



## **De definitieve Code Corporate Governance, enige beschouwingen vanuit risicoperspectief.**

In de Code van Commissie Peters 'De Veertig Aanbevelingen' (juni 1997) staat in zeer algemene termen iets over risicobeheersing. De aanbevelingen 17 en 21 zijn daarvan het meest bekend. (zie de bijlage)

Ik had de hoop dat de Commissie Tabaksblat in de nieuwe Code de overtuiging van de noodzaak van een structurele aanpak van Risk Management zou uitstralen. Of die hoop bewaarheid is, in het komende probeer ik daar een antwoord op te geven.

Eerst een terugblik. De Commissie Peters.

De uitgangspunten van de Commissie Peters kunnen als volgt worden samengevat:

- Het interne beheerssysteem valt onder verantwoordelijkheid van het Bestuur, die daarover één keer per jaar aan de Raad van Commissarissen moet rapporteren, het wordt gezien als een proces tot verkrijgen van zekerheid over het behalen van doelstellingen en is gefocust op doelstellingen, strategie en de financiële huishouding, met vermelding van enkele risico's met name.
- De in- en externe accountant / auditor hebben een rol als adviseur
- De auditcommissie heeft een rol als toezichthouder.

Wat zegt de Commissie Tabaksblat hierover? Ik zal relevante elementen van de definitieve Code eruit lichten.

- Er wordt niet meer gesproken van een intern beheerssysteem, maar van een intern risicobeheersings- en controlesysteem. Het woord 'risico' wordt toegevoegd, niet wordt uitgelegd wat het verschil is tussen een beheersings- en een controlesysteem.
- Risicoanalyses 'van de doelstellingen' worden als instrument gezien van een interne beheersings- en controlesysteem.
- Een gedragscode moet op het weg worden geplaatst. Niet wordt toegelicht over wat voor een soort gedragscode het gaat.
- Er moet een systeem komen van monitoring en rapportering.
- In het jaarverslag moet door het bestuur de effectiviteit van het interne risicobeheersings- en controlesysteem worden verklaard. In de toelichting op enkele begrippen van de Code wordt eraan toevoegend dat het 'in de rede ligt dat in de verklaring wordt aangegeven welk raamwerk of normenkader (bv COSO) het Bestuur heeft gehanteerd bij de evaluatie'.
- De Raad van Commissarissen houdt o.a. toezicht op de strategie en de risico's verbonden aan de ondernemingsactiviteiten en op de opzet en de werking van de interne risicobeheersings- en controlesystemen. Dit laatste is ook een taak van de auditcommissie. De oude aanbeveling 17 wordt overgenomen.
- De interne accountant heeft een belangrijke rol bij het beoordelen en toetsen van de interne beheersings- en controlesystemen.
- De externe accountant moet in zijn verslag aan Bestuur en Raad van Commissarissen zijn bevindingen over het interne beheers- en controlesysteem doorgeven.

Terwijl in het rapport Peters nog met een algemene verwijzing naar een beheerssysteem werd volstaan, in de huidige Code worden de contouren van een risicobeheersingssysteem scherper neergezet. Ik zal dit toelichten.

In de nieuwe opzet wordt verwezen naar een intern 'control' raamwerk als COSO, er wordt gesproken over uit te voeren risicoanalyses, over monitoring en rapportering. De in- en externe accountants



waren adviseur maar worden nu verantwoordelijk voor het beoordelen van beheersingssystemen en moeten daarover rapporteren.

Het Bestuur en de Raad van Commissarissen / Auditcommissie worden nog eens expliciet genoemd als resp. verantwoordelijke voor en toezichhouder op de kwaliteit van het risicobeheersingssysteem. Kortom, een Risk Managementstructuur, zoals risk managers die graag aan ondernemingen presenteren, is in de nieuwe code Tabaksblat zichtbaar geworden.

De opzet, verwoord door de commissie Tabaksblat heeft weliswaar nog niet de heldere contouren zoals aangegeven in het Turnbullrapport over Internal Control, de Bazel II regelgeving voor banken of de Risk Management standards van Australië en Nieuw Zeeland.

Toch is de nieuwe Code, vergeleken met het rapport Peters, een hele stap vooruit. Risk managers, auditors en adviseurs op dit terrein kunnen nu naar ondernemingen toe stappen en met de Code in hand tegen het bestuur zeggen dat de Code de toepassing van Risk Management c.q het bezit van een herkenbaar risicobeheersings- en controlesysteem voorschrijft.

Aan de slag dus.

Toch blijf ik zitten met de vraag hoe je nu een dergelijk risicobeheersings- en controlesysteem moet zien. De Code is gezien de gebruikte terminologie daar niet duidelijk in.

Bij COSO, Thurnbull en recent bij de Amerikaanse Sarbanes-Oxley Act (2002) is Internal Control het centrale begrip. Het is een begrip dat duidt op beleid, procedures en activiteiten om risico's 'under control' te krijgen en te houden. Het 'under control' krijgen is een proces dat je kunt beschrijven en waarover je kunt rapporteren en verantwoording over af kunt leggen (zie Sarbanes.Oxley Act). Een formele, top down en accountant georiënteerde aanpak.

Vooraf COSO ziet de risicoanalyse als een onderdeel van de interne controle.

Risk Managers daarentegen zien de risicobeheersingsmaatregelen als een onderdeel van het Risk Managementproces. Risk Managers kijken niet alleen naar procedures maar ook naar het effect. Doen de mensen wel wat ervan hen verwacht wordt in het kader van risicobeheersing. Bij Risk Managers spelen naast procedures ook de mens, de risk-awareness een grote rol.

Iedereen weet inmiddels, de grote incidenten als AHOLD, Laurus en recent Shell geven dat ook aan, dat je met procedures alleen niet komt tot een effectief Risk Management. Zicht op oorzaken en de impact van menselijk handelen en falen is bepalend voor het succes. Risk managers, zo zou je kunnen zeggen, hebben een meer informele, bottom up en op de praktijk gerichte aanpak.

De enige conclusie die je uit deze analyse kan trekken is dat alleen een samenspel tussen enerzijds zij die Risk Management toepassen en anderzijds de financiële mensen, controllers, interne en externe accountants de basis kan leggen voor een succesvol en effectief risicobeheersings- en controlesysteem. En dat samenspel is bij vele organisaties helaas nog ver te zoeken.

De beschrijving van een dergelijk systeem, dat getoetst moet worden door de interne accountant, waarover het Bestuur verantwoording moet afleggen en waar de Raad van Commissarissen toezicht op moet houden, kan dus niet zonder de hulp van de Risk Manager. Zijn rol moet worden geüpgraded. Niet aan de kantlijn, maar midden op het speelveld moet hij staan, weg uit de verzekeringshoek waar je ze nog veel in ondernemingen aantreft.

Tegelijkertijd moet de rol van de interne auditor goed worden gepositioneerd. Welke rol heeft hij bij de beschrijving van het systeem, bij de controle op de beheersmaatregelen en het systeem, bij het formuleren van uitgangspunten – risk based auditing?-, bij de rapportages etc.

Zoals gezegd, de verwijzing naar COSO, mogelijk ook dankzij mijn commentaar op de concepttekst, is winst. COSO praat echter nog steeds in algemene termen. In COSO noch in de Code wordt iets gezegd over de wijze waarop en door wie de risicoanalyses worden uitgevoerd, welke criteria worden aangehouden voor het wegen / meten van risico's, hoe de verantwoordelijkheden liggen, welke



doelstellingen, businessunits of processen daarvoor in aanmerking komen, wat met de resultaten wordt gedaan, wat voor een soort maatregelen er worden genomen en hoe de controle op de uitvoering en effectiviteit plaatsvindt en hoe de rapportage wordt verzorgd.

In de het rapport van de commissie Peters wordt de toepassing van een beheerssysteem gezien in het licht van risico's verbonden aan strategische doelstellingen en de financiële huishouding. Tabaksblat gaat daarin verder door te verwijzen naar risicoanalyses van operationele en financiële doelstellingen en naar het toezicht van Commissarissen o.a. op de risico's verbonden aan de ondernemingsactiviteiten. Geen risico mag uit principe buiten beeld blijven, ook wordt dat risico door Tabaksblat niet noemt.

Samenvattend.

Uit de nieuwe Code kan inspiratie worden geput voor de verdere vormgeving van risicobeheersing in de organisatie. Een aantal uitgangspunten en relevante partijen wordt genoemd.

Van groot belang is nu de uitwerking. Het formuleren van een goed risicobeheers- en controlesysteem heeft nu de eerste prioriteit. Als suggestie daarvoor heb ik een [Risk Management Protocol](#) opgesteld (zie bijlage).

Ik heb daarnaast het belang van een goede positionering van de Risk Manager de interne auditfunctie onderstreept.

Maar zoals altijd, het zijn de mensen die het moeten doen. Men kan formuleren en structureren wat men wil. Als men de mensen niet mee krijgt, of het nu leden van de Raad van bestuur zijn of zogezegd de jongste bediende, dan wordt het een moeizame strijd. Zij allen hebben een bijdrage in dit kader te leveren.

De Code is formeel georiënteerd. Risk managers praten over risk-awareness. Het is mijn stellige overtuiging dat alleen een goede mix van beiden tot een succesvol resultaat kan leiden.

VRIMS Integraal Risk Management Services

Mr.R.A.Vroom

035-5381555

[www.riskmanagement.nl](http://www.riskmanagement.nl)



## Corporate Governance Code, de Veertig Aanbevelingen (juni 1997)

(De commissie Peters)

### *De voor het risicobeheer relevante bepalingen.*

- Het Bestuur van de vennootschap is primair verantwoordelijk voor een adequate interne beheersingssysteem.
- Onder interne beheersing wordt het proces verstaan dat gericht is op het verkrijgen van redelijke zekerheid over het bereiken van doelstellingen in de volgende categorieën
  - De betrouwbaarheid van de financiële informatievoorziening
  - De effectiviteit en efficiëntie van bedrijfsprocessen
  - De naleving van relevante wet en regelgeving
- De Raad van Bestuur rapporteert schriftelijk aan de Raad van Commissarissen over de ondernemingsdoelstellingen, de strategie de daaraan verbonden risico's – ter illustratie van risico's kan worden gedacht aan valutaontwikkelingen, rentestand, economische groei, politieke risico's, grondstoffen en milieu- en de mechanismen tot beheersing van risico's van financiële aard. **(Aanbeveling 21)**
- Het Bestuur rapporteert aan de Raad van Commissarissen *tenminste* de uitkomsten van de beoordeling van de opzet en het functioneren van de systemen die gericht zijn op het verschaffen van redelijke zekerheid dat de financiële informatie betrouwbaar is.
- De Raad van Commissarissen bespreekt tenminste eenmaal 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 van de interne beheersingssystemen. **(Aanbeveling 17)**
- De Raad van Commissarissen of de auditcommissie houdt tenminste éénmaal per jaar en bespreking met de externe accountant.
- Een van de taken van de auditcommissie is 'het toezicht houden op de naleving van interne procedures en wet- en regelgeving en de beheersing van bedrijfsrisico's'.
- Interne en externe accountants worden in toenemende mate gevraagd om een adviserende en signalerende rol te spelen bij het beoordelen van de opzet en functioneren van systemen die gericht zijn op het beheersen van risico's en de verantwoording die daarover moet worden afgelegd.



## **De Nederlandse Corporate Governance Code (definitieve tekst december 2003)** (De commissie Tabaksblat)

### *De voor het risicobeheer relevante bepalingen.*

#### **PRINCIPES EN BEST PRACTICE BEPALINGEN**

##### **II. Het bestuur**

###### **II.1 Taak en werkwijze**

**Het bestuur is verantwoordelijk voor de naleving van alle relevante wet- en regelgeving, het beheersen van de risico's verbonden aan de ondernemingsactiviteiten en voor de financiering van de vennootschap. Het bestuur rapporteert hierover aan en bespreekt de interne risicobeheersings- en controlesystemen met de raad van commissarissen en zijn auditcommissie.**

###### **Best practice bepalingen**

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

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

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

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

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.

##### **III. Raad van commissarissen**

###### **Best practice bepalingen**

III.1.6 Het toezicht van de raad van commissarissen op het bestuur omvat onder andere:

- a) de realisatie van de doelstellingen van de vennootschap;
- b) de strategie en de risico's verbonden aan de ondernemingsactiviteiten;
- c) de opzet en de werking van de interne risicobeheersings- en controlesystemen;
- d) het financiële verslaggevingsproces;
- e) de naleving van de wet- en regelgeving.

III.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 het 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.

###### **III.5 Samenstelling en rol van drie kerncommissies van de raad van commissarissen**

###### **Principe**

**Indien de raad van commissarissen meer dan vier leden omvat, stelt de raad van commissarissen uit zijn midden een auditcommissie, een remuneratiecommissie en een selectie- en benoemingscommissie in.**

**De taak van de commissies is om de besluitvorming van de raad van commissarissen voor te bereiden. Indien de raad van commissarissen van vennootschappen besluit tot het niet instellen van een audit, remuneratie- en een selectie- en benoemingscommissie, dan gelden de best practice bepalingen III.5.4, III.5.5, III.5.8, III.5.9, III.5.10, III.5.13, V.1.2, V.2.3 en V.3.1 ten aanzien van de gehele raad van commissarissen. In het verslag van de raad van commissarissen doet de raad verslag van de uitvoering van de taakopdracht van de commissies in het boekjaar.**

#### **Best practice bepalingen**

##### *Auditcommissie*

III.5.4 De auditcommissie richt zich in ieder geval op het toezicht op het bestuur ten aanzien van:

a) 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;

### **V.3 Interne audit functie**

#### **Principe**

**De interne accountant, die een belangrijke rol kan spelen in het beoordelen en toetsen van interne risicobeheersings- en controlesystemen, functioneert onder de verantwoordelijkheid van het bestuur.**

#### **Best practice bepaling**

V.3.1 De externe accountant en de auditcommissie worden betrokken bij het opstellen van het werkplan van de interne accountant. Zij nemen ook kennis van de bevindingen van de interne accountant.

### **V.4 Relatie en communicatie van de externe accountant met de organen van de vennootschap**

#### **Principe**

**De externe accountant woont in ieder geval de vergadering van de raad van commissarissen bij waarin over de vaststelling of goedkeuring van de jaarrekening 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**

V.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 zijn controle van de jaarrekening en de daaraan gerelateerde controles onder de aandacht van het bestuur en de raad van commissarissen wil brengen. Daarbij kan aan de volgende onderwerpen worden gedacht:

C. 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, leningsconvenant en, vereisten van externe toezichthouders, etc.

### **Verklaring van en toelichting op enkele begrippen die in de code zijn gebruikt.**

#### **II. Het bestuur**

##### **II.1.3**

Het intern risicobeheersings- en controlesysteem dient te zijn toegesneden op de betreffende vennootschap. Dit geeft kleinere beursgenoteerde vennootschappen de mogelijkheid om met minder omvangrijke procedures te volstaan.

##### **II.1.4**

Het ligt in de rede dat het bestuur in de verklaring over de interne risicobeheersings- en controlesystemen aangeeft welk raamwerk of normenkader (zoals bijvoorbeeld het COSO raamwerk voor interne beheersing) hij heeft gehanteerd bij de evaluatie van het interne risicobeheersings- en controlesysteem.

##### **II.1.5**

Het gaat hier om een rapportage over de gevoeligheid van de resultaten ten aanzien van externe omstandigheden en variabelen in algemene zin.