

# Inhoud

Voorwoord	7
Inleiding	9
1 Corporate-governancecodes	13
2 Control frameworks	57
3 Strategie, risicobereidheid en doelstellingen	93
4 Risicomanagement	118
5 Procesmanagement	152
6 Projectmanagement	198
7 Informeren en communiceren	229
8 Bewaken	253
Bijlage A Voorbeelden van risico's	269
Bijlage B Afkortingen	272
Bijlage C Bronvermelding	274
Bijlage D De auteurs	280
Register	285

# Voorwoord

De laatste jaren is er het nodige gebeurd op het gebied van corporate governance. Vooral in de Verenigde Staten heeft de wetgever zware maatregelen genomen om beursschandalen zoals Enron, WorldCom en Tyco te voorkomen. De strafbepalingen in de Sarbanes-Oxley-wet (sectie 906) lopen op tot een boete van 5 miljoen dollar en een gevangenisstraf van twintig jaar bij een bewuste ontduiking van de bepalingen in de secties 302 en 404, die onder meer een managementrapportage over interne beheersing voorschrijven. Deze strafbepalingen zullen zeker hun effect hebben. In Europa hebben de wetgevers niet zover willen gaan. De Nederlandse corporate governance code (de 'code-Tabaksblat') kent geen strafbepalingen. Desalniettemin is ook in Nederland veel belangstelling ontstaan voor corporate governance, mede omdat de code-Tabaksblat inmiddels is uitgestraald naar tal van specifieke branches, zoals pensioenfondsen, woningcorporaties, ziekenhuizen enzovoort.

Corporate governance heeft enerzijds een juridische insteek, gericht op de positie, verantwoordelijkheden en bevoegdheden van directie, commissarissen en aandeelhouders, anderzijds heeft het een organisatorische insteek, gericht op het opzetten en in stand houden van een goede vorm van risicomanagement en interne beheersing.

Het vak bestuurlijke informatieverzorging, dat onder meer aan de accountants- en controllersopleiding van Nyenrode Business Universiteit wordt gedoceerd, richt zich in belangrijke mate op dit laatste aspect van corporate governance. De meeste docenten van Nyenrode Business Universiteit zijn naast hun parttime docentschap werkzaam in het bedrijfsleven of bij de overheid, zo ook de auteur en twee van de coauteurs van dit boek. Uit dit boek blijkt de waarde van deze combinatie. Theoretische concepten, zoals die met name in de masterfase van de opleiding aan de orde komen, zijn in dit boek op een soepele wijze vertaald naar praktijkoplossingen.

Lange tijd heeft in de Nederlandse opinie over interne beheersing het werk van Starreveld vooropgestaan. Nu zien wij dat er ook in het buitenland interessante ontwikkelingen op dit gebied hebben plaatsgevonden en dat veel van de concepten van Starreveld verouderingsverschijnselen be-

ginnen te vertonen. De auteurs stippen het typologiemodel van Starreveld nog even aan, maar richten zich daarna vooral op de internationale ontwikkelingen. Interne beheersing is immers een internationaal fenomeen, zij het dat daarbij rekening gehouden moet worden met cultuurverschillen tussen landen. Zo is de sterke aandacht die in de literatuur over *management accounting* en *management control* aan prestatiebeloning wordt besteed, waarschijnlijk te verklaren door de Angelsaksische achtergrond van veel auteurs op dit vakgebied. Prestatiebeloning past bij een cultuur waarin het eigenbelang vooropstaat.

Cultuur wordt steeds meer gezien als een belangrijke contingentiefactor voor interne beheersing. In dit boek komt dat ook meermalen aan de orde. Beheersingsmaatregelen moeten passen bij de bedrijfscultuur en de gekozen wijze van leidinggeven. Welke combinaties van bedrijfscultuur en beheersingsmaatregelen tot de beste resultaten leiden, is nog onderwerp van daarop gericht onderzoek, dat overigens ook bij Nyenrode Business Universiteit wordt uitgevoerd.

Dit boek geeft een interessant, praktijkgericht overzicht van de belangrijkste ontwikkelingen op het gebied van risicomanagement en interne beheersing. Managers zullen na dit boek gelezen te hebben, meer rekening kunnen houden met dit aspect van het leidinggeven en zullen een betere gesprekspartner worden voor deskundigen op dit gebied. Ik beveel het van harte in uw aandacht aan!

Prof. dr. W. Fred. de Koning  
Voorzitter vakgroep Bestuurlijke Informatieverzorging  
Nyenrode Business Universiteit

# Inleiding

Managers zijn verantwoordelijk voor het besturen van de organisatie waarin zij werkzaam zijn. Daarbij wordt onder meer van hen verwacht dat zij die organisatie continu verbeteren, gestelde doelen realiseren en voorkomen dat zich situaties voordoen die tot negatieve publiciteit leiden. Als zij dat goed doen, dan heeft dit een positieve uitstraling op zowel de organisatie als op henzelf. Slagen zij daar echter onvoldoende of niet in, dan kan dat vervelende gevolgen hebben. Denkt u maar aan glassplinters in babyvoeding, de mislukte ombouwstrategie van Laurus of de ICT-problemen bij de belastingdienst. Om dat te voorkomen moeten moderne managers hun organisatie in de greep hebben. Dat is binnen de huidige complexe organisaties geen sinecure en vereist een multidisciplinaire benadering. Managers moeten daarom om kunnen gaan met instrumenten die ingezet worden om de gewenste controle te verkrijgen en te behouden en moeten daarbij beseffen wat voor effecten deze hebben op andere instrumenten. Zo kan sturen op klanttevredenheid in de installatiebranche bijvoorbeeld een averechts effect hebben op de naleving van veiligheidsprocedures. De klant wil dat snel met het werk wordt gestart, terwijl natuurlijk eerst de werkomgeving veilig moet worden gesteld. Oplossingen voor dergelijke vraagstukken zijn volop in ontwikkeling en komen onder verschillende namen voor, zoals managementmodellen, *control frameworks* en risicobeheersingssystemen.

In dit boek bespreken wij<sup>1</sup> de in de praktijk meest toegepaste systemen, de instrumenten waaruit deze zijn samengesteld en de theorieën die eraan ten grondslag liggen. Wij vergelijken deze instrumenten en theorieën vervolgens met onze eigen visie en praktijkervaring. Wij adviseren managers hoe zij zo'n systeem voor de eigen organisatie kunnen opzetten, in stand kunnen houden of verder kunnen professionaliseren. Dit alles is gebaseerd op een combinatie van onze gezamenlijke praktijkervaring en pragmatische toepassing van bewezen concepten uit de managementliteratuur en -studies. Het boek bevat korte aansprekende praktijkcases en quotes om de behandelde onderwerpen verder te verduidelijken.

---

<sup>1</sup> Zie bijlage D voor het profiel van de auteurs.

Omdat elke organisatie uniek is en haar eigen cultuur heeft, hebben we niet één systeem of oplossing centraal gesteld maar worden diverse best practices behandeld en met een kritische beschouwing tegen elkaar afgezet. Wij geloven dat maatwerk noodzakelijk is om tot een succesvol beheersingssysteem te komen; standaardoplossingen voldoen niet. Dit boek geeft managers handreikingen om hieraan invulling te geven, zowel organisatiebreed als voor specifieke disciplines zoals HR, marketing, logistiek of ICT. Iedere manager die zijn of haar discipline wil beheersen, heeft daar (beheersings)instrumenten voor nodig. Nog niet zo lang geleden waren dit vooral financiële instrumenten, zoals begrotingen en autorisaties, waardoor beheersing soms een *finance*-feestje leek. De laatste jaren is dit beeld gelukkig sterk aan het veranderen omdat organisaties meer en meer tot de conclusie komen dat daadwerkelijke beheersing alleen te realiseren is door alle disciplines erbij te betrekken. Een probleem daarbij is dat beheersingsinstrumenten niet bij alle managers in hun opleiding aan de orde zijn gekomen en dat pragmatische literatuur die het gehele onderwerp op een toegankelijke wijze bespreekt, ontbreekt. Dit boek is geschreven om in die behoefte te voorzien en bespreekt onderwerpen waarvan een moderne manager kennis zou moeten hebben om zijn of haar zaak in de greep te kunnen houden. Een operationele manager ontdekt in dit boek bijvoorbeeld de relatie met ISO, een projectmanager de relatie met Prince2, een procesmanager met 6sigma, een ICT-manager met COBIT, enzovoort.

Tevens zal duidelijk worden dat door het in de greep willen hebben van de eigen organisatie automatisch een invulling wordt gegeven aan de eisen die de aangescherpte wet- en regelgeving op het gebied van corporate governance aan organisaties stelt. Ditzelfde geldt voor eisen die toezichthouders zoals De Nederlandsche Bank en AFM stellen aan organisaties die onder toezicht staan. De omgekeerde situatie, waarbij een beheerssysteem wordt opgezet en in stand gehouden omdat een code of toezichthouder dat wenst, blijkt in de praktijk namelijk niet te werken. Zo'n systeem is dan een papieren tijger geworden. Dat is onder meer gebleken bij Société Générale, de bank die begin 2008 miljarden heeft verloren door speculaties van *rogue trader* Jérôme Kerviel. Deze bank volgde corporate-governance-codes en stond onder toezicht van de centrale bank. Onderzoeken naar deze affaire laten zien dat de interne beheersing bij deze bank een papieren tijger was en dat het management de operaties niet in de greep had. Het enorme verlies aan geld en reputatie toont aan dat beheersing van de organisatie een belangrijk onderwerp voor managers is en blijft. Dit boek

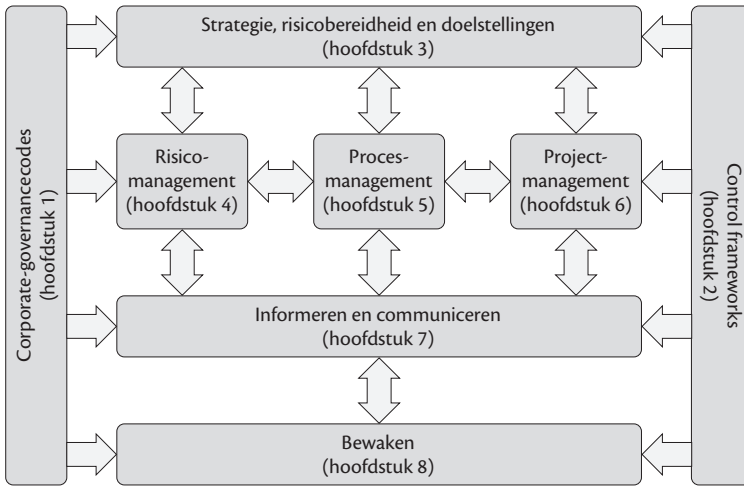
geeft managers handreikingen hoe daaraan het best invulling gegeven kan worden.

Greep krijgen op een organisatie werkt zoals de vingers aan uw handen. Iedere vinger heeft een eigen taak. U kunt ermee wijzen of er iemand mee wenken. Maar als u wilt schrijven, hebt u al snel twee vingers nodig en is de nodige coördinatie van uw hand vereist om de tekst leesbaar te krijgen. Als u een doos papier wilt oppakken, blijkt dat u beide handen en meerdere vingers nodig heeft. Zo werkt het ook met beheersingssystemen. Het inzetten van één instrument is relatief eenvoudig en de effecten zijn goed te overzien. Helaas volstaat één instrument niet om een organisatie in de greep te houden. Dat vereist samenspel en coördinatie, wat niet eenvoudig blijkt. Om hierin inzicht te geven bevat dit boek acht zelfstandig leesbare hoofdstukken. Ieder hoofdstuk bevat afgebakende onderwerpen die in de context van het grotere geheel worden geplaatst.

In hoofdstuk 1 starten wij met de behandeling van de complianceaspecten van organisatiebeheersing en leggen we de relatie met de diverse corporate-governancecodes. Hoofdstuk 2 bespreekt de diverse modellen, frameworks en systemen die een manager kan gebruiken om de beheersing van een organisatie vorm te geven. Als rode draad wordt daarbij het managementmodel dat wij in onze eigen praktijk gebruiken, geïntroduceerd. In de opvolgende hoofdstukken worden de bouwstenen van dat model tezamen met diverse andere best practices uitgewerkt. Hoofdstuk 3 behandelt het belang van de strategie van een organisatie als ankerpunt voor de beheersing. De hoofdstukken 4, 5 en 6 gaan vervolgens uitgebreid in op risico-, proces- en projectmanagement. Deze drie onderwerpen vormen de kern van de activiteiten die een organisatie uit moet voeren om de strategische doelen te realiseren. Om te weten of deze activiteiten op een juiste en beheerste wijze worden uitgevoerd, zijn informatie en communicatie daarover noodzakelijk. Dit wordt in hoofdstuk 7 behandeld, waarbij de informatie- en communicatietechnologie (ICT) en de razendsnelle ontwikkelingen die zich daarin voordoen aan de orde komen. De ICT heeft immers nieuwe uitdagingen op het gebied van de organisatiebeheersing tot gevolg gehad. Tot slot gaat hoofdstuk 8 in op de vraag hoe bewerkstelligd kan worden dat alles wat in de greep is dat ook in de toekomst blijft.

De afzonderlijke hoofdstukken komen samen in het volgende model dat de leidraad vormt voor dit boek. Wij hebben de overtuiging dat dit boek u kan helpen bij beheersingsvraagstukken die binnen uw organisatie spelen. De antwoorden helpen u de prestaties van uw organisatie op een beheerste wijze te verbeteren. Vragen over, reacties op of ervaringen met

dit boek vernemen wij graag van u zodat wij deze bij een herziene uitgave kunnen meenemen.



*Figuur 0.1 Structuur van dit boek*

Drs. Francis H.C. Bouman RA RM

Drs. René van Ast RA

M.F. (René) van Dijk RA

Dr. H.A. (Diederik) van Meenen MBA MSC CPA CFE

# Corporate-governancecodes

## 1.1 Corporate en internal governance

Corporate governance is een term die de laatste jaren in Nederland te pas en te onpas wordt gebruikt. Daarom is het wenselijk een eenduidig begrip te hebben wat hieronder wordt verstaan. Alhoewel een goede vertaling niet bestaat, is ‘goed organisatiebestuur’ nog de meest passende vertaling. Als we deze vertaling als uitgangspunt nemen, is het zinvol deze inhoudelijk nader uit te diepen.

### *Goed*

Dit is een kwalitatief element dat bovendien plaats- en tijdgebonden is. Plaatsgebonden omdat wat naar Nederlandse maatstaven goed is, dat naar bijvoorbeeld Afrikaanse maatstaven niet hoeft te zijn. Tijdgebonden omdat wat wij in Nederland vijftig jaar geleden goed vonden, dat nu niet meer hoeft te zijn.

Onder ‘goed’ verstaan we dat het is zoals het hoort te zijn en dat het voldoet aan de daaraan gestelde eisen.

### *Organisatie*

Onder organisatie moet worden verstaan een doelbewust samenwerkingsverband waarin partijen samenwerken om zowel gemeenschappelijke als eigen doelstellingen te bereiken. Deze doelstellingen kunnen sterk variëren, waarbij onder meer gedacht kan worden aan aandeelhouderswaarde, persoonlijk inkomen, openbaar nut en status.

Het is van belang te onderkennen dat organisaties een formele en informele verschijningsvorm hebben. De formele organisatie kan gevonden worden in jaarverslagen, organogrammen, rapportagelijnen en functie- en taakomschrijvingen. De informele organisatie is lastiger waarneembaar, maar zeker zo belangrijk. Zij kan de formele organisatie namelijk ondersteunen, maar ook tegenwerken.



### **Bestuur**

Onder besturen verstaan we het nemen van beslissingen en het bewerkstelligen dat deze worden uitgevoerd. Deze taak is primair in handen van het topmanagement, waarbij het ondersteund kan worden door commissarissen, stafafdelingen en adviseurs.

Wat onder goed organisatiebestuur wordt verstaan, verschilt per organisatie en hangt onder meer samen met de mate van professionaliteit en volwassenheid van de desbetreffende organisatie, het land waarin de organisatie actief is, de daarbij behorende cultuur en handelsmoraal en de tijdgeest van het moment. Aan goed bestuur bij een kleine sportvereniging worden andere eisen gesteld dan bij een beursfonds en aan een Afrikaanse voetbalbond stellen we andere eisen dan aan een Nederlandse.

'There is no one model of corporate governance that works in all countries and all companies...'

(Standard & Poor's research paper over corporate governance, februari 2007)

Morris Tabaksblat, de voorzitter van de Nederlandse corporate-governancecommissie, heeft corporate governance als volgt samengevat:<sup>1</sup>

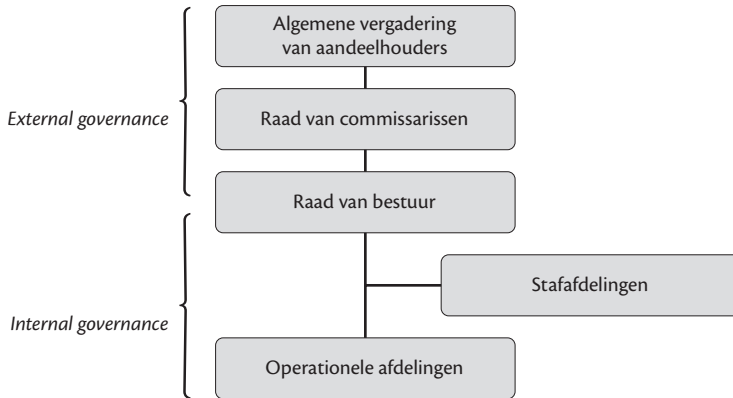
- intern betekent goede corporate governance efficiënt toezicht, een adequate inkadering van de topbestuurders en afdoende interne systemen van risicobeheersing;
- extern betekent goede corporate governance meer en betrouwbaardere informatie voor de buitenwereld, kapitaalverschaffers voorop.

Het tweede punt, dat kapitaalverschaffers vooropstelt, maakt duidelijk dat dit een uitwerking is voor beursgenoteerde organisaties. Omdat corporate governance ook van groot belang is voor organisaties zonder beursnotering, zouden wij daarom liever over belanghebbenden in bredere zin spreken. Daaronder vallen dan naast de kapitaalverschaffers ook het personeel, de leveranciers en andere stakeholders die een belang bij de organisatie hebben.

Om extern betrouwbare informatie te kunnen verschaffen zijn de interne vereisten volgens ons een randvoorwaarde. Daarom richten wij ons in dit boek op de interne vereisten, die ook wel *internal governance* worden genoemd.

---

<sup>1</sup> Speech op de Accountantsdag, 2003.



Figuur 1.1 Onderscheid external en internal governance voor profitorganisaties

Opgemerkt dient te worden dat figuur 1.1 het in Nederland gebruikelijke *two-tier*-model weergeeft, waarbij een duidelijke scheiding is aangebracht tussen de commissarissen en het bestuur. Het bestuur is binnen dit model verantwoordelijk voor het beleid en de uitvoering daarvan en de commissarissen zijn belast met het toezicht daarop.

In Angelsaksische landen wordt een ander model gebruikt, het *one-tier*-model. Daarbij is sprake van één *board* die is samengesteld uit *executives* en *non-executives*. Laatstgenoemden zijn vergelijkbaar met de commissarissen, echter met als belangrijk verschil dat zij volledig medeverantwoordelijk zijn voor het gevoerde beleid. Omdat dit boek met name voor de Nederlandse praktijk is geschreven, wordt in het vervolg van dit boek uitgegaan van het *two-tier*-model.

De aandacht voor *external* en *internal governance* is niet nieuw. Al eeuwen geleden was er bij de *voc* sprake van onvrede over transparantie, zeggenschap van aandeelhouders en beloning van het management. Feitelijk komt dit voort uit de scheiding tussen management en kapitaalverschaffing, oftewel het principaal-agentprobleem.<sup>2</sup> Aandeelhouders (principalen) delegeren de besturing van een organisatie aan het door hen aangestelde management (agenten), wat drie problemen met zich meebrengt.

### 1 Belangenconflict

Aandeelhouders streven waardecreatie na, terwijl het management ook belangstelling heeft voor de eigen carrière, status en welvaart.

<sup>2</sup> 'Theory of the firm', Jensen en Meckling, *Journal of Financial Economics*, 1976.

## II *Asymmetrische informatie*

Het management heeft meer informatie over de organisatie, de beslissingen die het kan nemen, de daaraan verbonden risico's en de activiteiten die het kan ontplooiën dan aandeelhouders. Laatstgenoemden kunnen daardoor moeilijk beoordelen of het management zich optimaal inspant om de waarde van de organisatie te maximaliseren.

## III *Risicoasymmetrie*

Aandeelhouders en managers hebben een verschillende risicobereidheid. Aandeelhouders hebben in het algemeen een gediversifieerde beleggingsportfolio en wensen dat de organisatie waarin zij beleggen een zeker risico loopt. Managers zijn verbonden aan de organisatie en zouden daardoor risicoavers zijn.

Doordat managers de belangen van aandeelhouders niet optimaal behartigen en aandeelhouders een en ander niet optimaal kunnen bewaken, vindt er waardevernietiging plaats, de zogenaamde *agency*-kosten. Lange tijd is gedacht dat door het toepassen van prestatiebeloning deze waardevernietiging kan worden verkleind. Door een deel van de beloning van het management te koppelen aan een prestatie maatstaf die bijdraagt aan de doelstelling van de aandeelhouder, wordt het belangenconflict verkleind en zal de manager zijn extra informatie eerder gebruiken om de aandeelhouderswaarde te maximaliseren. Randvoorwaarden hierbij zijn dat de prestatie maatstaf:

- door de manager beheersbaar of beïnvloedbaar moet zijn;
- doelmatig is, oftewel dat een bijdrage aan de prestatie maatstaf moet leiden tot een bijdrage aan de doelstelling van de organisatie.

De veronderstelde relatie tussen de beloning van managers en de prestaties die zij leveren, blijkt in de praktijk niet te bestaan. Een in 2007 gepubliceerd onderzoek<sup>3</sup> naar de beloningen van topmanagers bij Nederlandse beursgenoteerde organisaties heeft dat aangetoond. Hoge beloningen van topmanagers worden door het onderzoek enerzijds toegeschreven aan de macht en invloed die topmanagers hebben met betrekking tot het vaststellen van hun beloningspakket en anderzijds aan een schaarste aan topmanagers die hun beloning zou opdrijven. Daarbij speelt mee dat de beloning van topmanagers voor aandeelhouders een minder belangrijk punt is, omdat deze beloning in relatie tot het totaal van de kosten van een organisatie gering is.

<sup>3</sup> 'Geen relatie beloning en prestatie', Piet J.W. Duffhues, *NRC Handelsblad*, 2007.

## De Ahold-case

Ahold, dat onder leiding stond van Cees van der Hoeven (ceo) en Michiel Meurs (cfo), was jarenlang de lieveling van de Amsterdamse effectenbeurs. Het concern presteerde uitzonderlijk, wat Van der Hoeven meermalen de titel manager van het jaar opleverde.

In februari 2003 kwam aan al het enthousiasme abrupt een einde doordat meerdere fraudezaken in de openbaarheid kwamen.

Bij dochterbedrijf US-Foodservice was fraude gepleegd doordat inkoopkortingen als winst waren verantwoord, terwijl er geen recht op die kortingen bestond.

Alsof dat niet genoeg was, bleek dat Ahold creatief omging met joint ventures in Scandinavische en Zuid-Amerikaanse supermarkten. Volgens de boekhoudregels mag de omzet van een joint venture alleen volledig bij de eigen omzet worden opgeteld, in vaktermen geconsolideerd, als er beslissende zeggenschap in de joint venture kan worden uitgeoefend. Die zeggenschap zou Ahold op basis van contracten hebben, ware het niet dat sideletters deze zeggenschap weerspraken. De sideletters, die deels persoonlijk door Van der Hoeven waren ondertekend, waren geheimgehouden en ook niet aan de accountant verstrekt. Hierdoor werd jarenlang te veel omzet verantwoord, wat ernstig is omdat omzet in de detailhandel een belangrijke maatstaf is voor succes. Het gevolg van de fraudes was dat het vertrouwen in Ahold verloren ging en de beurskoers ineenstortte.

Van der Hoeven en Meurs waren bestuurder af en moesten zich voor de rechter verantwoorden. Hilarisch waren daarbij de woorden van Meurs die stelde: 'Consolideren, het is net als de vraag: wat is porno? Een blote vrouw op een foto, dat is porno, maar als er een lijst omheen zit met een handtekening van Jan Sluijters erbij is het kunst.' Het mocht niet helpen, zowel Meurs als Van der Hoeven is door de rechter veroordeeld.

Naast prestatiebeloning worden corporate-governancecodes ingezet om het principaal-agentprobleem te verkleinen en beursschandalen te voorkomen. Met name na de grote schandalen in 2001 bij beursfondsen zoals Enron, Worldcom, Tyco, Parmalat en Ahold zijn de problemen beantwoord met nieuwe wetten en codes die de relatie tussen het topmanagement, de commissarissen en de aandeelhouders proberen te regelen. Daarbij zijn tevens eisen gesteld aan de wijze van verantwoording, transparantie en risicobeheersing. De vraag is of dit een terechte reactie is geweest.

Uit onderzoek<sup>4</sup> naar de beursschandalen van 2001 is gebleken dat een slechte corporate governance daar niet de oorzaak van is geweest. Op basis van een vergelijking tussen 25 bekende 'fraudeorganisaties' uit diverse sectoren en landen en 25 'eerlijke organisaties' van vergelijkbare omvang en activiteiten is aangetoond dat de frauderende organisaties op het gebied van de corporate governance even goed scoorden als de andere organisaties. De oorzaak van de fraudes bleek veel meer te liggen in:

- een excessieve optiebeloning voor het topmanagement;
- een zonnekoningreputatie van de bestuursvoorzitter;
- irrealistische beloftes van het management aan beleggers.

## 1.2 Corporate-governanceregeling

Als reactie op de beursschandalen is in veel landen voor beursgenoteerde organisaties regelgeving ingevoerd die een goede corporate governance moet waarborgen. In Nederland zijn de Amerikaanse Sarbanes-Oxley-wet en de Nederlandse corporate governance code het meest bekend, waarbij laatstgenoemde vaak code-Tabaksblat wordt genoemd. Na de introductie van corporate-governancecodes voor beursfondsen zijn soortgelijke codes geïntroduceerd voor andere organisaties. Voor charitatieve instellingen geldt in Nederland bijvoorbeeld de Code goed bestuur voor goede doelen, die ook wel bekend is als de code-Wijffels.<sup>5</sup>

De corporate-governanceregeling kan van land tot land sterk verschillen,<sup>6</sup> alhoewel er wel een aantal gemeenschappelijke kenmerken zijn te herkennen:

- regelingen met betrekking tot de rechten en plichten van:
  - aandeelhouders;
  - bestuurders;
  - commissarissen;
- regelingen met betrekking tot de beloningsstructuur van bestuurders;
- regelingen met betrekking tot de rol van de accountant;
- vereisten ten aanzien van interne risicobeheersings- en controlesystemen (irc-systemen).

Misschien nog wel een belangrijker punt dan de inhoudelijke verschillen tussen de corporate-governanceregelingen in de diverse landen is de in-

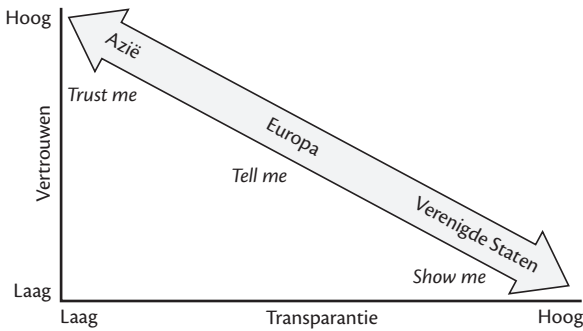
4 'Sturen op vertrouwen is antwoord op boekhoudschandalen', Kees Cools, persbericht, 2005.

5 *Code goed bestuur voor goede doelen*, Commissie Code Goed Bestuur voor Goede Doelen, juni 2005.

6 [www.ecgi.org](http://www.ecgi.org).

terne beheersingscultuur en mate van transparantie in de diverse landen. Deze verschillen hebben geresulteerd in *rule-based* regelgeving in de Verenigde Staten, waardoor goed ondernemingsbestuur aldaar in belangrijke mate is verworven tot een compliancetaak.

De Europese regelgeving daarentegen is *principle-based* van aard, wat organisaties ruimte voor eigen interpretatie geeft. Het gevolg daarvan is wel dat dit minder eenvoudig te toetsen is. Voorbeelden zijn de Nederlandse code-Tabaksblat, de Belgische code-Lippens en de Engelse *Combined Code*.



Figuur 1.2 Corporate governance in internationaal verband

Omdat de verschillende corporate-governancecodes veel gemeenschappelijke kenmerken hebben, is het niet noodzakelijk om op de inhoud van al deze codes in te gaan. Om een goed inzicht te krijgen in de eisen, in het bijzonder die inzake de interne beheersing die uit de codes voortvloeien, wordt in de volgende twee paragrafen nader ingegaan op twee codes die in Nederland grote invloed hebben gehad: de code-Tabaksblat en de Sarbanes-Oxley-wet.

### 1.3 De code-Tabaksblat

#### 1.3.1 Inleiding in de code-Tabaksblat

De Nederlandse corporate governance code<sup>7</sup> is opgesteld onder leiding van Morris Tabaksblat, de voormalig bestuursvoorzitter van Unilever. Zijn commissie heeft de code opgesteld op verzoek van onder meer beursorganisatie Euronext, de Vereniging van Effectenbezitters en de ministers van Financiën en Economische Zaken. De code vervangt het rapport met de veertig aanbevelingen van de commissie-Peters uit 1997.<sup>8</sup>

<sup>7</sup> De Nederlandse corporate governance code, Commissie Corporate Governance, 2003.

<sup>8</sup> Corporate governance in Nederland – de veertig aanbevelingen, Commissie Corporate Governance, 1997.

‘Voor die tijd, voor dat jaar 1996, soms wat langer, soms wat korter, hadden aspecten van goed bestuur en adequaat toezicht eigenlijk heel weinig aandacht in dit land. Het hebben en gebruiken van voorkennis was voor een aantal mensen gewoon een secundaire arbeidsvoorwaarde. Een onafhankelijke commissaris, dat was natuurlijk een begrip dat wij helemaal niet kenden, want de commissaris was juist bedoeld voor het netwerk. En de raad van commissarissen en de raad van bestuur waren innig samen dankzij onder meer de coöptatie, onder de dikke deken van het structuurregime. En u weet, dikke dekens geven warmte en bevorderen de wederzijdse genegenheid.’

(Jaap F.M. Peters, speech tijdens een seminar over corporate governance, augustus 2003)

De code is eind 2003 gepubliceerd en geldt met ingang van 2004 voor alle organisaties die een beursnotering in Nederland hebben. De code heeft de juridische status van een Algemene Maatregel van Bestuur. De doelstelling van de code is organisaties een handreiking te bieden voor het verbeteren van hun governance.

De code is opgebouwd uit een aantal *principle-based* principes, die weer verder zijn uitgewerkt in best-practicebepalingen. De principes worden geacht de moderne en breed gedragen algemene opvattingen over goede corporate governance weer te geven. De best-practicebepalingen worden geacht concreter te zijn en een zekere normstelling te verschaffen.

Organisaties met een beursnotering in Nederland dienen op basis van de code elk jaar in het jaarverslag te rapporteren op welke wijze zij de principes hebben toegepast. Daarvoor geldt de regel ‘pas toe of leg uit’ (*comply or explain*), wat wil zeggen dat afwijkingen van de code niet per definitie fout hoeven te zijn. Bij afwijkingen moet wel een duidelijke uiteenzetting van de argumenten opgenomen worden. De code schrijft overigens niet voor hoe het verslag eruit moet zien.

Na de initiële rapportage in het jaarverslag van 2004 hebben sommige organisaties er in de opvolgende jaren voor gekozen om vanuit hun jaarverslag te verwijzen naar hun corporate-governancewebsite<sup>9</sup>. Op die websites is alle informatie over de naleving van de code opgenomen.

### 1.3.2 Inhoud van de code-Tabaksblat

De code-Tabaksblat is onderverdeeld in vijf hoofdstukken.

<sup>9</sup> *Derde rapport over de naleving van de Nederlandse corporate governance code*, Monitoring Commissie Corporate Governance Code, december 2007.

### ***I Naleving en handhaving van de code***

Dit hoofdstuk stelt dat het bestuur en de commissarissen verantwoordelijk zijn voor de corporate governance van de organisatie en de naleving van de code-Tabaksblat. Merk hierbij op dat ook, in tegenstelling tot wat binnen een *two-tier*-model gebruikelijk is, de commissarissen samen met het bestuur verantwoordelijk zijn.

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

Het hoofdstuk over het bestuur legt de verantwoordelijkheid voor de naleving van de wet- en regelgeving, het beheersen van de risico's en de financiering van de organisatie expliciet bij het bestuur. Daarnaast bevat dit hoofdstuk principes voor de beloning van bestuurders en het voorkomen van eventuele tegenstrijdige belangen tussen het bestuur en de organisatie. Met name over de bezoldiging van bestuurders is veel te doen geweest in de media.

### ***III De raad van commissarissen***

De commissarissen hebben het meest uitgebreide hoofdstuk gekregen. Hierin worden principes gegeven ten aanzien van:

- de uitoefening van de toezichhoudende taak;
- de waarborging van de onafhankelijkheid, in het bijzonder bij het *one-tier*-model;
- de vereiste deskundigheid en samenstelling van de raad;
- het instellen van een audit-, remuneratie- en een selectie- en benoemingscommissie;
- de omgang met eventuele tegenstrijdige belangen tussen de commissarissen en de organisatie;
- de bezoldiging van de commissarissen.

### ***IV De aandeelhouders***

Een noviteit in de code is dat van de aandeelhouders, en in het bijzonder van de institutionele beleggers, een meer actieve en betrokken houding ten opzichte van de organisatie waarin zij beleggen, wordt verwacht. Aandeelhoudersvergaderingen waren in het verleden namelijk weinig stimulerende bijeenkomsten met een lage opkomst.

De principes uit dit hoofdstuk van de code zijn verder gericht op het voorkomen van beschermingsconstructies en een correcte omgang met koersgevoelige informatie.



### V De audit

Dit hoofdstuk gaat over de financiële verslaggeving en de rol van de interne en externe accountants daarbij. Aan de interne accountant wordt een belangrijke rol toegekend in het kader van het beoordelen en toetsen van de opzet en de werking van het interne risicobeheersings- en controlesysteem (irc-systeem) van een organisatie.

De externe accountant moet de aandeelhoudersvergadering bijwonen en zijn bevindingen over de controle van de jaarrekening gelijktijdig aan het bestuur en de commissarissen rapporteren. In het verleden was het gebruikelijk dat het bestuur de bevinding als eerste ontving.

Voor de *internal governance* zijn met name de hoofdstukken II en V van belang, die in de volgende subparagrafen nader worden uitgewerkt. De overige hoofdstukken van de code-Tabaksblat zijn in het kader van dit boek minder relevant en hierop wordt daarom niet nader ingegaan.

#### 1.3.3 Code-Tabaksblat – hoofdstuk II: het bestuur

Hoofdstuk II van de code omvat principes en best-practicebepalingen voor het bestuur van een organisatie. Als principe is onder meer gesteld dat het bestuur:

- belast is met het besturen, wat onder meer inhoudt dat hij verantwoordelijk is voor de realisatie van de doelstellingen, de strategie en het beleid;
- verantwoordelijk is voor de naleving van alle relevante wet- en regelgeving, voor het beheersen van de risico's verbonden aan de ondernemingsactiviteiten en voor de financiering van de vennootschap;
- hierover rapporteert aan de raad van commissarissen en zijn auditcommissie;
- de interne risicobeheersings- en controlesystemen bespreekt met de raad van commissarissen en zijn auditcommissie.

Het principe wordt nader uitgewerkt in de best-practicebepalingen II.1.3 en II.1.4. Bepaling II.1.3 stelt dat in de organisatie een op de organisatie toegesneden irc-systeem aanwezig moet zijn. Onder instrumenten van zo'n systeem worden in ieder geval verstaan:

- risicoanalyses van de operationele en financiële doelstellingen van de organisatie;
- een gedragscode die in ieder geval op de website van de organisatie wordt geplaatst;

- handleidingen voor de inrichting van de financiële verslaggeving en de voor de opstelling daarvan te volgen procedures;
- een systeem van monitoring en rapportering.

Als nadere toelichting op de best practice is opgenomen dat doelbewust wordt gesproken over een op de organisatie toegesneden irc-systeem. Dat geeft namelijk kleinere organisaties de mogelijkheid om met minder omvangrijke procedures te volstaan.

‘Op verschillende plaatsen in de conceptcode vraagt de commissie aandacht voor het verhogen van de kwaliteit van het irc-systeem en de verantwoording daarover. Wij zijn het met de commissie eens dat dit een uitermate belangrijk onderwerp is, maar willen wel wijzen op een aantal onduidelijkheden. Hoe moet het systeem worden geëvalueerd? Hoe ziet de rapportage eruit? En welke rol speelt de accountant? Bovendien zijn er geen normen gedefinieerd voor wat een goed irc-systeem is.’

(Reactie van accountantskantoor KPMG op de conceptcode Tabaksblat)

Bepaling 11.1.4 voegt daar nog aan toe dat door het bestuur in het jaarverslag wordt verklaard dat de irc-systemen adequaat en effectief zijn met een duidelijke onderbouwing daarbij. Het bestuur wordt geacht in het jaarverslag te rapporteren over de werking van het irc-systeem in het boekjaar. Daarbij moet tevens worden aangegeven welke eventuele significante wijzigingen zijn aangebracht, welke eventuele belangrijke verbeteringen zijn gepland en dat één en ander met de auditcommissie en de commissarissen is besproken. De op grond van bepaling 11.1.4 in het jaarverslag op te nemen verklaring is bekend geworden als de in-controlverklaring.

Als nadere toelichting op best-practicebepaling 11.1.4 is opgenomen dat het logisch wordt geacht dat het bestuur in de verklaring aangeeft welk raamwerk of normenkader is gehanteerd bij de evaluatie van het irc-systeem. Als voorbeeld is daarbij verwezen naar het coso-raamwerk<sup>10</sup> voor interne beheersing. Dit raamwerk wordt in hoofdstuk 2 van dit boek nader toegelicht.

‘De raad van bestuur vertrouwt erop dat de onderneming een adequaat systeem van risicobeheersing en interne controle heeft ingesteld, dat geëigend is

<sup>10</sup> *Internal control – integrated framework*, coso, mei 1994.

voor de onderneming en in overeenstemming is met de vereisten op grond van aanbeveling 11.1.4. van de Nederlandse corporate governance code.’

(Jaarverslag Koninklijke Grolsch, 2006)

Sommige auteurs<sup>11</sup> stellen dat de bepalingen 11.1.3 en 11.1.4 feitelijk weinig nieuws bevatten, omdat in het Burgerlijk Wetboek (2:141) reeds is opgenomen dat ‘het bestuur stelt ten minste een keer per jaar de commissarissen schriftelijk op de hoogte van de hoofdlijnen van het strategisch beleid, van de algemene en financiële risico’s en van het beheers- en controlesysteem van de vennootschap’. Wij zijn het slechts ten dele met deze stelling eens. De code-Tabaksblat gaat namelijk verder, omdat deze ook een externe verantwoording voor de opzet en werking van het irc-systeem vereist.

### 1.3.4 Code-Tabaksblat – hoofdstuk V: de audit

Hoofdstuk v van de code omvat principes en best practicebepalingen voor de audit van de financiële verslaggeving en de positie van de interne auditfunctie en van de externe accountant. Als principe is onder meer gesteld dat:

- de interne accountant, die een belangrijke rol kan spelen in het beoordelen en toetsen van irc-systemen, functioneert onder de verantwoordelijkheid van het bestuur;
- de externe accountant zijn bevindingen betreffende het onderzoek van de jaarrekening gelijkelijk aan het bestuur en de raad van commissarissen rapporteert.

‘Ernst & Young is van mening dat de code op belangrijke onderdelen nog nadere duiding en uitwerking behoeft. Hierbij valt met name te denken aan de genoemde behoefte aan een referentieraamwerk voor interne controle; de exacte rol van de accountant bij de verklaring van het management over die interne controle; de gewenste inhoud van de corporate-governanceverklaring in het jaarverslag en de aard van het optreden van de accountant tijdens algemene vergaderingen van aandeelhouders. Ook het toezicht op de naleving (en de verantwoording daaromtrent) van de code en een eventuele rol daarbij voor de externe accountant, behoeven nadere explicitering.’

(Reactie van accountantskantoor Ernst & Young op de conceptcode-Tabaksblat)

11 O.a. Steven R. Schuit van Allen & Overy, juni 2007.

Het laatstgenoemde principe wordt nader uitgewerkt in de best-practicebepaling v.4.3. Deze bepaling stelt onder meer dat de externe accountant, naar aanleiding van zijn controle van de jaarrekening, in het accountantsverslag aspecten met betrekking tot het irc-systeem onder de aandacht van het bestuur en de raad van commissarissen kan brengen. Voorbeelden van aspecten die daarbij onder de aandacht gebracht zouden kunnen worden, zijn:

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

Expliciet is vermeld dat de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking deel uitmaakt van het risicobeheersings- en controlesysteem.

### 1.3.5 Kritiek op de code-Tabaksblat

Op de code-Tabaksblat is veel kritiek gekomen. De belangrijkste kritiekpunten zijn:

- De code is gebaseerd op het *comply or explain*-principe, waardoor organisaties alleen verplicht zijn om afwijkingen van de code te rapporteren. Met uitzondering van de in-controlverklaring is het niet vereist expliciete mededelingen te doen over de naleving van bepalingen uit de code. Belanghebbenden dienen hierdoor zelf te bepalen welke codebepalingen worden nageleefd.
- De rapportage van afwijkingen van de code is niet aan voorschriften gebonden, waardoor onduidelijkheid kan ontstaan over de vraag of een gerapporteerde afwijking op de juiste wijze is weergegeven.
- De in-controlverklaring is breed gedefinieerd, waardoor het moeilijk is om daarover een gefundeerde uitspraak te doen. De verklaring heeft zowel betrekking op de opzet, het bestaan als de werking van het irc-systeem ten aanzien van alle risicocategorieën. In omringende landen beperkt de regelgeving zich veelal tot de risico's ten aanzien van de financiële rapportage.
- In de code ontbreken duidelijke richtlijnen ten aanzien van:
  - wat onder een irc-systeem moet worden verstaan;
  - welke diepgang in de organisatie dit moet hebben;
  - hoe de effectieve werking ervan moet worden aangetoond;

- wat onder een tekortkoming moet worden verstaan en wanneer deze moet worden gerapporteerd;
- hoe in het jaarverslag moet worden gerapporteerd wat tot onvergelijkbaarheid tussen de risicoparagrafen en de in-controlverklaringen van organisaties kan leiden.
- De juridische consequenties voor het management dat de in-controlverklaring afgeeft zijn onduidelijk.
- De in-controlverklaring wordt afgegeven door het management, zonder dat is voorzien in een inhoudelijke controle hierop. De accountant hoeft de verklaring slechts marginaal te toetsen, wat wil zeggen dat hij slechts hoeft vast te stellen dat de verklaring niet strijdig is met de overige informatie die in het jaarverslag of de jaarrekening is opgenomen. Dit kan tot verwarring leiden, omdat niet iedereen helder voor ogen heeft dat de accountant ‘slechts’ een verklaring over de getrouwheid van de jaarrekening geeft en geen uitspraak doet over informatie die is opgenomen in het jaarverslag van het management, waarvan de in-controlverklaring een onderdeel is. Ten aanzien van het jaarverslag hoeft de accountant alleen te toetsen of het, voor zover hij kan beoordelen, overeenkomstig het jaarrekeningrecht is opgesteld en of het beeld dat het jaarverslag oproept verenigbaar is met de jaarrekening.<sup>12</sup>

Ondanks dat de lijst met kritiekpunten lang is, delen wij de kritiek op de code niet en beschouwen deze als een goede aanvulling op het ondernemerschap. Met name de *principle-based* opzet van de code voorkomt, althans bij een goede implementatie van de code, een afvinkmentaliteit waardoor het gedachtegoed van de code de bedrijfsvoering van een organisatie breed kan ondersteunen. Daarnaast zijn wij van mening dat de brede definiëring van het in-controlbegrip de juiste is, omdat financiën volgen uit de operationele activiteiten en niet fragmentarisch mogen of kunnen worden beschouwd. Het is niet waarschijnlijk dat een organisatie die operationeel niet *in control* is, dat financieel wel kan zijn.

‘Op een aantal punten voorziet de code in belangrijke, extra in het jaarverslag op te nemen informatie, bijvoorbeeld ten aanzien van de effectiviteit van de irc-systemen en de naleving van de corporate-governancecode. Op de rol van de externe accountant wordt in dit kader niet expliciet ingegaan. Deze rol moet naar de mening van het NIVRA duidelijk worden aangegeven, om misverstanden

<sup>12</sup> BW2 titel 9 artikel 393:3.

bij belanghebbenden te vermijden. Hierbij moet ons inziens worden uitgegaan van de in de wet genoemde verantwoordelijkheid van de externe accountant ten aanzien van in het jaarverslag opgenomen informatie.’

(Reactie van het Koninklijk NIVRA, de beroepsorganisatie voor registeraccountants in Nederland, op de conceptcode-Tabaksblat)

Ons positieve beeld van de code wordt onderschreven door een onderzoek dat in 2007 onder beursgenoteerde organisaties in Nederland is uitgevoerd.<sup>13</sup> Daaruit blijkt dat 45 procent van de beursgenoteerde organisaties van mening is dat de baten van de code groter zijn dan de lasten. Hierbij moet worden aangetekend dat met name de grotere beursfondsen aangeven baat te hebben bij de code en dat kleinere beursfondsen het meer als een last beschouwen.

Uit het onderzoek is tevens naar voren gekomen dat zowel grote als kleine beursgenoteerde organisaties het vergroten van de transparantie en de externe communicatie veruit als grootste voordeel van de code zien. Dit voordeel wordt op grote achterstand door het tweede voordeel gevolgd, namelijk dat regels, procedures en processen verder zijn gestructureerd en geformaliseerd.

Tot slot heeft het onderzoek ook duidelijk gemaakt wat als de grootste nadelen van de code gezien worden. Met stip op nummer één staan de administratieve kosten die uit de naleving van de codebepalingen voortvloeien. Dit nadeel wordt op grote achterstand gevolgd door een beperking van de bewegingsvrijheid.

‘Ik ben wel meer voor duidelijke regels dan voor principes die voor meerdere uitleg vatbaar zijn. En op zich is het ook heel goed dat er scherp toezicht is en dat er sancties zijn.’

(Peter Wakkie, *chief corporate governance counsel* van Ahold, in *De Accountant*, juni 2007)

De kritieken die op de code-Tabaksblat zijn geuit, zijn ten dele weggenomen door de commissie-Frijns. Deze commissie is belast met de bewaking van de implementatie van de code en heeft diverse nadere aanwijzingen gegeven inzake vraagstukken die omtrent de code spelen.

---

<sup>13</sup> ‘Corporate governance: kosten en baten van de Nederlandse corporate governance code’, Auke de Bos en Luc Quadackers, juni 2007.