediend bij het inrichten van het internal control systeem.

	Raamwerk
0	Er wordt **geen** verwijzing gemaakt naar een raamwerk dat gehanteerd is bij de inrichting van het internal control systeem.
1	Er wordt naar **COSO**[13] **of een ander raamwerk**[14] verwezen als het raamwerk dat is gehanteerd bij de inrichting van het internal control systeem.

10. Verantwoordelijkheid. Aan de hand van het jaarverslag wordt vastegesteld of het bestuur van de onderneming verklaart verantwoordelijk te zijn voor een adequate opzet en functioneren van de systemen van interne risicobeheersing en controle.

	Verantwoordelijkheid
0	Het bestuur neemt **niet** expliciet in het jaarverslag de verantwoording voor het interne risicobeheersings- en controle systeem.
1	Het bestuur neemt **wel** expliciet in het jaarverslag de verantwoording voor het interne risicobeheersings- en controle systeem.

11. *Verklaring accountant.* Indien in het jaarverslag (dan wel Form 20-F voor ondernemingen die een beursnotering in de Verenigde Staten hebben) een verklaring van het bestuur omtrent de effectiviteit van het internal control systeem is opgenomen dan is het mogelijk dat een derde partij (zoals een accountant) wordt gevraagd om die verklaring inzake de effectiviteit van een oordeel te voorzien. Het doel hiervan is uiteraard de geloofwaardigheid van de verklaring inzake de effectiviteit te verhogen.

	Accountantsverklaring
0	Er wordt **geen** verklaring door een externe accountant of andere deskundige van *buiten de onderneming* afgegeven bij de verklaring van het bestuur inzake de effectief van het internal control systeem..
1	Er is **wel** een verklaring inzake de betrouwbaarheid van de bestuursverklaring ten aanzien van de effectiviteit van het internal control systeem aanwezig in het jaarverslag. Deze verklaring is afgegeven door een externe accountant of een andere deskundige van buiten de onderneming.

[13] Onder COSO wordt in dit verband verstaan zowel COSO I uit 1992, als COSO II uit 2004. Dit laatste raamwerk staat ook wel beter bekend als COSO Enterprise Risk Management (oftewel COSO ERM).
[14] Voorbeelden van andere raamwerken zijn het Britse Turnbull report en het Canadese CoCo-rapport.

Bijlage II: Indeling van risico's per categorie is gebaseerd op het risicomodel van het Institute of Chartered Accountants of England and Wales (ICAEW)

Strategische risico's:
- Omgevingsanalyse
- Sectorinvloeden
- Activiteiten in portefeuille
- Concurrentiebeleid
- Prijsbeleid
- Waarderingsvraagstukken
- Planning

Operationele risico's:
- Klanttevredenheid
- Productontwikkeling
- Efficiëntie van het productieproces
- Voorraadbeheer
- Inputmanagement
- Gebreken betreffende producten en diensten
- Milieuaspecten
- Gezondheid en veiligheid
- Aantasting merknaam

Financiële risico's:
- Rentepercentages
- Wisselkoerseffecten
- Liquiditeitseffecten
- Leencapaciteit (credit ratings)
- Schommelingen van grondstoffenprijzen

"Empowerment" risico's:
- Leiderschap en management
- Outsourcing
- Prestatiebeloning
- Bereidheid tot verandering
- Communicatie

Risico's betreffende de informatietechnologie:
- Integriteit van de informatiesystemen
- Beschikbaarheid
- Toegankelijkheid
- Infrastructuur

Risico's betreffende de integriteit van de onderneming:
- Fraude van het management en personeel
- Illegale activiteiten
- Reputatie

Risico's betreffende de financiële rapportage:[15]

- Opzet en werking van de financiële rapportage processen en systemen
- Aanwezigheid van functiescheidingen
- Opzet van interne controlemaatregelen
- Waardering van activa en passiva

[15] Deze risicocategorie is niet ontleend aan de indeling zoals die door de ICAEW is opgesteld.