Het evalueren van de interne beheersingsomgeving

Een onderbelicht thema

Oscar van Leeuwen en Philip Wallage

SAMENVATTING Aangezien de effectiviteit van de werking van de zogenaamde interne beheersingsomgeving een belangrijke factor is voor het al of niet verstrekken van betrouwbare informatie, verdient het aanbeveling een goede evaluatie uit te voeren van zowel de opzet als werking van de interne beheersingsomgeving.
In dit artikel wordt een verkenning uitgevoerd naar het beschikbare instrumentarium om een dergelijke evaluatie uit te kunnen voeren. Dit doen we op basis van een synthese tussen het gedachtegoed van COSO (1992, 1994) en Simons (1995, 2000). Wij beogen hiermee een aanzet te geven tot het ontwikkelen van een model om de opzet en werking van een beheersingsomgeving te kunnen beoordelen.

RELEVANTIE VOOR DE PRAKTIJK De beoordeling van de opzet en werking van de interne beheersingsomgeving is in de praktijk complex en vergt de nodige professionele oordeelsvorming. Het in dit artikel geschetste model kan helpen om te komen tot een zorgvuldige evaluatie. Verdergaande ontwikkeling van het model kan eraan bijdragen frauduleuze financiële rapportages in de toekomst te voorkomen.

1 Inleiding

De laatste jaren is er de nodige aandacht geweest voor het beheersen van risico's. Financiële debacles, vaak veroorzaakt door fraude, hebben aanleiding gegeven tot de eis in wet- en regelgeving om risico's en interne beheersingssystemen te evalueren. Achterliggend doel hiervan is zorg te dragen voor betrouwbare rapportages. Tot de verbeelding sprekende voorbeelden van dergelijke debacles zijn Enron en Worldcom en de hieruit voortvloeiende Sarbanes-Oxley Act (2002).

Ook valt te constateren dat de huidige economische crisis langlopend frauduleus handelen blootlegt, omdat dergelijke onregelmatigheden bij dalende markten niet meer zijn vol te houden (zoals Madoffs 'Ponzi Schemes', fraude bij het Indiase IT-bedrijf Satyam Computer Services[1] en de Repo 105-affaire bij Lehman Brothers[2]). Genoemde geruchtmakende debacles kenmerken zich door een tekortschietende interne beheersingsomgeving, waarbij het gedrag van CEO en *board members* verklarende factoren blijken (IFAC, 2003; COSO, 1987[3]; Cools, 2005). Eén en ander resulteert vervolgens in onbetrouwbare externe rapportages waarop aandeelhouders en andere stakeholders vervolgens hun besluiten baseren.

Interne beheersing van financiële rapportages (*internal control* over *financial reporting*) wordt in de context van corporate governance veelal bezien vanuit het Amerikaanse COSO-model. Volgens dit model vormt de interne beheersingsomgeving de basis voor de overige interne beheersings (internal control) -componenten en verschaft de nodige discipline en structuur. Factoren die de IB-omgeving mede bepalen, zijn (COSO, 1992):

- integriteit en waarden;
- competenties;
- filosofie en stijl van leidinggeven;
- toewijzing van bevoegdheden en verantwoordelijkheden;
- organisatie en ontwikkeling van personeel;
- betrokkenheid bestuur.

Dit model kent – voor zover wij hebben kunnen nagaan – geen theoretisch fundament. Gegeven de doelstelling[4] en samenstelling van de COSO Commissie[5] is het overigens niet verwonderlijk dat een praktisch hanteerbaar model tot stand is gebracht. Het model is instrumenteel en sterk gericht op systemen, processen en procedures. Deze technische infrastructuur of architectuur wordt ook wel aangeduid met de term *hard controls*. Echter, de goede werking van deze hard controls is in belangrijke mate afhankelijk van menselijk gedrag (COSO, 1994, p. 15).

Naar onze mening wordt de effectiviteit[6] van de interne beheersingsomgeving (verder voor de leesbaarheid aangeduid met IB-omgeving) voor zover deze invloed heeft op

(financiële) rapportages niet alleen door mensen beïnvloed, maar in belangrijke mate 'bepaald' (Vink en Kaptein, 2008). Deze gedragscomponent is besloten in de cultuur, ethiek en 'tone at the top' van organisaties.[7] Vanwege de door COSO veronderstelde relatie tussen (frauduleuze) financiële verslaggeving en de effectiviteit van de IB-omgeving is het opmerkelijk dat tot op heden weinig onderzoek naar deze relatie is verricht (Hogan, Rezaee, Riley en Velury, 2008). Onderzoek van Hernandez en Groot (2007) impliceert echter het bestaan van een dergelijke relatie.[8] Over de vraag hoe de effectiviteit van de IB-omgeving het beste getoetst kan worden, valt in de literatuur weinig te vinden. Wij zullen in dit artikel daartoe een aanzet geven.

In de volgende paragraaf (par. 2) gaan wij in op de vereiste evaluatie van de IB-omgeving volgens Nederlandse en Amerikaanse en regelgeving. Daarna behandelen wij een alternatieve benadering voor het evalueren van de IB-omgeving gebaseerd op de controltheorie van Simons (par. 3). Vervolgens gaan wij in op de vraag hoe een evaluatie van de IB-omgeving praktisch kan worden uitgevoerd (par. 4). Dit doen we met name op basis van een vergelijking tussen het COSO-model en de 'levers of control' van Simons. In par. 5 doen wij suggesties voor verbetering van het model ter beoordeling van de opzet en werking van de IB-omgeving.

2 De vereiste evaluatie van de interne beheersingsomgeving volgens codes en wetgeving

Hierna volgt een korte beschrijving van de noodzakelijke evaluatie van de IB-omgeving volgens de Amerikaanse Sarbanes-Oxley-wetgeving en de Nederlandse Corporate Governance Code.

Sarbanes-Oxley

In de Verenigde Staten wordt in Sectie 404 van de Sarbanes-Oxley Wet (2002) een verklaring van het management vereist over de effectiviteit van het systeem van interne beheersing met betrekking tot financiële rapportage. De effectiviteit betreft zowel de opzet als de werking. Opvallend genoeg wordt de IB-omgeving in de *guidance* voor het management niet afzonderlijk benoemd (SEC, 2003). Ook in de nadere guidance wordt opmerkelijk weinig aandacht besteed aan de IB-omgeving als onderdeel van zogenaamde *entity level controls* (SEC, 2007).
Opgemerkt wordt dat deze controls een indirect effect hebben op de kans dat een afwijking tijdig wordt voorkomen of ontdekt (SEC, 2007, p. 18). Zij hebben de nodige invloed op andere controls, maar genereren onvoldoende bewijskracht om financiële verslaggevingsrisico's te beheersen. Wel kan volgens de guidance de respectievelijk relatieve sterkte en zwakte van de IB-omgeving de inschatting van de werking van andere beheersingsmaatregelen (*risk of control failure*) door het management beïnvloeden (SEC, 2007, p. 22). Opmerkelijk is dat de inschatting door het management van de kans dat een control niet goed werkt onder andere afhankelijk is van het ingeschatte risico van management *override*. Het management beoordeelt hierbij dus zichzelf!
Ten behoeve van het evalueren wordt het COSO-model in de Sarbanes-Oxley Wet expliciet als een algemeen aanvaard raamwerk benoemd.[9]

Nederlandse Corporate Governance Code (Tabaksblat)

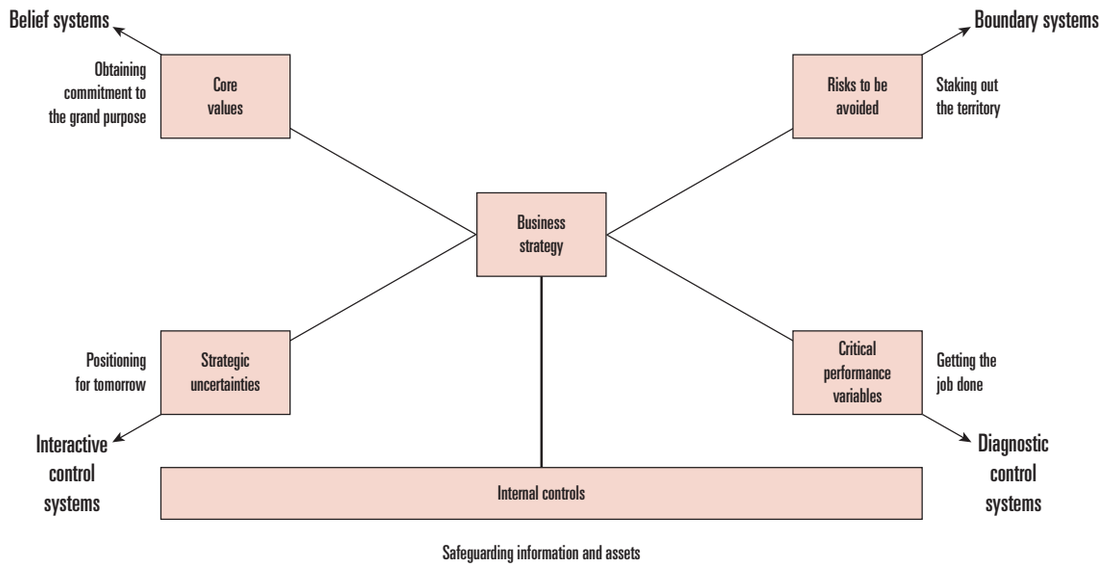
De code-Tabaksblat (2008) vereist in bepaling II.1.5 dat ten aanzien van financiële verslaggevingsrisico's het bestuur in het jaarverslag verklaart 'dat de interne risicobeheersings- en controlesystemen een redelijke mate van zekerheid geven dat de financiële verslaggeving geen onjuistheden van materieel belang bevat en dat de risicobeheersings- en controlesystemen in het verslagjaar naar behoren hebben gewerkt. Het bestuur geeft hiervan een duidelijke onderbouwing.' In de code wordt echter niet toegelicht hoe een dergelijke evaluatie uit te voeren. Ook wordt het belang van de IB-omgeving niet expliciet genoemd. Impliciet gebeurt dit wel doordat de toelichting op de code (Tabaksblat 2003, p. 34) stelt dat het in de rede ligt 'dat het bestuur in de verklaring over de interne risicobeheersings- en controlesystemen aangeeft welk raamwerk of normenkader bij de evaluatie is gehanteerd'. Als voorbeeld wordt het COSO-raamwerk genoemd.

3 Het systeem van interne beheersing volgens Simons

Het COSO-model wordt derhalve als algemeen aanvaard beschouwd voor het evalueren van de effectiviteit van het systeem van interne beheersing op het gebied van (financiële) rapportages.[10] Het kent voor zover bij ons bekend echter geen theoretische fundering. Critici stellen dat een alomvattende set van instrumentarium en technieken nodig is om een effectieve beheersing en naleving te bereiken (Alles en Datar, 2004[11]). Een management controlbenadering kan voorkomen dat een te sterke focus wordt gelegd op het bestaan en de documentatie van het beheersingssysteem in plaats van de effectieve werking ervan. Het ontbreken van een theoretische fundering kan dan ook leiden tot een ongebalanceerde toepassing van het COSO-model. Daar komt bij dat het hanteren van een theoretisch fundament een waardevolle toevoeging aan het COSO-model levert doordat niet alleen gekeken wordt welke beheersingsmaatregelen op het gebied van betrouwbaarheid van (financiële) rapportages bestaan, maar ook waarom deze noodzakelijk zijn (relevantie).

Om te bezien of het COSO-raamwerk vanuit een theoretisch kader verrijkt kan worden, zullen wij de elementen van de

Figuur 1 Simon's Lever's of Control*



* Adapted from Kaplan & Norton, Figure 13.1, p. 349. Original source, Simons, p. 159.

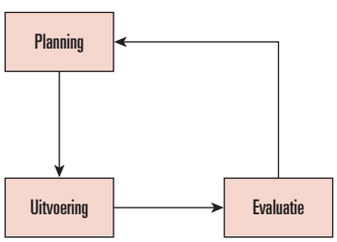
IB-omgeving zoals uitgewerkt door COSO, confronteren met de management control-theorie van Robert Simons zoals die is uitgewerkt in vier 'levers of control'.[12] Hierna geven wij een illustratie van en toelichting op de vier 'levers of control' die Simons onderscheidt (zie figuur 1).

3.1 Diagnostic control systems

'Diagnostic control systems are the formal information systems that managers use to monitor organizational outcomes and correct deviations from preset standards of performance' (Simons, 1995, p. 59).

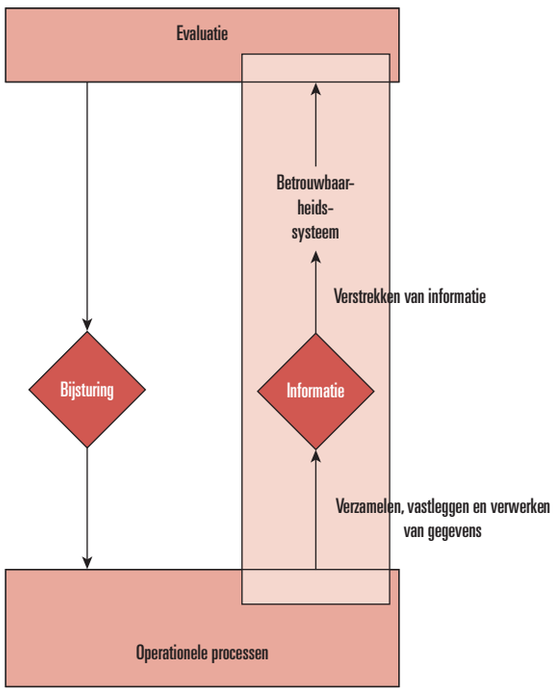
Management control betreft in de *diagnostic control systems*-visie: 'Het door de leiding van een organisatie aangestuurde en toegepaste proces ten behoeve van het beheersen van de uit te voeren bedrijfsactiviteiten.' Management control is gericht op het implementeren en realiseren van vooraf gedefinieerde doelen. Traditioneel is management control ingevuld vanuit een regelkringgedachte (zie figuur 2). In het algemeen zal men ten behoeve van het beheersen van (bedrijfs)activiteiten informatie nodig hebben voor het nemen van besluiten. Besluiten inzake de planning worden genomen op basis van informatie inzake allerlei verwachtingen en schattingen aan de hand waarvan diverse afspraken en standaarden worden afgeleid. Vervolgens wordt gemeten wat er werkelijk gebeurt. Daarna wordt de planning vergeleken met de realisatie (evaluatie). Uiteraard dient men ook na te gaan of de uitvoering niet te sterk afwijkt van hetgeen was beoogd. Ten slotte vindt indien noodzakelijk bijsturing plaats. Deze bijsturing kan betrekking hebben op zowel de wijze van uitvoering als de gebruikte normen of de planning. Informatie en daarmee de betrouwbaarheid hiervan maken onlosmakelijk deel uit van het diagnostic control systeem (zie figuur 3).

Figuur 2 Regelkringgedachte



Simons (2000) toont aan dat diagnostische control systems niet onfeilbaar zijn, zeker niet waar 'empowered employees' verantwoordelijk zijn voor het behalen van de gestelde normen. Hij noemt het voorbeeld van een bedrijf waar medewerkers die volgens een diagnostic control system werden afgerekend op omzet naar rato van uren, door hun managers onder druk werden gezet om minder uren in te vullen teneinde mooiere ratio's te behalen. Dergelijke omstandigheden blijken het laatste decennium een belangrijke oorzaak van frauduleuze financiële verslaggeving. Dit onderstreept de noodzaak dat er binnen een orga-

Figuur 3 Het betrouwbaarheidssysteem als onderdeel van het diagnostic control systeem



nisatie nog andere 'control systems' aanwezig moeten zijn en dat de wijze van beheersen ook invloed uit kan oefenen op de betrouwbaarheid van de informatie.

Het achterliggende probleem is dat morele dilemma's ontstaan als gevolg van conflicterende waarden. Enerzijds is er de norm te voldoen aan interne procedures, anderzijds de norm managers te gehoorzamen (met als mogelijk aanvullend belang het verkrijgen van een hogere bonus). Het 'beliefs system' geeft de nodige richting aan het verantwoord oplossen van dergelijke dilemma's.

3.2 Beliefs systems

'A beliefs system is the explicit set of organizational definitions that senior managers communicate formally and reinforce systematically to provide basic values, purpose, and direction for the organization. (...) The primary purpose of a beliefs system is to inspire and guide organizational search and discovery' (Simons, 1995, p. 36).

In wat Simons 'beliefs system' noemt, worden de waarden waar een organisatie voor staat tot uitdrukking gebracht. De waarden waarvan managers graag zien dat medewerkers ze tot uitdrukking brengen in hun gedrag. Kenmerkend voor deze systemen is hun bondige, normerende, liefst inspirerende karakter. Als gedeelde waarden in beleid en gedrag centraal staan, zijn 'beliefs systems' een krachtig middel om de organisatie 'in control' te houden. Bij organisaties waar 'corporate responsibility' hoog in het vaandel staat (zie bijvoorbeeld CSR-verslagen van TNT, Shell, Philips, Heineken), worden deze waarden dikwijls openbaar gemaakt. Deze uitingen geven inzicht in de opzet van de IB-omgeving, maar het is moeilijk vast te stellen wat het werkelijke gedrag is. Het 'beliefs system' kan worden gezien als de kern van de IB-omgeving zoals COSO die definieert. Het al dan niet transparant rapporteren door een organisatie is een belangrijk onderdeel van het 'beliefs system', dat een bijdrage kan leveren aan de betrouwbaarheid van (financiële) rapportages.

3.3 Boundary systems

'Although boundary controls are essentially proscriptive or negative systems, they allow managers to delegate decision making and thereby allow the organization to achieve maximum flexibility and creativity' (Simons, 1995, p. 41).

In 'boundary systems' worden de grenzen aangegeven van het gedrag in organisaties. Anders dan een generatie antiautoritaire opvoeders ooit dacht, bieden systemen van verbod veel vrijheid. Ze zeggen namelijk wat je níet moet doen, en laten je impliciet zelf bepalen wat je wél moet doen. Medewerkers vertellen wat ze niet moeten doen, laat ruimte voor innovatie, maar binnen helder gestelde grenzen en limieten. Controle op naleving van wet- en regelgeving (*boundary*) wordt door COSO aangeduid als compliance. Er bestaat (inter)nationaal de nodige gedetailleerde wet- en regelgeving die gericht is op wat wel en niet mag bij het opstellen en verschaffen van betrouwbare financiële rapportages. Ook dergelijke 'boundary systems' hebben de nodige debacles niet weten te voorkomen.

3.4 Interactive control systems

'Interactive controls are formal information systems managers use to involve themselves regularly and personally in the decision activities of subordinates...' (Simons, 1995, p. 95).

Bij 'interactive control systems' gaat het om de vraag 'gaan we wel de goede kant op?' *Interactive control systems* richten zich op het soort onzekerheden waar managers 's nachts wakker van liggen. Om deze systemen van gegevens te voorzien, zijn 'sensoren' nodig die gegevens verschaffen over bijvoorbeeld markt, klanten en belangrijke technologische ontwikkelingen. Managers gebruiken deze systemen dan ook om zich persoonlijk te bemoeien met beslissingen van medewerkers, teneinde hun aandacht en het leervermogen te richten op belangrijke strategische

issues. Daarmee is het interactive control systeem een belangrijk middel voor het management om een belangrijk onderdeel van de IB-omgeving, namelijk de 'tone at the top', enerzijds uit te dragen en anderzijds *bottom-up* vast te stellen in hoeverre de organisatie de 'juiste toon' weet te vinden.

Bij interactive control systems gaat het om onbekende problemen, om onverwachte bedreigingen maar ook om onverwachte kansen. Omdat de oplossing hier niet bij voorbaat aanwezig is, komt de interpretatie van gegevens het beste in dialoog tot stand.
Interactive controls zijn belangrijk omdat zij het senior management aangeven wanneer zij de strategie moeten aanpassen en wijzigingen moeten aanbrengen in de beliefs, boundary en diagnostic controls die ervoor moeten zorgen dat de strategie wordt bereikt. Met andere woorden, interactive controls zorgen ervoor dat de gehele beheersingsarchitectuur dynamisch is. Interactive controls worden om twee redenen belangrijker als het gaat om betrouwbare financiële rapportage. In de eerste plaats door de toenemende complexiteit van financiële markten, producten en verslaggeving en in de tweede plaats door de grote snelheid van veranderingen in regels, systemen en processen, vooral als gevolg van verdergaande automatisering.

3.5 De vier levers of control en betrouwbaarheid van de informatieverzorging

Geen van de vier levers of control is – zoals hiervoor blijkt – afzonderlijk in staat om de betrouwbaarheid van de (financiële) informatieverzorging te borgen. Volgens Simons is continue bewaking van de beliefs en boundary controls nodig om te zorgen dat geen van de twee de andere domineert. Het voordeel van beide controls is dat, indien deze samenwerken, geen extremen ontstaan zoals het geval kan zijn als er slechts één van de twee werkt. Om te begrijpen welke bijdrage een expliciet beheersingsperspectief kan hebben aan het voorkomen van frauduleuze financiële rapportage, moeten ook de diagnostic en interactive controls bezien worden. Diagnostic controls zorgen ervoor dat de doelstellingen efficiënt en effectief worden bereikt, met een minimaal beslag op de schaarse tijd van het management. Het doel is om het juiste gedrag te stimuleren door het aloude adagium 'meten is weten'. Stappen die het diagnostische beheersingsproces kenmerken, zijn het onderkennen van relevante prestatie-indicatoren, het volgen van de informatiestroom die deze prestatie-indicatoren automatisch genereert en vergelijken met vooraf geformuleerde verwachtingen ten behoeve van 'management by exception'. Interactive controls maken onlosmakelijk deel uit van dit proces. Vanwege het delegeren van taken is communicatie (dialoog) tussen de verschillende (hiërarchische) niveaus nodig om af te stemmen of de overeengekomen doelstellingen worden bereikt of moeten worden aangepast.

Er wordt door Simons dus een onderscheid gemaakt tussen beheersingsmaatregelen die het registreren en verzenden van informatie richting geven en maatregelen die het gedrag van degenen die de informatie opstellen, beïnvloeden. COSO en Sarbanes-Oxley (in het bijzonder Sectie 404) maken een dergelijk onderscheid niet. Hierdoor ontstaat het risico dat het evalueren van het systeem van interne beheersing op het gebied van (financiële) rapportages zich meer richt op de groep controls rondom het registreren en verzenden van informatie (*hard controls*), die conceptueel veel simpeler zijn, veel omvangrijker en mechanisch kunnen worden geïmplementeerd, dan de tweede groep, die bijvoorbeeld een fundamentele beoordeling van de beloningsstructuur en van de interne gezagsverhoudingen en cultuur vereisen (*soft controls*). Om de betrouwbaarheid van de financiële informatieverzorging te borgen, is een goede balans tussen de levers of control dan ook onmisbaar.

4 Het beoordelen van de IB-omgeving: een vergelijking van COSO met Simons

In deze paragraaf gaan wij in op de verschillen en samenhang tussen COSO en Simons als het gaat om de evaluatie van de effectiviteit van de IB-omgeving. In bijlage 1 hebben wij de vragen opgenomen die COSO stelt om de IB-omgeving te evalueren (COSO, 1992, p. 31). Per vraag hebben wij vervolgens een inschatting gemaakt op welk van de vier 'levers' van Simons deze vraag betrekking heeft.[13]

Bij het analyseren van de 'confrontatie' van COSO met Simons valt een aantal zaken op:

- De vragen die COSO stelt, betreffen merendeels diagnostic controls (60 procent). Vragen op het gebied van beliefs (25 procent), maar vooral boundary (7 procent) en interactive controls (8 procent) lijken onderbelicht.
- De vragen die COSO stelt, bevatten geen (inherente) normen waar de IB-omgeving aan moet voldoen (de antwoorden op de vragen kunnen daardoor niet SMART[14] gemeten worden ten opzichte van een norm). Zo is onduidelijk welke frequentie van de interactie tussen senior en operating management als norm moet worden gehanteerd voor een goede IB-omgeving. Het beoordelen hiervan is dus subjectief van aard.
- De vragen die COSO stelt, hebben met name betrekking op de opzet van de IB-omgeving. Of de IB-omgeving ook echt zo werkt, wordt niet vastgesteld.

Wij merken overigens op dat de vragen die COSO stelt ter zake van de IB-omgeving zich niet beperken tot het beheersen van de betrouwbaarheid van de (financiële) rapportage, maar ook de andere twee hoofddoelstellingen van COSO betreffen, namelijk het naleven van wet- en regelgeving en effectiviteit en efficiency van bedrijfsprocessen. Voor het verstrekken van betrouwbare informatie zijn effectiviteit en efficiëntie van andere dan informatieverzorgende bedrijfsprocessen niet nodig. Aangezien de vragen inzake de IB-omgeving door COSO zodanig zijn geformuleerd dat ze elk van de COSO-doelstellingen afdekken, is naar onze mening een splitsing van de vragen naar de verschillende COSO-doelstellingen niet per definitie nodig.
In de volgende paragraaf gaan wij nader in op enkele bevindingen die uit deze analyse volgen.

5 Mogelijke verbeteringen van het COSO-model ter beoordeling van de effectiviteit van de IB-omgeving

Om de IB-omgeving te evalueren, zal het management van een organisatie op dit moment in het algemeen slechts beschikken over de vragenlijsten die als bijlage zijn opgenomen in het COSO-rapport van 1992 (Martin, 2007). Zoals in de vorige paragraaf opgemerkt, verdient het COSO-model de nodige aanpassingen om de effectiviteit van de IB-omgeving goed te kunnen evalueren. Hierbij moet steeds in gedachten worden gehouden dat een belangrijk doel van COSO is om een IB-omgeving te creëren die leidt tot betrouwbare financiële verslaggeving die in overeenstemming is met wet- en regelgeving. Wij richten ons met name op de betrouwbaarheid van deze rapportages. In deze paragraaf doen wij enkele suggesties ter verbetering van het COSO-model, waarbij in paragraaf 5.1 en 5.2 eerst de beoordeling van de opzet en het bestaan van de IB-omgeving behandeld worden en daarna in paragraaf 5.3 de werking.

5.1 Uitbreiding van het model met vragen op het gebied van beliefs, boundary en interactive controls

Om de vragen van COSO meer nadruk te geven op het gebied van beliefs, boundary en interactive controls, kan gebruik worden gemaakt van het model dat Vink en Kaptein hebben ontwikkeld (Vink en Kaptein, 2008; Martin, 2007). Vink en Kaptein beschrijven een model dat ontwikkeld is voor het bepalen van de mate van aanwezigheid van soft controls. Dit 'organisatiekwaliteitenmodel' is naar onze mening bruikbaar om de opzet van de IB-omgeving te beoordelen. Zo hebben Vink en Kaptein dit model onder meer gebruikt bij het analyseren van oorzaken van rechtmatigheidsfouten in de jaarverslagen 2006 van de rijksoverheid. De analyse leert dat geen van de fouten als oorzaak het falen van louter hard controls is, terwijl bij 17 procent van de fouten het ontbreken van soft controls de oorzaak is. In 80 procent van de fouten is de oorzaak gelegen in het falen van zowel soft als hard controls. Soft controls blijken vooral belangrijk te zijn bij het tegengaan van oneigenlijke druk van de politiek en de ambtelijke leiding (Vink en Kaptein, 2008). Hun model omvat acht dimensies van de IB-omgeving. Toegespitst op het onderwerp betrouwbaarheid van informatie en ingepast in het management control-model van Simons van informatie kunnen deze dimensies als volgt worden geherformuleerd:

Beliefs systems

1. Helderheid: Is voor iedere medewerker duidelijk wat er van hen mag worden verwacht om zorg te dragen voor een betrouwbare informatieverzorging?
2. Betrokkenheid: zijn bestuurders en medewerkers voldoende gemotiveerd om betrouwbare informatie te verstrekken?[15]

Interactive control systems

3. Voorbeeldgedrag: geven managers en controllers het goede voorbeeld ten aanzien van betrouwbaarheid van informatie?
4. Transparantie: is er voldoende zicht op het gedrag van mensen ten aanzien van de betrouwbaarheid van informatie?
5. Bespreekbaarheid: zijn dilemma's op het gebied van betrouwbaarheid van informatie voldoende bespreekbaar?
6. Aanspreekbaarheid: is de cultuur zodanig dat managers, controllers en medewerkers elkaar aanspreken op (ongewenst) gedrag?

Boundary systems

7. Uitvoerbaarheid: ervaren managers, controllers en medewerkers voldoende ruimte om rechtmatig te handelen?
8. Handhaving: wordt gewenst gedrag op het gebied van betrouwbaarheid van informatie gewaardeerd en ongewenst gedrag bestraft?

Om meer balans te brengen in de evaluatie van de IB-omgeving, raden wij aan de vragenlijst van COSO uit te breiden met voorgaande typen vragen.

5.2 De vragen zoals COSO die stelt, bevatten geen norm voor wat een goede beheersingsomgeving is

Op de constatering dat de vragen zoals COSO die stelt, geen norm bevatten voor wat nu een goede en wat een slechte IB-omgeving is, zou de meest eenvoudige suggestie zijn om een dergelijke norm te incorporeren in de vragen zodat de antwoorden op de vragen ook 'SMART' ten opzichte van

de norm gemeten kunnen worden. Dit is niet eenvoudig aangezien een dergelijke norm sterk situatieafhankelijk is (contingentie-theorie). Zo zal, indien er sprake is van losse delegatie, er een lagere rapportagefrequentie zijn en zijn andere interne beheersingsmaatregelen gewenst dan in een situatie van strakke delegatie. Bij het bepalen van de norm zijn in dergelijke situaties de nodige deskundigheid en ervaring gewenst. Maar ook als de specifieke situatie bekend is, kan lang worden getwist over de invulling van de norm. Wat is bijvoorbeeld de norm voor integriteit? Hoe meet je integriteit dan? Ook deze norm wordt vaak bepaald door de specifieke context.

Dit betekent dat voor elke organisatie het management (en ten aanzien van het management de toezichthouder) per te beantwoorden vraag expliciet een norm zou moeten bepalen waartegen de IB-omgeving gemeten kan worden. Een dergelijke norm kan mede op basis van meerjarige ervaringen worden ontwikkeld. Van belang is dat deze normen voor beoogde gebruikers beschikbaar zijn.

Het zou vervolgens helpen als bij het beantwoorden van de vragen ten opzichte van de norm gemeten wordt op bijvoorbeeld een ordinale vijfpuntsschaal in hoeverre de norm wel of niet behaald wordt. Hierdoor is het tevens mogelijk ontwikkelingen in de tijd te volgen.

Een apart vraagstuk hierbij is nog wie de vragen moeten beantwoorden. Om tot een goed afgewogen beeld te komen, zou dit niet alleen het management moeten zijn, maar ook een subset van de overige medewerkers van de organisatie. Daarbij moet uiteraard aandacht worden besteed aan verschillen in beantwoording door verschillende participanten in de organisatie. Dit laatste vraagstuk werken wij in het kader van dit artikel niet verder uit.

Voorgaande paragraaf maakt in elk geval helder dat het normeren van de IB-omgeving een nog nader te ontginnen terrein is, waar op dit moment 'professional judgement' noodzakelijkerwijs een belangrijke rol bij speelt.

5.3 Een goede werking van de IB-omgeving wordt niet vastgesteld

Het is bij de evaluatie van de IB-omgeving noodzakelijk dat de beoordeling op een transparante wijze wordt uitgevoerd.[16] Dat vereist dat niet alleen de conclusie toetsbaar is, maar ook zoals gezegd de normen beschikbaar zijn en dat het uitgevoerde proces en bijbehorende overwegingen om te komen tot een oordeel, transparant en toetsbaar zijn. Het gaat hierbij onder meer om het kunnen toetsen van de overwegingen die betrekking hebben op dilemma's waarvoor het management zich ten aanzien van de IB-omgeving gesteld zag.

De vragen zoals behandeld in de bijlage en in paragraaf 5.1 en 5.2 betreffen met name de opzet van de IB-omgeving. Deze moeten vervolgens nog op hun werking worden getoetst, waarbij de getrokken conclusie op een transparante wijze moet volgen uit de analyse.

Als het antwoord op bijvoorbeeld de vraag 'Is er voldoende zicht op het gedrag van het management ten aanzien van de betrouwbaarheid van informatie?' ja is, dan moet dit niet alleen in opzet zo zijn, maar moet ook worden vastgesteld hoe dit toezicht gewerkt heeft en behoort deze conclusie gedocumenteerd te worden.

Soms is het vaststellen van de werking eenvoudig. Bijvoorbeeld bij de vraag naar de rapportagefrequentie. Er is eenvoudig vast te stellen hoe vaak een rapportage verstrekt wordt. Maar soms is het niet eenvoudig. Hoe meet je bijvoorbeeld integriteit?Zijn wij als (management) integer? Aan wie vraag je dat dan allemaal? Hoe weeg je verschillende uitkomsten? Hoe moet een toezichthouder het antwoord van het management vervolgens wegen? Het management zal waarschijnlijk niet van zichzelf zeggen dat hij niet integer omgaat met de betrouwbaarheid van de informatieverzorging. Het minste wat het management kan doen, is periodiek in een vergadering met het bestuur (en het bestuur met de commissarissen) bespreken of er aanwijzingen zijn dat één van de vragen niet op de 'norm' scoort.

Het management kan bij het beoordelen van de IB-omgeving onder meer gebruikmaken van de volgende instrumenten:

- Het ondertekenen van een 'letter of representation', waarin expliciet voorgaand raamwerk wordt getoetst. Hiermee wordt het probleem van het vaststellen van de goede werking van de IB-omgeving (deels) omlaag gedelegeerd. Het risico van bias door het tekenende management is hierbij uiteraard aanwezig, aangezien dit in feite een vorm van zelfcontrole betreft. Een ander risico van een dergelijke 'zelfevaluatie' is het risico dat het hogere management niet van alle feiten en gebeurtenissen op de hoogte is.
- Een afzonderlijke functionaris (eventueel daarin gespecialiseerde externe of eigen medewerkers) de werking van het raamwerk laten toetsen door interviews en enquêtes.
- Stimuleren van een onafhankelijk gepositioneerde rapportagelijn inzake afwijkingen van het raamwerk (*whistleblower*-regelingen).
- Van de norm afwijkend gedrag moet worden meegenomen in de beoordeling (wellicht gekoppeld aan de beloning) van de betreffende medewerker.

Afsluitend achten wij het opportuun indien het management vervolgens (in het kader van bijvoorbeeld de code-Tabaksblat) de belangrijkste risico's met betrekking tot de IB-omgeving in relatie tot de betrouwbaarheid van de financiële verslaggeving openbaar maakt en daarbij uiteenzet hoe de effectiviteit wordt gewaarborgd.

6 Conclusie

Wij concluderen dat het belang van de evaluatie van de effectiviteit van de IB-omgeving als het gaat om de betrouwbaarheid van financiële verslaggeving in wet- en regelgeving wordt onderkend. Er zijn echter nauwelijks methoden en/of instrumenten beschikbaar om een dergelijke beoordeling van de IB-omgeving uit te voeren. In dit artikel is, gebaseerd op het raamwerk van COSO en Simons, aangevuld met de inzichten van onder meer Vink en Kaptein, geïllustreerd dat een praktisch maar goed gefundeerd raamwerk kan worden ontworpen voor het beoordelen van de IB-omgeving. Het verdient aanbeveling om dit handvat of een alternatief model nader te onderzoeken en uit te werken aangezien de werking van de IB-omgeving een belangrijke factor is voor het al of niet verstrekken van betrouwbare informatie! ■

Prof. dr. O.C. van Leeuwen is hoogleraar Bestuurlijke Informatieverzorging aan de Vrije Universiteit Amsterdam en tevens Chief Executive Officer van Atos Consulting.
Prof. dr. Ph. Wallage is hoogleraar Accountantscontrole aan de Universiteit van Amsterdam en tevens als partner werkzaam bij KPMG.

Literatuur

- Alles, G.A. en S.M. Datar (2004), How do you stop the books from being cooked? A management control perspective on financial accounting standard setting and the section 404 requirements of the Sarbanes Oxley Act, *International Journal of Disclosure and Governance*, vol.1, no. 2, pp. 119-137.
- Cadbury Report (1992), *The Financial Aspects of Corporate Governance* (*The Cadbury Report*), Financial Reporting Council, London Stock Exchange, The Accountancy Profession, December 1992.
- Commissie Corporate Governance, (commissie-Peters) (1997), *Corporate Governance in Nederland, De 40 aanbevelingen*.
- Commissie Corporate Governance (commissie-Tabaksblat), *De Nederlandse Corporate Governance Code (2003, 2008)*, zie www.commissiecorporategovernance.nl.
- Cools, K. (2005), *Controle is goed, vertrouwen is nog beter*, Assen: Van Gorcum.
- Hogan, C.E., Z. Rezaee, R.A. Riley Jr. en U.K. Velury (2008), Financial statement fraud: Insights from the academic literature, *Auditing: A Journal of Practice and Theory*, vol. 27, no. 2, pp. 231-252.
- Committee of Sponsoring Organizations (COSO) (1987), *Report of the National Commission on Fraudulent Financial Reporting*; zie: http://www.coso.org/FraudReport.htm.
- Committee of Sponsoring Organizations (COSO) (1992, 1994), *Internal Control – Integrated Framework*; zie www.coso.org.
- Hernandez, J.R. en T. Groot (2006), *How trust underpins auditor fraud risk assessments*, ARCA Research Memorandum, Vrije Universiteit, Amsterdam.
- International Federation of Accountants (2003), *Rebuilding public confidence in financial reporting, An international perspective*; zie: www.ifac.org.
- Knoops, C.D. (2008), Transparantie in de beloning van topbestuurders, *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 82, nr. 7/8, pp. 314-316.
- Martin, R.D. (2007), Through the ethics looking glass, *Journal of Business Ethics*, vol. 70, no. 1, pp. 5-14.
- Mulders, H.A. en H.P. Zevenhuizen (2009), Soft controls in the Netherlands: more recognized than anywhere else (interview met James Roth), *Auditing Magazine*, no. 4, december, pp. 6-8.
- SEC (2003), Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports of Non-Accelerated Filers and Foreign Private Issuers.
- SEC (2007), Interpretive Release: Commission Guidance Regarding Management's Report on ICFR Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934.
- Simons, R. (1995), *Levers of control: how managers use innovative control systems to drive strategic renewal*, Harvard Business School Press.
- Simons, R. (2000), *Performance measurement and control systems for implementing strategy*, Prentice Hall.
- Valukas-rapport (2010), Report of Anton R. Valukas, Examiner in the Lehman Brothers Holding Inc., vol 3. Section III.A.4: Repo 105; zie: http://lehmanreport.jenner.com.
- Vink, H.-J. en M. Kaptein (2008), Soft controls bij de Rijksoverheid, *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 82, nr. 6, pp. 256-263.

Bijlage 1 Vragen die COSO stelt rondom de IB-omgeving, geclassificeerd naar de levers of control systems van Simons

	Diagnostic	Beliefs	Boundary	Interactive
COSO				
1. Integriteit en ethische waarden				
a. bestaan en implementatie van gedragscodes en overig beleid m.b.t. handelen, tegengestelde belangen of verwachte standaarden m.b.t. ethisch en moreel handelen		x		
b. totstandkoming van 'tone at the top' inclusief richtlijnen ten aanzien van goed en kwaad en de mate van communicatie hiervan in de organisatie		x		
c. relaties met werknemers, leveranciers, verzekeraars, concurrenten en accountants, enz. (bijvoorbeeld of management handelt op een hoog ethisch niveau en van anderen eist dat zij dat ook doen, respectievelijk weinig aandacht besteedt aan ethische issues)		x[17]		
d. toereikendheid van herstelactie genomen in reactie op afwijkingen van goedgekeurde policy's en procedures of afwijkingen van de gedragscode. Mate waarin herstelactie is gecommuniceerd of bekend wordt in de organisatie			x	
e. houding van management ten opzichte van respectievelijk interventie en overriding van interne beheersing		x		
f. druk om onrealistische prestatiedoelen te bereiken, m.n. als het gaat om kortetermijnresultaten en de mate waarin beloning is gebaseerd op deze prestatiedoelen	0,5 x[18]	0,5 x		
2. Commitment to competence				
a. formele of informele taakbeschrijvingen of andere wijze van vastlegging van specifieke functies	x[19]			
b. analyse van de kennis en vaardigheden die nodig zijn om functies adequaat uit te voeren	x			
3. Board of Directors or Audit Committee				
a. onafhankelijkheid van management zodat wanneer nodig ook in moeilijke en uitdagende situaties vragen worden gesteld	x			
b. instelling van commissies indien nodig om diepgaande of directe aandacht aan zaken te besteden	x			
c. kennis en ervaring van directors	x			
d. frequentie en tijdigheid waarin wordt vergaderd met de CFO en of accounting officers, interne en externe accountants	x			
e. tijdigheid en mate waarin informatie wordt verstrekt aan de board om bewaking van doelstellingen en strategie van management, de financiële positie en resultaten alsmede de belangrijkste afspraken te bewaken	x			
f. mate en tijdigheid van informeren van de board van gevoelige informatie, onderzoeken en onethisch gedrag (reiskosten, overtreding van regels, omkoping e.d.)	0,5 x[20]		0,5 x	
g. toezicht op bepalen van beloning van executives, hoofd IAD, aanstelling en ontslag	x			
h. rol bij het tot stand brengen van juiste 'tone at the top'		x		
i. nodige acties die board neemt in geval van bevindingen van bijvoorbeeld bijzondere onderzoeken				x
4. Organisatiestructuur				
a. toereikendheid van organisatiestructuur en de mogelijkheid om de nodige informatie te verstrekken om activiteiten te beheersen	x			
b. juistheid/toereikendheid van definities van verantwoordelijkheden van belangrijke managers en van het begrip dat zij van deze verantwoordelijkheden hebben	x			
c. juistheid/toereikendheid van kennis en ervaring van belangrijke managers in het licht van verantwoordelijkheden	x			
d. toereikendheid van rapportagelijnen	x			
e. mate waarin veranderingen in de organisatiestructuur in het licht van veranderende omstandigheden zijn gemaakt				x
f. mate waarin voldoende mensen beschikbaar zijn, met name in managemewnt- en toezichthoudende functies	x			
5. Toekennen van beschikkingsbevoegdheden en verantwoordelijkheden				
a. toereikendheid van verantwoordelijkheden en delegatie van bevoegdheden om te kunnen omgaan met organisatiedoelen en doelstellingen, operaties en wettelijke vereisten inclusief verantwoordelijkheden voor informatiesystemen en bevoegdheden	x			

b. toereikendheid van beheersingsgerelateerde standaarden en procedures, inclusief taakbeschrijvingen van werknemers	x			
c. toereikendheid van aantal werknemers, in het bijzonder voor wat betreft dataprocessing en accounting functies, met vereiste vaardigheden bezien vanuit omvang van organisatie en aard en complexiteit van activiteiten en systemen	x			
d. toereikendheid van delegatie van bevoegdheden in relatie tot toegewezen verantwoordelijkheden	x			
6. Filosofie en stijl van leidinggeven				
a. aard van aanvaarde bedrijfsrisico's (neemt management bijvoorbeeld vaak veel risico's of is het management extreem conservatief)				x
b. verloop van belangrijk personeel (in operaties, verslaggeving, dataprocessing, internal audit)	x			
c. houding van management t.o.v. data processing en accounting functies en de zorg die bestaat m.b.t. de betrouwbaarheid van financiële rapportages en bewaken van activa		x		
d. frequentie van de interactie tussen senior en operating management, met name als de operaties geografisch verspreid zijn	x			
e. houding en acties ter zake van financiële rapportage inclusief onenigheid over toepassing van verslaggevingsstandaarden (selectie van respectievelijk conservatieve en liberale standaarden, in hoeverre verslaggevingsstandaarden zijn misbruikt, belangrijke informatie niet is toegelicht, enz.)		x		
7. HR policies and practices				
a. mate waarin beleid en procedures voor het aannemen, trainen, promoveren en belonen van werknemers zijn geïmplementeerd	x			
b. mate waarin mensen zich bewust zijn van hun verantwoordelijkheden en verwachtingen daaromtrent		x		
c. toereikendheid van herstelactie die wordt genomen n.a.v. afwijkingen van goedgekeurd beleid en goedgekeurde procedures			x	
d. mate waarin personeelsbeleid invulling geeft aan juiste/toereikende ethische en morele standaarden		x		
e. juistheid/toereikendheid van achtergrondonderzoek van kandidaten, vooral m.b.t. eerdere gebeurtenissen of activiteiten die door de organisatie als niet onaanvaardbaar worden beschouwd	x			
f. juistheid/toereikendheid van de criteria voor werknemersretentie en promotie en de hiertoe beschikbare technieken (prestatie-evaluatie) in relatie tot de gedragscode of andere gedragsrichtlijnen	x			
Totaal	**23**	**9,5**	**2,5**	**3**

Noten

1 *Het Financieele Dagblad*, 7 januari 2009.
2 Rapport van Valukas, 2010.
3 COSO (1987) stelt als belangrijkste aanbevelingen om frauduleuze financiële verslaggeving te voorkomen: 'The tone set by top management that influences the corporate environment within which financial reporting occurs. To set the right tone, top management must identify and assess the factors that could lead to fraudulent financial reporting; all public companies should maintain internal controls that provide reasonable assurance that fraudulent financial reporting will be prevented or subject to early detection – this is a broader concept than internal accounting controls – and all public companies should develop and enforce effective, written codes of corporate conduct.'
4 'We believe this report offers a number of benefits. With this foundation for mutual understanding, all parties will be able to speak a common language and communicate more effectively. Business executives will be positioned to assess control systems against a standard, and strengthen the systems and move their enterprises toward established goals. Future research can be leveraged off an established base. Legislators and regulators will be able to gain an increased understanding of internal control, its benefits and limitations. With all parties utilizing a common internal control framework, these benefits will be realized' (COSO, 1994, p. 9).
5 Auteur Coopers & Lybrand (COSO, 1992).
6 In deze bijdrage impliceren wij met de effectiviteit van de werking zowel de opzet als de werking.
7 Gedrag blijkt ook een belangrijke factor voor het ontstaan van de kredietcrisis en de daarop volgende recessie. Zo valt een mix van gedragsgerelateerde kenmerken te onderkennen zoals hebzucht, roekeloosheid, het onvoldoende begrip hebben van complexe producten, het wegvallen van vertrouwen en zekerheden met alle (financiële) gevolgen van dien.
8 Zie ook interview met James Roth (Mulders en Zevenhuizen, 2009).
9 'After consideration of the comments, we have modified the final requirements to specify that management must base its evaluation of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment.' COSO wordt ook in Auditing

Standard no. 2 en 5 van de PCAOB expliciet genoemd als een te hanteren raamwerk.

10 Zo verwijzen Cadbury (1992), Peters (1997) en Tabaksblat (2003) naar het COSO- model.

11 In de woorden van Alles en Datar (2004): 'A management control perspective can provide a much-needed framework within which the COSO standards can be applied, avoiding an excessive focus on the existence and documentation of controls rather than on their efficacy.'

12 Alles, Datar (2004):

- 'Belief systems, such as the Ten Commandments, the US Constitution, or a firm's mission statement lay out the fundamental principles for what constitutes acceptable behavior.
- Boundary controls are rules that very clearly state what people must or mustn't do in specific situations.
- Diagnostic controls, are such familiar procedures as budgets, variance analysis, pay-for-performance and reporting requirements, that are used by firms to set up routines that ensure that everyday, repetitive work is carried out predictably and with minimal risk
- Interactive controls, are that subset of diagnostic controls that control imposers choose to use as the benchmark for how well the other controls are working in achieving the firm's goals.'

13 Er is derhalve sprake van een subjectieve inschatting door de auteurs. Deze inschatting is eerst door ieder afzonderlijk gemaakt. Vervolgens zijn eventuele verschillen besproken waarbij uiteindelijk consensus bereikt is.

14 Specifiek, meetbaar, acceptabel, realistisch, tijdgebonden.

15 Ook beloningssystemen oefenen hier invloed op uit. Zie bijvoorbeeld Knoops, 2008.

16 Betoogd zou nog kunnen worden dat het beoordelen van de werking van de IB-omgeving door middel van monitoring plaats moet vinden. De in paragraaf 5.3 behandelde problematiek speelt echter dan ook een rol.

17 Wij hebben hier gekozen voor een classificatie als interactive gezien het dialoogkarakter dat deze vraag van COSO heeft.

18 Aangezien zowel beliefs systems als diagnostic systems hier een rol spelen, hebben wij deze vraag in beide categorieën voor de helft mee laten wegen.

19 Aangezien taakbeschrijvingen als norm functioneren, hebben wij deze ingedeeld als diagnostic systems.

20 Deze vraag van COSO bevat zowel diagnostic- als boundary-aspecten. Daarom hebben wij deze in beide categorieën voor de helft meegenomen.