Corporate Governance, reactie concept 1 juli 2003 door Mr R.A.Vroom.

Algemene beschouwing Risk Management.

Alvorens in te gaan op de tekst van het concept, wil ik eerst een aantal opmerkingen maken over de huidige stand van zaken van Risk Management zoals ik die ervaar.
Deze algemene beschouwing bepaalt en verklaart mijn reactie op de tekst van het concept.

1- Risk Management is bij een groot aantal ondernemingen geen 'corporate' aangelegenheid. Risico's worden door Raden van Bestuur en topmanagers niet structureel aangepakt. Documenten die de basis leggen voor een structurele aanpak van Risk Management, geldig voor de gehele organisatie, zijn er niet. Er wordt wel op diverse niveaus en afdelingen binnen ondernemingen gefragmenteerd aan risicobeheersing gedaan. Van een samenhangend geheel, van een enterprise wide risk management programma, is geen sprake.

2- Waar ligt dat aan. Eén van de belangrijkste oorzaken is de wil om vooruit te gaan, vergezichten te realiseren, waarbij het rekening houden met risico's als een lastige, vertragende factor wordt gezien. Een aspect dat vooral bij Raden van Bestuur en hoger management zichtbaar is. Een andere factor van betekenis is de druk van alledag, men wil zaken realiseren waarbij men zichzelf geen ruimte gunt om naar de oorzaken en effecten van deze druk te kijken. We zien de invloed van deze druk vooral bij de lagere managers. Aandacht voor Risk Management heeft in de praktijk daardoor geen prioriteit.

3- In jaarverslagen is de rapportage over de risico's op dit moment uiterst mager. Men maakt opmerkingen over politieke omstandigheden, onzekere marktomstandigheden, valutakwesties en dergelijke. Allen buitengewoon voor de handliggend verklaringen, open deuren, die voor het bedrijf en bedrijfstak waarin de onderneming werkzaam is, voor de handliggend en daardoor van weinig betekenis zijn.

4- Er is onvoldoende besef dat voor een goede Risk Managementstructuur Raden van Bestuur en managers zowel subject als object van handelen zijn. Zij zijn verantwoordelijk voor een goede uitvoering. Tegelijkertijd is hun eigen handelen ook onderworpen aan de afspraken / procedures van het Risk Management programma.

5- Een goede Risk Managementstructuur kent de volgende aspecten: de risicoanalyse- de beheersing- het verbeteren en het toetsen. De verantwoordelijkheid van de eerste 3 aspecten hoort bij de lijnmanagers te liggen. Risk managers zijn er om deze managers te ondersteunen. Veelal hebben deze Risk managers onvoldoende autoriteit om het management ook op corporate level op adequate wijze te ondersteunen. Er is geen afstemming tussen de aanpak van de Risk Managers en de internal auditors.

6- Het toetsen – de auditfunctie- maakt een wezenlijk onderdeel van een succesvol programma uit. De integratie van de auditfunctie in een Risk Managementprogramma kan alleen slagen indien de auditfunctie uitgaat van Risk Based auditing. Alleen dan kan gewerkt worden aan een samenhangende aanpak van de risicobeheersing in de hele organisatie.

Artikelsgewijze opsomming van commentaar naar aanleiding van de Concepttekst.

In mijn commentaar zal ik mij laten leiden door de volgorde per pagina van relevante artikelen / alinea's in de concepttekst. Deze zijn in de tekst vetgedrukt.

I Raad van bestuur / Taak en werkwijze / Principe.

De Raad van bestuur is verantwoordelijk voor het beheersen van de risico's verbonden aan de ondernemingsactiviteiten en voor de financiering van de vennootschap. De raad van bestuur rapporteert hierover aan en bespreekt de interne risicobeheersings- en controlesystemen met de raad van commissarissen en zijn auditcommissie.

a) In deze alinea, dat zich richt op de beheersing van risico's, staat de 'verantwoordelijkheid voor de financiering van de vennootschap' er een beetje los bij. Het wordt in het Concept niet nader

uitgewerkt. Anders wordt het als er aan wordt toegevoegd: ‘voor de financiering **van de risico’s** van de vennootschap’. Een belangwekkende toevoeging. Daarmee wordt de risicofinanciering (het al of niet in eigen beheer nemen, het afdekken van risico’s via de geldmarkt of via verzekering etc.) expliciet een aangelegenheid waar de Raad van bestuur zich over moet uitlaten.

b) Interne risicobeheersings – en controlesystemen. In dit concept een veel gebruikte terminologie. Maar wat wordt daaronder verstaan? De verwarring komt vanuit het woord ‘controle’. De Engelsen zien ‘controle’ als beheersing, de franssprekenden zien ‘contrôle’ als ‘toetsen’. Als de engelse opvatting wordt bedoeld, dan staat er in feite tweemaal hetzelfde: risicobeheersing en controle. Voor de franse opvatting van ‘contrôle’, welke onder controlesystemen slechts toetssystemen verstaat, vind ik de concepttekst geen ondersteuning. In het Turnbull rapport d.d. september 1999 ‘Intenal Control, Guidance for Directors on the Combined Code’ wordt een onderscheid gemaakt tussen Risk Management en Internal Control. Internal Control wordt dan gezien als het samenstel van beheersingsmaatregelen door de hele organisatie heen, inclusief het toetsen (de auditfunctie). Als men zich voor ogen houdt dat *Internal Control* dé uitdrukking is, dan is de Nederlandse omschrijving: ‘interne risicobeheersingsystemen’ ook niet terecht. Beter zou dan zijn: ‘risicobeheersings- en interne controlesystemen.. Uiteindelijk gaat mijn voorkeur uit naar de Thurnbull aanpak dus: ‘risk management en interne controlesystemen. Deze terminologie doet recht aan het risk managementproces én aan het beheersingsysteem.

c) Auditcommissie. Inmiddels zijn er grote ondernemingen die deze commissie een ruimere taak en dus ook een aangepaste naam geven: Risk- en Auditcommissie. De achtergrond daarvan is dat in de praktijk de auditor een rol aan de zijlijn vervult. Hij kijkt toe of het risk managementproces wel goed verloopt. De risico-inventarisatie en analyse, de risicoacceptatie, prioriteitstelling, risicofinanciering en de maatregelen ter verbetering van het risico vinden met name in de lijn plaats. Het is van het grootste belang dat de risico’s en de omgang daarmee in volle omvang aan de orde komen in de auditcommissie. Pas dan mag je ervan uitgaan dat niet alleen bij de Raad van Bestuur maar ook bij de Raad van Commissarissen een verantwoord beeld en bewustzijn van de risico’s ontstaat. Omdoping van de naam van de auditcommissie tot Risk- en auditcommissie geeft een betere garantie dat Risk management en de beheersingsstructuur op het hoogste niveau onder de aandacht van het (toezicht op het) management komt. Bovendien versterkt deze aangepaste naam de noodzaak tot samenspel tussen diegenen die direct bij het Risk Management betrokken zijn en de auditors.

Best practice bepalingen

I. 1.2 **De raad van bestuur legt ter goedkeuring voor aan de raad van commissarissen:**
a) de operationele en financiële doelstellingen van de vennootschap;
b) de strategie die moet leiden tot het realiseren van de doelstellingen;
c) de randvoorwaarden die bij de strategie worden gehanteerd, bijvoorbeeld ten aanzien van de financiële ratio's.
De hoofdzaken hiervan worden vermeld in het jaarverslag.

a) Operationele en financiële doelstellingen. Begrippen die veel worden genoemd. Helderheid over deze begrippen is temeer van belang omdat aan deze begrippen ook de noodzakelijke risicoanalyses worden verbonden.
Naast operationele en financiële risico’s zijn op corporate niveau allerlei andere risicobenamingen in zwang. Als belangrijkste: de strategische risico’s, maar daarnaast ook compliance, human resource, ICT, etc (de Bazel II regulering spreekt expliciet van market- en creditrisks naast de operational risks). Wat ik wil onderstrepen is dat elke nadere precisering vragen oproept omtrent de bedoeling en de reden van die precisering. Tegelijkertijd wordt ruimte geboden om bepaalde zaken die niet specifiek genoemd worden buiten de regeling en toezichtkader te houden. Voorts moet daarbij aangetekend worden dat op corporate level het met name om de strategische doelstellingen gaat. De keuzes van AHOLD om naar Noord en

Zuid Amerika te gaan en van Laurus om de Konmar organisatie op te zetten waren strategische keuzes, waar overigens ook bij de uitwerking het nodige fout ging. Strategisch keuzes en strategische risico's behoren dus bij uitstek onder de aandacht van de Raad van Bestuur en raad van Commissarissen te komen. Bij de huidige tekst betwijfel ik of dat wordt bereikt.

b) Doelstellingen. Hoe duidelijk en effectief is dit begrip? Omdat doelstellingen ook belangrijk zijn bij de risicoweging vraag ik veel bedrijven naar hun doelstellingen. Meestal krijg ik geen antwoord of het zijn nietszeggende antwoorden als veel verkopen, aardig zijn voor klanten of goede werksfeer. Kortom, doelstellingen aanhouden als richtinggevend voor goedkeuring van Raad van Commissarissen en als basis voor risicoanalyse e.d. acht ik een buitengewoon zwakke schakel.

c) Diverse zaken moeten aan de Raad van Commissarissen worden voorgelegd. Wat is er tegen om ook te eisen dat de voorstellen van de Raad van bestuur worden voorzien van een risicoanalyse en een plan van aanpak hoe met die risico's zal worden omgegaan. Een dergelijke regeling dwingt de Raad van bestuur te expliciteren welke risico's zij verwacht bij de ingediende plannen. Deze regeling sluit aan bij het beeld van I 1.3.a)

Best practice bepalingen

I. 1.3 **In de vennootschap is een goed 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 en d) een systeem van monitoring en rapportering.**

a) Wat is de ratio om minimumeisen aan de aard van de risicoanalyses te stellen. Waarom alleen aan de operationele en financiële doelstellingen gekoppeld? Moeten niet alle risico's waar een onderneming mee geconfronteerd kan worden onderwerp van aandacht zijn? Turnbull maakt, terecht, geen enkel onderscheid tussen de diverse risico's. Immers alle risico's zijn relevant. Dat risico's aan doelstellingen gekoppeld worden, prima, doelstellingen mogen m.i. nooit bepalend zijn voor aard en omvang van de risicoanalyse.

b) Er moet een gedragscode zijn. Dit wordt niet toegelicht. Wat wordt bedoeld. Zonder toelichting heeft dit instrument geen enkele betekenis.

c) Handleiding voor financiële verslaglegging. Een aangepaste versie van accounting standards? M.i. geen regeling die in het kader van Risk Management en control thuis hoort.

d) Tot slot worden nog genoemd: monitoring en rapportering. Deze facetten moeten terecht onderdeel uitmaken van een volwaardig risk managementsysteem. Maar als deze begrippen niet worden uitgewerkt, vrees ik dat het loze kreten blijven. Niet wordt aangegeven wat moet worden gemonitord /gerapporteerd, hoe moet worden gemonitord /gerapporteerd en door wie moet worden gemonitord /gerapporteerd.

e) Wat ik in deze opsomming mis zijn samengevat de volgende aspecten:
   - De daadwerkelijke evaluatie en management van risico's;
   - Hoe het systeem van interne controle er uit zou moeten zien.;
   - En tot slot, het toetsen, de assurance, zoals de Engelsen het noemen. In lijn met het gezegde: 'vertrouwen is goed, controle is beter', moet het toetsen, de audit, een belangrijke plaats hebben in de opzet van een risicobeheersingsysteem. (Om deze reden is in de Combined Code onder D 2.2.de provisie openomen dat 'Companies which do not have an internal audit function should from time to time review the need for one'). Duidelijk moet worden gemaakt door wie, wat en wanneer wordt getoetst. Als het toetsen niet voldoende aandacht krijgt, hoe weet men dan of al datgene wat aan of door de Raad van Bestuur wordt voorgelegd ook klopt?

Best practice bepalingen

I. 1.4 **In het jaarverslag verklaart het bestuur dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn en geeft het een duidelijke onderbouwing van deze verklaring.**

I. 1.5 **Het bestuur rapporteert in het jaarverslag over de werking van het interne risicobeheersings- en controlesysteem in het verslagjaar. 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.**

a) Zonder 'assurance', wat is de waarde van een dergelijke verklaring. Veel belangrijker is de vraag: Wat is een adequaat en effectief risicobeheersings- en controlesysteem? Als ik nu aan managers zou vragen of zij beschikken over een effectief risicobeheersings- en controlesysteem denk ik dat 9 van de 10 daar positief op zullen reageren. Kortom, er zal een groot verschil zijn tussen dat wat van binnen in de onderneming wordt beleefd en wat de buitenwacht er van vindt. Van belang is dat er een systeem is, dat als meetlat kan fungeren. De Engelsen hebben een uitgewerkt systeem voor interne controle vastgelegd in het Turnbull rapport, de banken hebben nu Bazel II, Australië en Nieuw Zeeland hebben eigen Risk Management standards en tot slot door mij is een Risk Management Protocol opgesteld met 10 verankerpunten.

b) Alleen indien een dergelijk meetlat (is dat misschien de gedragscode waar eerder naar werd verwezen?) van kracht is en de effectiviteit daarvan op een objectieve wijze is aangetoond, pas dan kunnen verklaringen van die strekking in het jaarverslag worden opgenomen.

c) Als ik deze 2 paragrafen vergelijk met die van Turnbull, dan lees ik aldaar dat de Raad van bestuur verantwoordelijk is voor 'reviewing the effectiveness of internal control' Deze verantwoordelijkheid wordt met een groot aantal artikels uitgewerkt. Over de resultaten van dit 'reviewproces' moet de raad van bestuur rapporteren. De directe verantwoordelijkheid van de Raad van bestuur voor de beheersing van risico's wordt in de Engelse aanpak uitdrukkelijk onderkend.

Best practice bepalingen

I. 1.6 **De raad van bestuur rapporteert in het jaarverslag over de gevoeligheid van de resultaten van de vennootschap ten aanzien van externe omstandigheden en variabelen.**

a) Ik kan niet warm lopen voor deze bepaling. In de huidige jaarverslagen wordt, wanneer over risico's wordt gesproken, vaak gewag gemaakt van deze gevoeligheden. Het zijn meestal nietszeggende en voor de handliggende statements. Als men aan deze gevoeligheden ook niet aangeeft hoe men deze gevoeligheden denkt te pareren hebben deze verklaringen geen zin.

I Raad van commissarissen / Taak en werkwijze / Principe

De raad van commissarissen heeft tot taak toezicht te houden op de raad van bestuur en op de algemene gang van zaken in de vennootschap en de met haar verbonden onderneming. De raad van commissarissen 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 de bij de vennootschap betrokkenen af. De raad van commissarissen is verantwoordelijk voor de kwaliteit van zijn eigen functioneren.

Best practice bepalingen

II. 1.4 **De raad van commissarissen draagt zorg voor de ontvangst, het opslaan en behandeling van klachten die door de vennootschap worden ontvangen ten aanzien van de financiële verslaggeving, de interne risicobeheersings- en controlesystemen en de audit. Interne "klokkenluiders" hebben zonder gevaar voor hun rechtspositie de mogelijkheid te rapporteren over onregelmatigheden in de hiervoor genoemde zaken en om klachten over de leden van de raad van bestuur te melden aan de voorzitter van de raad van commissarissen.**

a) Onderscheid wordt gemaakt tussen externe, aan de vennootschap gerichte klachten en interne klachten. Er wordt gewezen op een mogelijkheid van klokkenluiders om te rapporteren. Niet wordt bijgezegd bij wie. Suggestie is ondernemingen te verplichten een 'echte klokkenluiders' regeling te hebben.

II. 1.6 **Tot de algemene taken van de raad van commissarissen kunnen worden gerekend toezicht op onder andere i) de realisatie van de doelstellingen van de vennootschap, ii) de strategie en de risico's verbonden aan de ondernemingsactiviteiten, iii) de opzet en de werking van de interne risicobeheersings- en controlesystemen, iv) het financiële verslaggevingsproces en v) de naleving van de wet- en regelgeving.**

a) De toezichthoudende rol van de Raad van commissarissen is een goede zaak. Maar hoe is die toezichthoudende rol waar te maken. Alleen als zij kan beschikken over getoetst, objectieve informatie, welke aan van tevoren gestelde eisen voldoet. Alleen als er helder omschreven Risk Management en Internal Controle framework is kan zij naar behoren die toezicht houdende rol waarmaken.

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

a) In deze bepaling wordt gesproken over de verplichting van de Raad van bestuur om de beoordeling van opzet en werking van het risicobeheersingsysteem met de Raad van commissarissen te bespreken.. De verplichting tot beoordelen, 'reviewen', wordt niet opgenomen in de taakbeschrijving van de Raad van bestuur.
b) Tenminste éénmaal per jaar bespreken van de risico's lijkt mij erg mager. Dat moet telkenmale gebeuren als daartoe aanleiding is. Het zou een permanent agendapunt moeten zijn. De bespreking van de risico's moet los gezien worden van de jaarlijkse beoordeling van het risicobeheersingsysteem.

II. 4 Samenstelling en rol van drie kerncommissies van de raad van commissarissen / Principe.

De raad van commissarissen stelt uit zijn midden in ieder geval een auditcommissie alsmede een remuneratiecommissie en een selectie- en benoemingscommissie samen. De raad van commissarissen blijft verantwoordelijk voor besluiten, ook als deze worden voorbereid door uit de raad van commissarissen samengestelde commissies.

<u>Best practice bepalingen</u>

II. 4.2 **Voor iedere commissie wordt een reglement opgesteld. Het reglement geeft aan wat de rol en verantwoordelijkheid van de betreffende commissie is, haar samenstelling en op welke wijze zij haar taak uitoefent. De reglementen en de samenstelling van de commissies worden in ieder geval op de website van de vennootschap geplaatst.**

Auditcommissie

II. 4.6 De auditcommissie heeft in ieder geval de volgende taken:

- **a) toezicht op de werking van de interne risicobeheersings- en controlesystemen, waaronder het toezicht op de naleving van de relevante wet- en regelgeving en het toezicht op de werking van gedragscodes;**
- **b) toezicht op de naleving van aanbevelingen en opvolging van opmerkingen van in- en externe accountants**
- **c) toezicht op het functioneren van de interne accountantsdienst**

a) De wens om de te naamspelling van deze commissie uit te breiden tot een Risk en auditcommissie heb ik eerder toegelicht.
b) Indien aan de auditcommissie de rol van toezichthouder wordt toebedeeld, dan zal duidelijk moeten worden aangegeven hoe deze commissie die rol kan waar maken en welke bevoegdheden aan die commissie worden toegekend.
c) Waarom worden specifieke risicovelden als de toepassing van wet- en regelgeving en de naleving van gedragscodes, wat die ook mogen zijn, genoemd? Men zal moeten aangeven waarom deze onder het directe toezicht staan van de auditcommissie. Indien toch noodzakelijk, dan moeten ze apart worden genoemd en niet worden opgenomen onder a) waar alleen over systemen wordt gesproken.
d) Ten overvloede, er moet een helder beeld bestaan wat de interne en externe accountants in het kader van de risicobeheersing doen. Toezicht op het functioneren alleen is niet voldoende. Het gaat ook om de inhoud en daarbij behorende verantwoordelijkheden en bevoegdheden. Tegelijk is relevant de relatie tussen de interne en externe accountant te vermelden. Welke controle voeren op hun beurt de externe accountants weer uit?

IV. 4 Relatie en communicatie van de externe accountant met de organen van de vennootschap Principe

De externe accountant woont de vergaderingen van de auditcommissie en van de raad van commissarissen bij waarin over de periodieke financiële externe verslaglegging wordt besloten. De externe accountant rapporteert zijn bevindingen betreffende het onderzoek van de jaarrekening gelijkelijk aan het bestuur en de raad van commissarissen.

Best practice bepalingen

IV. 4.2 **De externe accountant woont eveneens de vergaderingen van de auditcommissie bij waarin wordt gesproken over de periodieke financiële externe verslaggeving. Hierin komen de bevindingen van de externe accountant aan de orde, alsmede de controleaanpak en de risicoanalyse.**

IV.4.3 **Het verslag van de externe accountant ingevolge artikel 2:393 lid 4 BW bevat datgene wat de externe accountant met betrekking tot de jaarrekening en het jaarverslag en de overige gegevens onder de aandacht van het bestuur en de raad van commissarissen wil brengen. Daarbij kan aan de volgende onderwerpen worden gedacht:**

B. Met betrekking tot de werking van de interne risicobeheersings- en controlesystemen (inclusief de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking) en de kwaliteit van de interne informatievoorziening:

- **verbeterpunten, geconstateerde leemten en kwaliteitsbeoordelingen;**
- **opmerkingen over bedreigingen en risico's voor de vennootschap en de wijze waarop daarover in de te publiceren gegevens gerapporteerd dient te worden;**
- **naleving van statuten, instructies, regelgeving, leningsconvenanten, vereisten van externe toezichthouders etc.**

a) De tekst van IV 4.2 roept twijfels op ter zake de reikwijdte. Gaat het hier alleen om de controle door de externe accountant van de financiële verslaglegging of gaat het om alle controles en risicoanalyses? Deze onduidelijkheid onderstreept de relevantie van een duidelijke taakafbakening tussen de interne en externe accountants.
b) Ook onder B worden zaken specifiek benoemd die twijfels oproepen of het hier gaat om alleen financiële zaken of over een veel ruimere aandachtsterrein.
c) Ook hier worden specifieke voorbeelden (risico's) genoemd zoals de geautomatiseerde gegevensverwerking en informatievoorziening. Waarom deze speciaal benoemd?

d) Er wordt hier voor het eerst gesproken over verbeterpunten, elementaire zaken die tot het Risk Managementproces behoren. Waarom hier? Waarom niet eerder in het rapport als gesproken wordt over de opzet van een risicobeheersingsysteem.
e) Voorts wordt hier voor het eerst over 'bedreigingen ' gesproken. Waarom? Wat wordt ermee bedoeld?
f) Tot slot, er worden specifieke zaken benoemd als het voldoen aan eisen van statuten, etc., de compliance. Ook hier weer de vraag, waarom specifiek benoemd en hoe verhoudt e.e.a zich tot de rol van de interne accountantsdienst?

Conclusie

De samenleving verwacht dat ondernemingen zo goed mogelijk hun risico's onder controle hebben. De afgelopen jaren van grote economische groei en de economische terugval daaropvolgend hebben de noodzaak daartoe extra onderstreept. Bedrijven en toezichthouders worden steeds meer aangesproken op hun verantwoordelijkheid in deze. Kortom, risk management moet.
Echter de praktijk is weerbarstig. Risk Management op corporate niveau heeft wel enige, groeiende, belangstelling, de uitwerking schiet nog danig tekort.
Er rest dan maar één conclusie, als ondernemingen niet zelf de nodige actie nemen, dan moeten zij daartoe worden aangespoord, zo niet worden gedwongen.

Internationaal wordt dat ook zo gevoeld. Ik heb eerder verwezen naar het Turnbullrapport over Internal Control, naar de Bazel II regelgeving voor banken, naar de Risk Management standards van Australië en Nieuw Zeeland.

De nieuwe Corporate Governance regeling zou een fantastische gelegenheid zijn om ondernemingen op een heldere wijze aan te sporen, te dwingen, hoe risk management op een effectieve manier gestructureerd zou moeten zijn. Het zou een inspirerend document kunnen zijn waaruit niet alleen voor beursgenoteerde ondernemingen, maar ook andere ondernemingen en non- profitorganisaties kunnen afleiden dat ook voor hen structurele risicobeheersing een noodzakelijke aangelegenheid is en hoe die structuur er dan uit zou kunnen zien. De nieuwe Corporate Governance regeling zou daarbij normatief kunnen zijn.

Deze concepttekst van Corporate Governance levert helaas die nodige inspiratie niet op. Het is geen document dat belanghebbenden het vertrouwen kan geven dat ondernemers beter dan voorheen met risico's om zullen gaan. Met al mijn opmerkingen heb ik aangetoond dat het voorstel rammelt aan alle kanten. Het is geen weerslag van de eisen die aan een goed Risk management systeem moeten worden gesteld. In de aanbevelingen zal ik dit nader uitwerken.

Aanbevelingen tot een betere opzet van Risk Management in de Corporate Governance regeling.

a) In het Risk Management model moeten de diverse stappen van het Risk managementproces duidelijk worden benoemd te weten: de risicoanalyse, de weging van risico's en evaluatie, de beheersingsmaatregelen, de monitoring, het toetsen en de rapportage.
b) In het model moeten de verantwoordelijkheden van de diverse functies helder worden geformuleerd te weten: van de Raad van Bestuur, de Raad van commissarissen (risk – en auditcommissie), lijnmanagement, risk managers, interne auditors en externe accountants.
c) Het is denkbaar dat uitwerking hiervan in de Coprorate Goverance teveel tekst vraagt. Beperk dan tot enkele niet mis te verstane hoofdlijnen (in de Combined Code worden slechts 2 paragrafen gewijd aan Internal Control) maar stel aansluitend een document op dat e.e.a uitwerkt zoals in het Trunbullrapport (15 pagina's).
d) Details, specificaties, voorbeelden moeten zo veel mogelijk worden vermeden. Ze kunnen aangegrepen worden voor het minimaliseren van de aanpak, ze kunnen leiden tot misverstanden. Hoe algemener de structuur wordt opgesteld des te beter. Laat de ondernemingen zelf uitmaken hoe zij e.e.a. willen aanpakken en waar zij de accenten op willen leggen. Elk richtinggevend voorbeeld in de tekst doet afbreuk aan de eigen situatie van de onderneming.

e) In het model moet uitgegaan worden van een risk management theorie die algeheel, uniform en ondernemingbreed wordt onderschreven en wordt toegepast. Het gaat dan om de frequentie en wijze van uitvoer van risicoanalyses, over weging en prioriteren van risico's op corporate niveau en lager in de organisatie, over de acceptatie en financiering van risico's, over de aard en omvang van de beheersingsmaatregelen, over risk indicators en schaderegistratie, over monitoring, toetsen en de wijze van interne en externe rapportage. Een dergelijke coherente aanpak is niet te realiseren als de interne auditors risk based auditing niet als uitgangspunt hanteren en de risk managers geen functie krijgen op corporate niveau.

f) 'Assurance' is voor binnen als buiten de onderneming buitengewoon belangrijk. Men moet kunnen vertrouwen dat de onderneming daadwerkelijk voldoet aan nader aangegeven standaards. Aan nietszeggende statements heeft men niets. Permanent moet de objectiviteit van de informatie worden bewaakt. Iedere onderneming zal formeel een model moeten hebben waarin alle risk management en control elementen worden beschreven en waarlangs intern en extern wordt getoetst. Dat model is richtinggevend en moet algemeen kenbaar zijn voor binnen als buiten de onderneming. Publicatie op het web is een voor de handliggende suggestie. Zolang geen ander document beschikbaar is zou mijn Risk Management Protocol die functie kunnen hebben.

Slot

De paragrafen in de concepttekst Corporate Governance betreffende risicobeheersing hebben in de pers geen rumoer opgeroepen. Dat moet nu wel gaan gebeuren. Dat is nog meer nodig, indien men de aandacht voor risicobeheersing in ondernemingen op een hoger plan wil brengen. Hopelijk leidt dit document binnen uw commissie en daarbuiten tot een discussie over de vraag hoe daadwerkelijk Risk Management binnen ondernemingen gestructureerd zou moeten zijn.
De commissie Corporate Governance kan hierbij een sleutelrol vervullen. Het is mijn wens dat de Commissie die rol met beide handen aangrijpt.
In ieder geval zal ik er voor zorgen dat deze tekst op mijn website wordt geplaatst.

Mr R.A.Vroom
VRIMS Integraal Risk Management Services
16 juli 2003
www.riskmanagement.nl

Verwijzingen:

De Nederlandse Corporate Governance code 1 juli 2003
Concept: een uitnodiging voor commentaar
http://www.commissiecorporategovernance.nl/Conceptcode

The Combined Code, Principles of Good Governance and Code of Best Practice
http://www.eccg.org/codes/country_documents/uk/combined_code.pdf

Internal Control,
Guidance for Directors on the Combined Code
(The Institute of Chartered Accountants)
http://www.icaew.co.uk/viewer/index.cfm?AUB=TB2I_6342

RISK Management and the value added by Internal Audit
(The Institute of Chartered Accountants)
http://www.icaew.co.uk/viewer/index.cfm?AUB=TB2I_50771

Basel Committee on Banking Supervison of Operational Risk
Best Practice bepalingen
(bijlage)

Austalian and New Zealand Risk Management Standards (AS/NZS 4360:1999)
www.standards.com.au

Risk Management Standards van de Association of Insurance and Risk Managers (AIRMIC)
http://www.narim.com/files/AIRMIC_RiskManagementStandard.pdf

Risk Management Protocol, 10 Verankerpunten en toelichting
VRIMS Integraal Risk Management Services
(bijlage)

Basel Committee on Banking Supervision

Part 1: Sound Practices tor the Management and Supervision of Operational Risk. December 2001 Page 3-5.

13. In developing these sound practices, the Committee has drawn upon its existing work on the management of other significant banking risks, such as credit and liquidity risk, and the Committee believes that similar rigour should be applied to the identification, measurement, monitoring and control of operational risk. Nevertheless, it is clear that operational risk differs from other banking risks in that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity, and that this impacts the risk management process. In common with its work on other banking risks, the Committee has structured this sound practice paper around a number of principles. These are as follows:

Developing an Appropriate Risk Management Environment

Principle 1: The board of directors2 should be aware of the major aspects of the bank's operational risks as a distinct and controllable risk category and should approve and periodically review the bank's operational risk strategy. The strategy should reflect the bank's tolerance for risk and its understanding of the specific characteristics of this risk category. The board should also be responsible for approving the basic structure of the framework for managing operational risk and ensuring that senior management is carrying out its risk management responsibilities.

Principle 2: Senior management should have responsibility for implementing the operational risk strategy approved by the board of directors. The strategy should be implemented consistent I y throughout the whole banking organisation, and al I levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's products, activities, processes and systems.

Principle 3: Information flows within the banking organisation play a key role in establishing and maintaining an effective operational risk management framework. Communication flows within the bank should establish a consistent operational risk management culture across the bank. Reporting flows should enable senior management to monitor the effectiveness of the risk management system for operational risk, and also enable the board of directors to oversee senior management performance.

Risk Management: Identification, Measurement, Monitoring, and Control

Principle 4: Banks should identify the operational risk inherent in all types of products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken the operational risk inherent in them is subject to adequate assessment procedures.

Principle 5: Banks should establish the processes necessary for measuring operational risk.

Principle 6: Banks should implement a system to monitor, on an on-going basis, operational risk exposures and loss events by major business lines.

Principle 7: Banks should have policies, processes and procedures to control or mitigate operational risk. Banks should assess the costs and benefits of alternative risk limitation and control strategies and should adjust their operational risk exposure using appropriate strategies, in light of their overall risk profile.

Role of Supervisors

Principle 8: Banking supervisors should require banks to have an effective system in place to identify, measure, monitor and control operational risks as part of an overall approach to risk management.

Principle 9: Supervisors should conduct, direct I y or indirectly, regular independent evaluation of a bank's strategies, policies, procedures and practices related to operational risks. Supervisors should ensure that there are effective reporting mechanisms in place which allow them to remain apprised of developments at banks.

Role of Disclosure

Principle 10: Banks should make sufficient public disclosure to allow market participants to assess their operational risk exposure and the quality of their operational risk management.