



**Reactie op rapport 'Monitoring Commissie Corporate Governance Code' over de naleving van de Code.
(december 2005)**

'Handen af van de bepalingen over de Interne risicobeheersings- en controle systemen in de Code'!

Na lezing van het rapport van de Commissie over de naleving van de Nederlandse Corporate Governance Code kan er naar mijn mening maar één conclusie zijn: blijf van de tekst van de Code af! De Commissie denkt daar anders over. Zeker als dat een 'zware' commissie is die na bestudering van de resultaten over de naleving, na consultatierondes en met input van geïnteresseerde organisaties voorstellen tot wijziging doet, dan moet je met goede argumenten komen om toch een andere mening te zijn toegedaan. In het volgende zal ik die trachten naar voren te brengen.

De argumenten om tot voorstellen te komen.

De Commissie stelt voor om de verklaring over de adequaatheid (wie heeft overigens dit kwaliteitscriterium bedacht dat internationaal nergens wordt genoemd?) en effectiviteit van het interne risicobeheersings- en controlesystemen door het bestuur van de onderneming in het jaarverslag op te nemen (II 1.4) anders te redigeren. Als belangrijkste argument wordt aangegeven dat ondernemingen moeite hebben met de afgifte van een dergelijke verklaring, vrezende verkeerde conclusies en een verhoogde aansprakelijkheid. Die verkeerde conclusies zouden dan liggen in de veronderstelling dat niets meer fout kan gaan.

Laat ik beginnen te zeggen dat in het algemeen ondernemers moeite hebben met 'systemen', modellen of structuren, die hen dwingt op een bepaalde manier te handelen. Ondernemers willen vrijheid, ruimte hebben om naar eigen inzicht te kunnen handelen. Dat de Code ondernemers dwingt wat meer aandacht te besteden aan risico's, dat vinden ze uiteindelijk nog wel goed, maar dan liefst niet volgens een van boven opgelegd model. Dus die 'natuurlijke' terughoudendheid van ondernemers valt nog wel te verklaren. Ik vrees echter dat niet zo zeer die verkeerde conclusies of vermeende aansprakelijkheid de reden zijn, maar veeleer het feite dat ondernemingen nog niet over een goed werkend systeem beschikken. Daarover later meer.

Overigens vind ik de veronderstelde de risicoloosheid van de onderneming, die aandeelhouders en anderen als conclusies aan een dergelijke verklaring zouden verbinden wel erg vergezocht. Verrassend dat de Commissie die vrees overneemt. Immers het moet toch duidelijk zijn dat het beschikken over een dergelijk systeem geen enkele indicatie wil geven dat er niets meer fout kan gaan. Een simpel voorbeeld Als je huis beschikt over alarmsystemen, je ramen en deuren zijn beveiligd met goede sloten, dan nog kan er toch worden ingebroken. Immers dieven kunnen er doorheen breken, maar deuren kunnen ook open blijven of ramen kan men vergeten af te sluiten Kortom, het adequate en effectieve beveiligingssysteem, waar de huiseigenaar met gerust hart een II 1.4 verklaring over af zou kunnen leggen, beperkt doch sluit niet het risico volledig uit.

En dan de vrees voor aansprakelijkheid. Mogelijk gevoed door de idee van die verkeerde conclusies, wordt een druk op de aansprakelijkheid verondersteld. Verrassend, ik zou juist het tegendeel veronderstellen. Juist bij het ontbreken van een verklaring wordt de aansprakelijkheid vergroot. Immers indien de verklaring ontbreekt geef je te kennen dat de onderneming niet beschikt over een dergelijk systeem, waarover een 'goed' ondernemer wel zou moeten kunnen beschikken. Dat maakt de onderneming kwetsbaar. Als er dan iets mis gaat dan moet je sterk in je schoenen staan te kunnen verklaren dat je er alles aan hebt gedaan om een en ander te voorkomen.

Een verwijzing naar internationale beleggers is interessant. SOX en Turnbull stellen simpel, zonder nadere toelichting of verfijning, zoals de commissie voorstelt, dat een directie de 'effectiveness of the



internal controlsystem' moet aangeven. Dat is, kun je gerust zeggen, internationale usance. Niet de huidige verklaring, die in of meer aansluit bij de internationaal gebruikelijke, roept vraagstekens bij de internationale beleggers op, maar juist een inperking of verfijning daarvan.

Kortom, het feit dat die verklaring nauwelijks wordt afgegeven en de veronderstelde argumenten daarvoor zijn voor mij geen enkele reden om nu al, zeg na 1 jaar na de Code, om aanpassing van de Best Practice bepalingen over te gaan.

De voorstellen zelf.

Allereerst het onderscheid tussen financiële verslaggeving risico's en andere risico's, zoals operationele risico's.

Nog afgezien van het feit dat de z.g. verslaggeving risico's geen 'andere' risico's zijn maar ook operationele risico's, net zoals compliance risks ook operationele risico's zijn, is niet aangegeven wat financiële verslaggeving risico's zijn. Fraude? IT? Communicatie? Vertaling? Waardebepaling? Alleen risico's die het proces van verslaggeving betreffen of ook risico's die de inhoud aangaan? In het SEC rapport ** worden als voorbeeld IT- risico's aangehaald. IT- risico's kunnen van invloed zijn op de betrouwbaarheid van de financiële gegevens, maar dat hoeft niet.

Zolang niet helder is wat met deze risicocategorie bedoeld wordt, moet dat onderscheid ook niet gebruikt worden.

In de toelichting wordt aangegeven dat wat betreft de financiële verslaggeving risico's: 'verklaard moet kunnen worden dat deze onder controle zijn'. Wat wordt met de 'under control' statement bedoeld? Dat deze risico's worden beheerst? Dat er niets fout kan gaan of dat er voldoende beheersingsmaatregelen van toepassing zijn (en getoetst worden?) zodat als er onverhoopt toch iets gebeurt de gevolgen beperkt zijn? Is dat dan iets anders dan een effectief risico en controlesysteem? Kortom, nieuwe begrippen, nieuwe vragen en onduidelijkheden.

Voorts wordt een onderscheid gemaakt ten opzichte van andere risico's. Voor die andere risico's kan worden volstaan met een beschrijving van het risicobeheersings- en controlesysteem. Er wordt daarbij toegelicht dat sommige risico's beter zijn te beheersen dan andere, dat sommige risico's beter zijn te kwantificeren dan andere. Geldt dat niet m.m. ook voor de zg verslaggeving risico's? Veelal worden die geassocieerd met fraude. In hoeverre is het fraude risico te beheersen? In hoeverre is het fraude risico te kwantificeren? Wat rechtvaardigt uiteindelijk het onderscheid tussen verslaggeving risico's en andere risico's. Ik zou het niet weten.

De Commissie komt ten aanzien van financiële verslaggeving risico's tot de volgende Best Practice bepaling: dat t.a.v. deze risico's wordt verklaard dat het risicobeheersings –en controlesystemen een redelijke mate van zekerheid geven dat de financiële verslaggeving geen onjuistheden van materieel belang bevat. Is dit, het ontbreken van onjuistheden, misschien wat men bedoelt met de under control statement?

Hier wordt de effectiviteit van de systemen vervangen door het begrip 'redelijke mate van zekerheid'. Waarin zit het verschil? Waarom in dit kader het kwaliteitselement van een systeem vervangen door doelstellingen wat je met een systeem wilt bereiken

In het begin heb ik me afgevraagd wat nu financiële verslaggeving risico's zijn. Misschien wordt nu hier het antwoord gegeven namelijk: risico's die tot onjuistheid van de financiële verslaggeving leiden. Interessanter is echter te constateren dat in deze verklaring bijna letterlijk de tekst van SOX 302,2 wordt overgenomen, waarin wordt aangegeven dat de (signing) officer dient aan te geven dat 'the report does not contain any untrue statement of a material fact or omit to state a material fact'. Separaat dient de signing officer te verklaren dat het interne controle systeem effectief en geëvalueerd is.

De samenvoeging in het advies van de Commissie van de de 2 verklaringen die in SOX los van elkaar worden genoemd is verwonderlijk. Opvallender is echter de toevoeging over de afwezigheid van ‘onjuistheden van materieel belang’. Deze toevoeging van het mogelijk effect van het risico- en beheersingsysteem is nieuw, wordt verder niet gedragen door de tekst van de Code en wordt verder ook niet aangegeven of vereist voor andere risico’s.

Aanvullend moet volgens de nieuwe Best Practice bepaling worden verklaard dat de risicobeheersings- en controlesystemen t.a.v. financiële verslagleggingsrisico’s naar behoren hebben gewerkt. Wat is naar behoren? Waarin verschilt ‘naar behoren’ van ‘effectief’? Waarom voor deze groep risico’s iets anders verklaren dan voor de andere operationele risico’s?

Ter zake de andere risico’s is volstaat een beschrijving van de systemen op basis van de geïdentificeerde belangrijke risico’s.

Ook hier een paar opmerkingen.

Risico- en beheersingsystemen zijn generieke systemen zoals COSO, maar dan nog meer uitgewerkt. Het zijn continue processen van inventariseren en beoordelen van risico’s, het nemen van maatregelen, het testen en monitoren en van de verslaggeving.

Uit deze processen vloeien uiteindelijk beheersingsmaatregelen voort, al of net intensieve betrokkenheid van management, al of niet discussie over risicoacceptatie of verzekering, al of niet extra investeringen etc.etc.

Kortom het is van tweeën één. Of men beschrijft de systemen of men beschrijft hoe men met bepaalde risico’s omgaat. Het zijn 2 verschillende zaken, die niet met elkaar verward moeten worden.

Als toegestaan wordt dat de verklaring beperkt wordt tot een beschrijving van de omgang met bepaalde belangrijke risico’s, dat misschien in een vergadering van aandeelhouders een veel leukere discussie kan opleveren dan een discussie over een risicobeheersings – en controlesysteem, dan is er echt sprake van een aanzienlijke verschraving van datgene wat de Code bedoelt en in andere regelgeving wordt vereist, namelijk een statement over de effectiviteit van het risicobeheersings- en controlesysteem.

Als dat niet bedoeld wordt, wat ik veronderstel naar aanleiding van de toelichting waarin ‘een beschrijving van het risico- en beheersingsysteem op hoofdlijnen’ wordt voorgesteld, dan dient men dat in de voorgestelde tekst niet aan te geven als een omschrijving van risico- en beheersingsysteem op basis van geïdentificeerde risico’s. Ik hoop duidelijk te hebben gemaakt dat de ‘beschrijving van het systeem op hoofdlijnen’ iets anders is dan een beschrijving van de belangrijke risico’s.

Mijn conclusie.

Het zal duidelijk zijn dat ik verre van gelukkig ben met de nieuwe aanpassingen. Zij lossen niets op, creëren alleen maar nieuwe verwarring en zij leiden af van datgene waar het uiteindelijk om gaat: de opzet en instandhouden door ondernemingen van effectieve risicobeheersings- en controlesystemen. De Code is pas net een jaar oud, staat aan het begin van een hopelijk lange successtory. Waarom nu al na een jaar de tekst wezenlijk aanpassen. Laten we ons inspannen er voor te zorgen dat ondernemers uiteindelijk wel die verklaring gaan afgeven.

COSO, Turnbull en SOX hebben allemaal verschillende historie en kennen verschillende doelstellingen, eensgezind zijn ze in het streven naar een effectief intern risicobeheersings- en controlesysteem. De betekenis en uitwerking van SOX voor ondernemingen heeft veel vragen opgeroepen, (zie het SEC rapport*) geen enkel twijfel bestaat er over het uitgangspunt SOX: namelijk de noodzaak te beschikken over een effectief risicobeheersings- en controlesysteem (for financial reporting) en dat te verklaren nadat het getest is.



Wat moet dan wel gebeuren?

Laat ik eerst dit nog eens zeggen. Risicobeheersings- en controlesystemen zijn bedoeld om risico's effectiever te beheersen. Betere beheersing van risico's leidt tot meer grip op de continuïteit van de onderneming en tot meer vertrouwen in de toekomst van de onderneming. Risicobeheersings- en controlesystemen zijn er niet to please een of andere instantie of de heer Tabaksblat, maar zijn slechts middelen om doelen te bereiken. Hoe effectiever deze systemen werken, hoe meer vertrouwen in de onderneming gerechtvaardigd is.

Hoe die systemen er uit moeten zien, dat is aan de onderneming zelf om dat aan te geven. Dat behoeft ook niet te worden beschreven in het Jaarverslag. Volstaan kan worden met een verklaring dat er een systeem is, dat getest is en waar de accountants zich mee kunnen verenigen.

Dat geldt eveneens ter zake de noodzaak om allerlei risico's te beschrijven. Dat zijn veelal open deuren. De echte problemen van de organisatie zullen, terecht toch niet in het Jaarverslag worden vermeld. Kortom, veel schiet je met dat soort voorschriften niet mee op.

Maar hoe zou een dergelijk effectief risicobeheersings- en controlesysteem er dan uit moeten zien? Welke criteria leggen de auditcommissie en de accountant aan om daadwerkelijk van een effectief systeem te kunnen spreken? Een niet zo een simpele vraag. In de praktijk zie je dat risicobeheersing allerlei verschijningsvormen kent. Dat kan per lokatie of business unit verschillen, dat kan per onderwerp verschillen, dat kan per proces verschillen, van zeer oppervlakkig tot zeer gedetailleerd. Ondernemingen proberen daar nu wat meer uniformiteit in aan te brengen soms door van boven af structuren op te leggen, door het ontbreken van draagvlak niet altijd effectief, soms vanonder af aan, bottom up. Ook dat gebeurt niet altijd met succes omdat steun van management nog al eens ontbreekt. Kortom, een moeizaam en langdurig proces dat alleen maar steun verdient. Banken, die nu voor de implementatie van Bazet II staan, kunnen daar over mee praten.

Die noodzakelijke morele en praktische steun komt wat mij betreft niet door de tekst van de Code af te zwakken. Veel meer effect heeft 'to improve the process going forward' zoals in de toelichting van de SEC naar aanleiding van het vele commentaar op de ontwikkeling van SOX wordt aangegeven:

The entire financial reporting community, including investors, auditors, management, and regulators, shares the common goal of improving the reliability of financial reporting and the information available to the market. With the experience of the first round of Section 404 implementation, we should continue to focus on the lessons learned and ways to improve the process going forward. Section 404 is too important not to get right, but getting it right requires both effective and efficient implementation.

Om ondernemingen en zij die betrokken zijn bij de validatie van de systemen te helpen, heb ik 2 documenten opgesteld. Het Risk Management Protocol en het Risk Management Maturity Model. Het Protocol geeft een handvat over de inrichting van het risicobeheersing- en controlesysteem, het Maturity Model geeft een indicatie hoe ver men met de implementatie van het Protocol is gevorderd.

Hopelijk draagt deze notie bij tot de nodige inspiratie van ondernemers door te gaan op de ingeslagen weg en niet te wanhopen of te klagen als het iets tegen zit. Wij allen zijn daarbij gebaat.

Samenvattend kan gesteld worden dat naar mijn mening de argumenten om na 1 jaar ervaring met de Code de tekst aan te passen niet valide zijn, dat de voorgestelde wijzigingen onduidelijk zijn, die de normen van risicobeheersing waaraan een ondernemer overeenkomstig de Code zou moeten voldoen



eerder verslappen dan versterken. Ook internationaal gezien een slechte zaak. Kortom, blijf bij de internationaal kort maar helder geformuleerde regel welke ondernemers oproept te verklaren 'that the internal control system is effective'.

Tot slot nog dit.

Het is jammer dat bij de consultatie van de Commissie over een oordeel over de naleving geen mensen zijn betrokken die in de praktijk iets te maken hebben met risk management.

In het bijzonder denk ik daarbij aan mijn persoon. Uiteindelijk is het mijn commentaar op de concept Code Tabaksblad geweest dat er toe heeft geleid dat een verwijzing naar COSO in de toelichting bij de Code is opgenomen.

Mr. R.A.Vroom
VRIMS Integraal Risk Management Services
035-5381555

www.riskmanagement.nl

***Commission Statement on Implementation of Internal Control Reporting Requirements
2005-74**

****Staff Statement on Management's Report on Internal Control Over Financial Reporting**

**Division of Corporation Finance Office of the Chief Accountant
U.S. Securities and Exchange Commission
May 16, 2005**