Sarbanes-Oxley wet sectie 404

De top-down, risk-based benadering

Dr. C.M. van Nieuw Amerongen RA[1]

1 Niels van Nieuw Amerongen is senior SOx consultant en adviseert accountantsorganisaties op het gebied van de controlemethodologie en is als partner verbonden aan New Venture, New Advisers bv. Daarnaast is hij part-time onderzoeker en docent Auditing aan de Vrije Universiteit Amsterdam. In 2007 is hij gepromoveerd aan deze universiteit op het onderwerp 'Auditors' Performance in Risk and Control Judgments'. Hij bedankt twee anonieme reviewers voor de feedback op eerdere versies van dit artikel.

1 Inleiding

Naar aanleiding van faillissementen en 'boekhoudschandalen' van grote multinationale ondernemingen (denk aan Enron, WorldCom, Tyco enzovoort) werd de zogenaamde Sarbanes-Oxley wetgeving (verder SOx te noemen) ontworpen. President Bush tekende deze wet op 30 juli 2002, die van toepassing zou worden voor *local filers* vanaf boekjaar 2004, voor *foreign filers* vanaf boekjaar 2006 en voor *non-accelerated filers* vanaf boekjaar 2007 (management report) respectievelijk boekjaar 2008 (auditor's report).[1] De omvang en de consequenties van de boekhoudschandalen voor de financiële markten waren dusdanig, dat het ontwerpen en aanvaarden van de SOx-wet zonder al te veel problemen verliep. Het vertrouwen van investeerders in de Amerikaanse kapitaalmarkt moest worden hersteld. In Nederland kennen we de uitdrukking: 'Vertrouwen komt te voet en gaat te paard'. Ofwel, het kost veel tijd en moeite om vertrouwen te winnen en op te bouwen. Aan de andere kant kan een enkele gebeurtenis het in het verleden moeizaam opgebouwde vertrouwen in één klap doen instorten.

Met de SOx-wet beoogde de Amerikaanse regering een dusdanige daad te stellen dat het vertrouwen van Amerikaanse investeerders in korte tijd herwonnen zou worden. Dit was geen gemakkelijke opdracht, duidelijkheid en daadkracht waren geboden. Aan het persbericht van het Witte Huis bij de inwerkingtreding van de SOx-wet kwam ferme taal te pas. Onoprechte leiders van grote ondernemingen zouden meer risico gaan lopen en zware gevangenisstraffen wachten bij overtreding van de wet. En ook de accountants zouden onderwerp van controle gaan worden en grotere aansprakelijkheidsrisico's gaan lopen. De implementatie van SOx zou natuurlijk wat kosten met zich meebrengen, maar de baten van SOx rechtvaardigden deze extra kosten.

Inmiddels leven we ruim vier jaar na de inwerkingtreding van de SOx-wet en zijn sindsdien vele debatten gevoerd over de 'voors', maar belangrijker nog de 'tegens' van SOx. Wagner en Dittmar (2006) betogen bijvoorbeeld dat de invoering van SOx een belangrijk aantal positieve aspecten met zich heeft meegebracht:

- aanzienlijke versterking van de interne beheersingsomgeving;
- noodzakelijke verbeteringen in de documentatie van de interne beheersingsmaatregelen;
- vergroting van de betrokkenheid van leden van het audit committee, die hun taken serieuzer opvatten dan voorheen;

1 Zie SEC releases 33-8760 en 34-54942, 2006.

– integratie van SOx met andere projecten gericht op het verbeteren van interne beheersing van de gehele organisatie (niet alleen interne beheersing over financiële verslaggeving);
– SOx heeft bijgedragen aan verdere standaardisering/optimalisatie van processen;
– reductie van complexiteit van taken;
– versterking van de grip op uitbestede processen, partnerships en shared service centers;
– het verkleinen van de kans op menselijke fouten.

Het aantal critici van SOx is echter groeiende. Toonaangevende Amerikaanse onderzoekers suggereren dat SOx niet alleen geen oplossing is voor herstel van het geschonden vertrouwen van beleggers – immers, objectief bezien is de 'failure rate' van ondernemingen 'close to zero'; de vérgaande Sox-wetgeving is gericht op enkele uitwassen – maar ook dat SOx 'unintended consequences' zal hebben (DeFond en Francis, 2005). Enkele belangrijke nadelige consequenties van SOx zijn (zie voor een gedetailleerdere uiteenzetting Gupta, 2006):
– de kosten van SOx-implementatie hebben de in 2003 geschatte kosten met een factor 20 overtroffen;
– SOx is nadelig voor de concurrentiepositie van de in Amerika genoteerde ondernemingen, zowel vanuit het oogpunt van de kosten als vanuit het oogpunt van een toenemende bureaucratie waardoor hun slagkracht wordt gehinderd;
– de aantrekkelijkheid van de Amerikaanse kapitaalmarkt is significant verminderd, onder meer door een dalend aantal IPO's (*initial public offerings*) en doordat een groeiend aantal ondernemingen overweegt om zich terug te trekken uit de Amerikaanse kapitaalmarkt.

In aanvulling op de genoemde nadelen werd het in de praktijk als belangrijke leemte ervaren dat voor het management van in Amerika genoteerde ondernemingen geen specifieke SOx-richtlijnen beschikbaar zijn. Dit heeft als gevolg dat het management van deze ondernemingen zich tot op heden vooral heeft gebaseerd op de voor accountants geschreven richtlijnen (Auditing Standard No. 2, PCAOB, 2004). Accountants interpreteren de standaarden vaak te conservatief door het eisen van excessieve documentatie en testwerkzaamheden voor een groot aantal beheersingsmaatregelen, zelfs voor beheersingsmaatregelen in een 'low risk area' (Gupta, 2006, p. 14 en p. 18). Dit zou wel eens ingegeven kunnen zijn door het toegenomen risico van aansprakelijkheid: 'auditors must be held accountable'.

Op 20 december 2006 heeft de SEC een nieuwe conceptinterpretatie gepubliceerd die aan het management van in Amerika genoteerde ondernemingen verdere aanwijzingen geeft voor de implementatie van een 'top-down, risk-based approach', een

benadering waarvan de hoofdlijnen reeds zijn beschreven in een SEC-statement gedateerd 16 mei 2005 (SEC, 2005) en die nu verder zijn uitgewerkt.

In dit artikel zullen de belangrijkste elementen van de genoemde conceptinterpretatie van de SEC worden besproken en kritisch geëvalueerd. De centrale vraag die hierbij wordt gesteld, betreft de vraag in hoeverre het management met deze interpretatie voldoende handvatten heeft om zijn Sox-aanpak te kunnen stroomlijnen. Tegelijk met de SEC conceptrichtlijn heeft de PCAOB een herziene auditing standard (een herziening van AS2) voorgesteld. Deze herziene standaard vormt niet de focus van dit artikel. Wel zal daaraan, waar dit nuttig is, worden gerefereerd.

De conceptinterpretatie kent de volgende onderwerpen die achtereenvolgens zullen worden beschreven:
- evaluatie:
  - het identificeren van risico's en beheersingsmaatregelen met betrekking tot financiële verslaggeving,
  - het evalueren van bewijsmateriaal voor de effectieve werking van interne beheersingsmaatregelen,
  - overwegingen bij multilocatie omgeving;
- rapportering.

2 Bespreking SEC conceptinterpretatie

De methoden en werkzaamheden gericht op het identificeren van verslaggevingsrisico's en het daarop gebaseerde raamwerk van interne beheersingsmaatregelen verschillen van onderneming tot onderneming, afhankelijk van specifieke karakteristieken van de ondernemingen. De conceptinterpretatie vormt geen gedetailleerde uiteenzetting van voorschriften, maar geeft nadere uitwerking aan de zogenaamde 'top-down, risk-based' benadering. De conceptinterpretatie is derhalve niet 'rule-based', maar 'principle-based'.[1] Een dergelijke aanpak is naar verwachting zowel het efficiëntst als het effectiefst.

Het raamwerk van interne beheersing dat ondernemingen hanteren, dient alle beheersingsmaatregelen te beschrijven die relevant zijn voor de beoogde effectieve werking. Dit impliceert dat zowel individuele aandachtsgebieden als meeromvattende (organisatiebrede) gebieden worden beschreven. Tegelijkertijd betekent dit dat niet alle te identificeren beheersingsmaatregelen relevant zijn voor een effectief intern beheersingssysteem voor financiële verslaggeving. Het gaat er vanuit SOx-optiek

1 De voorgestelde nieuwe PCAOB auditing standard is ook gebaseerd op een dergelijke benadering. (PCAOB, 2006, p. 30).

om dat de key controls[1] een redelijke mate van zekerheid bieden dat de financiële verslaggeving een getrouwe weergave van de werkelijkheid is en dat de jaarrekening in overeenstemming is met algemeen aanvaarde grondslagen van financiële verslaggeving.

2.1 Evaluatie

2.1.1 Identificatie van risico's en beheersingsmaatregelen

Beschrijving conceptinterpretatie

De identificatie van verslaggevingsrisico's begint met het vaststellen van de voorschriften ten aanzien van algemeen aanvaarde grondslagen van financiële verslaggeving. De jaarrekening is derhalve het vertrekpunt voor de risicoanalyse. De conceptinterpretatie definieert in dit verband 'financial reporting risks' als risico's op een materiële fout in de jaarrekening (SEC, 2006, p. 31). Risicofactoren kunnen zowel intern (zoals risico's ten aanzien van de initiatie, autorisatie, verwerking en boeking van transacties) als extern (zoals risico's die gerelateerd zijn aan de branche waarin de onderneming werkzaam is) van aard zijn. Het management dient te evalueren in hoeverre de geïdentificeerde *interne beheersingsmaatregelen* de onderkende jaarrekeningrisico's adequaat afdekken. Hierbij neemt het management met name de organisatiebrede beheersingsmaatregelen in ogenschouw omdat deze het meest *'pervasive'* (grotere reikwijdte) van aard zijn. Doorgaans zal de evaluatie in het eerste jaar de meeste inspanning vergen, afhankelijk van de mate waarin een onderneming in het verleden haar jaarrekeningrisico's heeft geëvalueerd. In latere jaren zal deze exercitie slechts een update hoeven te zijn van in voorgaande jaren geïdentificeerde jaarrekeningrisico's.

Het management gebruikt bij het inschatten van relevante jaarrekeningrisico's zijn kennis van de omgeving waarin de onderneming opereert alsmede zijn kennis van de interne organisatie. Elke organisatie is uniek en heeft daardoor haar eigen risicoprofiel (inclusief het profiel van frauderisico's). Hierdoor zal een instrumentarium van interne beheersingsmaatregelen altijd op maat moeten worden gemaakt. Onder andere de grootte, de complexiteit en de organisatiestructuur zijn variabelen die mede bepalend zijn voor de inrichting van het interne beheersingsinstrumentarium. Het gebruikmaken van beschikbare kennis zal bij grotere ondernemingen plaatsvinden op basis van specialisten die de vereiste knowhow hebben. Bij kleinere on-

1 De voorgestelde SEC interpretatie en de concept PCAOB controlestandaard gebruiken als zodanig de term 'key controls' niet. Aangezien de term in de praktijk veel en op eenduidige wijze wordt gebruikt, wordt het toevoegsel 'key' in dit artikel gehanteerd. Deze benaming geeft ook kernachtig aan dat interne beheersingssystemen naast de key controls ook 'redundant controls' kunnen bevatten: aanvullende beheersingsmaatregelen die in een bepaalde mate ook het desbetreffende risico van materiële fouten afdekken.

dernemingen heeft het management zelf veelal deze vereiste kennis.

Voor het bepalen van de toereikendheid van de *key controls* in het afdekken van jaarrekeningrisico's, vormt het management zich een mening omtrent de omvang en de mate van waarschijnlijkheid van een materiële jaarrekeningfout ten gevolge van het desbetreffende jaarrekeningrisico. De conceptinterpretatie geeft als voorbeeld beheersingsmaatregelen die geïmplementeerd zijn als onderdeel van het jaarafsluitingsproces en die een vorm van een organisatiebrede beheersingsmaatregel kan zijn. In een dergelijk geval is het niet altijd nodig om aanvullende beheersingsmaatregelen voor een bepaalde jaarrekeningpost te ontwerpen en te testen. Daarnaast zal het veelal zo zijn dat in geval er sprake is van effectieve algemene IT-gerelateerde beheersingsmaatregelen, de beheersingsmaatregelen verweven in applicaties veelal efficiënter toetsbaar zijn vergeleken met manuele interne beheersingsmaatregelen.

Organisatiebrede beheersingsmaatregelen zijn in een aantal gevallen effectiever en efficiënter vergeleken met beheersingsmaatregelen op transactieniveau. De mate van effectiviteit van organisatiebrede beheersingsmaatregelen neemt echter wel af naarmate de desbetreffende beheersingsmaatregel een indirectere relatie[1] heeft met informatie-elementen van de financiële verslaggeving.

De vorm (papier, elektronisch) en de omvang van de benodigde documentatie zullen ook van onderneming tot onderneming verschillen. De wijze van vastleggen kan ook aanzienlijk verschillen (bijvoorbeeld manuals, processchema's, taakbeschrijvingen en interne memoranda). De focus van de documentatie is van veel groter belang: deze dient te liggen op bewijsmateriaal ten aanzien van opzet, bestaan en werking van de key controls. De conceptinterpretatie geeft aan het management mee om te heroverwegen hoe de bestaande documentatieset aansluit op de key controls.

Samenvattend geeft de conceptinterpretatie de volgende aanwijzingen:
- Breng in het instrumentarium van interne beheersingsmaatregelen een focus aan op key controls en key risks. Voer in navolgende jaren *slechts* een update uit.
- Overweeg omwille van de efficiëntie en de effectiviteit een grotere focus op organisatiebrede beheersingsmaatregelen

1 Voorbeeld van een directe relatie: beheersingsmaatregelen die erop gericht zijn dat het personeel zorgvuldige tellingen en boekingen verricht voor de fysieke voorraadpositie. Deze maatregel raakt direct de bewering 'juistheid' van het informatie-element 'voorraden'.

die een directe relatie met (elementen van) de jaarrekening hebben.
- Overweeg omwille van de efficiëntie een grotere focus in de *control mix* op application controls indien de algemene IT-controls effectief zijn.
- De vorm van de documentatie is niet zozeer belangrijk als wel dat deze documentatie op transparante wijze inzicht biedt in opzet en werking van de key controls.

Reflectie

In de inleiding van dit artikel werd beschreven dat ondernemingen die onder de SOx-wetgeving vallen zich bij de implementatie van SOx hebben gericht op de voor accountants bedoelde standaard Auditing Standard No. 2 (PCAOB, 2004; verder AS2 te noemen) bij gebrek aan richtlijnen voor ondernemingen. De conceptinterpretatie zou deze bestaande leemte moeten ondervangen. Een eerste aspect dat opvalt bij bestudering van de conceptinterpretatie is dat deze ten opzichte van AS2 geen wezenlijk nieuwe informatie bevat. De conceptinterpretatie ligt overigens ook in lijn met AS5. De vraag kan worden gesteld in hoeverre ondernemingen met de conceptinterpretatie worden geholpen. Ik ben enerzijds geneigd deze vraag negatief te beantwoorden. Immers, door als uitgangspunt te kiezen dat een raamwerk voor interne beheersingsmaatregelen per onderneming uniek is, bestaat zeer veel ruimte voor interpretatie door het management van de onderneming. Anderzijds, doordat de conceptinterpretatie aansluit op AS2 en AS5, beschikken ondernemingen en hun externe accountants over min of meer dezelfde uitgangspunten, hetgeen in de praktijk zou kunnen leiden tot minder disputen met de externe accountant. Het eerder aangehaalde onderzoek van Gupta stelt (2006, p. 48): 'What is not clear is whether each stakeholder (management, auditor, board, investor, etc.) shares a common view of what constitutes a risk-based audit and risk-based internal control assessment.' Nu een definitie van risico is gegeven, hebben onderneming en externe accountant een zelfde vertrekpunt.

Gupta wijst er terecht op dat onderneming en externe accountant zich dienen te richten op de aanvaardbaarheid van restrisico's ('residual risks'). Het is dit aspect dat in de praktijk aanzienlijke oordeelsvorming vraagt: oordeelsvorming van de zorgvuldige bestuurder en (professionele) oordeelsvorming van de externe accountant. Duidelijk is dat dit veelal een stevige discussie met zich mee zal brengen, maar dat juist de wederzijdse kruisbestuiving tussen het management en de externe accountant meer licht zal werpen op de materie. In de praktijk is overigens gebleken dat de risicoanalyse (identificatie en weging) in het eerste jaar van SOx-implementatie veelal door interne accountants wordt uitgevoerd in plaats van door het ma-

nagement en dat veelal de interne accountants in hoge mate betrokken zijn bij de besprekingen met de externe accountant (Gupta, 2006, p. 34). De interne accountant heeft in het algemeen – gelet op de genoten vooropleiding – een zelfde begrippenkader als de externe accountant. De betrokkenheid van de interne accountant vermindert weliswaar een belangrijk deel van de mogelijkheid dat onderneming en externe accountant een verschillende perceptie en definitie van risico's hebben, maar brengt ook een belangrijk ander aandachtspunt met zich mee. Namelijk, dat – gegeven het feit dat interne accountants volgens hun beroepsstandaarden zoveel mogelijk intern *onafhankelijk* zijn – in jaar twee van SOx-compliance het eigenaarschap van de activiteit 'risicoanalyse' hoogstwaarschijnlijk meer naar het management zal verschuiven. Om dat te realiseren heeft AS5 voor de externe accountant ook meer ruimte aangebracht om te kunnen steunen op andere medewerkers dan interne accountants.[1] In jaar twee zal de onderneming haar interne beheersingsinstrumentarium tegen het licht houden en verdere focus aanbrengen op basis van een top-down, risk-based aanpak die het management onder de genoemde veronderstelling in dat jaar zal moeten uitvoeren. Resumerend kan worden gesteld dat eenduidigheid van begrippenkader een belangrijk winstpunt is van de conceptinterpretatie. Tevens is in de praktijk nog veel ruimte gelaten voor oordeelsvorming door het geven van een principles-based interpretatie.

Een ander aspect dat opvalt betreft de suggestie dat ondernemingen meer aandacht zouden moeten besteden aan organisatiebrede beheersingsmaatregelen. Dit punt is zeer valide. Tegelijkertijd hebben veel ondernemingen (Gupta, 2006, p. 72) vanwege het ontbreken van nadere interpretaties moeite met het implementeren van het COSO-raamwerk[2], waarvan de organisatiebrede beheersingsmaatregelen onderdeel uitmaken. In zijn onderzoek concludeert Gupta dat slechts een derde van de deelnemers aan zijn onderzoek van mening is dat COSO 1992 in grote mate voldoet aan de 'suitability criteria'.[3] Belangrijk is ook de constatering dat ondernemingen kennelijk onvoldoende

1 Het door de externe accountant steunen op de testwerkzaamheden van 'others' (zijnde, niet-interne accountants) was voor wat betreft de SOx-certificering reeds toegestaan, maar niet voor de jaarrekeningcontrole. AS5 heeft op dit punt de SOx-certificering en de jaarrekeningcontrole geïntegreerd.

2 AS2 suggereert dat COSO een geschikt raamwerk is in het kader van SOx; andere algemeen erkende raamwerken zijn eveneens toegestaan.

3 Gupta (2006, p. 64): 'A suitable framework must: be free from bias; permit reasonably consistent qualitative and quantitative measurements of a company's internal control; be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal control are not omitted; and be relevant to an evaluation of internal control over financial reporting.'

richting wordt aangewezen in het COSO-rapport zodat zij zelf zijn aangewezen op het geven van invulling aan het COSO-raamwerk.

Opvallend en ook zeer valide betreft de suggestie dat IT-aspecten nadrukkelijker aanwezig moeten zijn in de control mix. In de praktijk kunnen hiervoor belangrijke obstakels aanwezig zijn, zoals de aanwezigheid van verouderde IT-systemen die niet zonder significante investeringen kunnen worden aangepast. Daarnaast geldt in de praktijk dat de IT-control documentatie door medewerkers met een verschillende achtergrond wordt samengesteld. In sommige situaties betreft dit medewerkers die uitvoerend actief zijn in de 'business' zelf, maar in andere situaties gebeurt dit ook wel door medewerkers met een louter technische achtergrond. Het denken in termen van risico's met betrekking tot financiële verslaggeving en key controls vindt met name in de laatstgenoemde situatie niet altijd op adequate wijze plaats. Ook de teststrategie met betrekking tot applicatie controls kan aanleiding zijn tot forse verschillen van inzicht in bijvoorbeeld de situatie dat sprake is van ineffectieve algemene IT-controls. Kruisbestuiving met de externe accountant (EDP-auditor) zou hier uitkomst kunnen bieden, alsmede de aanwijzingen die in AS2 hierover worden gegeven. De SEC conceptinterpretatie geeft daarvoor naar mijn mening onvoldoende aanknopingspunten.

2.1.2 *Evaluatie van bewijsmateriaal*

Het bewijsmateriaal dat het management vergaart, dient toegesneden te zijn op zijn inschatting van de risicokarakteristieken van de onderneming ten aanzien van financiële verslaggeving. Het vergaren van bewijsmateriaal kan in hoofdzaak op twee manieren plaatsvinden. In de eerste plaats door directe testprocedures van de key controls en daarnaast via doorlopende monitoringactiviteiten. De aard, timing en omvang van uit te voeren testwerkzaamheden worden bepaald door de uitkomsten van de risicoanalyse die gericht is op materiële fouten in de jaarrekening. Het management dient zowel de kwantitatieve als de kwalitatieve toereikendheid van het bewijsmateriaal te overwegen. Kwalitatieve aspecten zijn bijvoorbeeld de aard van de uitgevoerde evaluatiewerkzaamheden, de periode waaraan het bewijsmateriaal is gerelateerd en – in geval van monitoringactiviteiten – de mate van validering van de uit monitoringactiviteiten voortvloeiende bevindingen.

In algemene zin zal meer (in zowel kwantitatieve als kwalitatieve zin) bewijsmateriaal worden verzameld, naarmate het risico van een materiële jaarrekeningfout hoger is en naarmate het risico van een tekortschietende beheersingsmaatregel hoger is. De kans op een materiële fout zal aanmerkelijk groter zijn indien:

1. meer oordeelsvorming met betrekking tot een informatie-element uit de financiële verslaggeving nodig is;
2. dit informatie-element fraudegevoeliger is;
3. de mate van complexiteit in onderliggende boekhoudkundige verwerking van transacties groter is;
4. van invloed zijnde omgevingsfactoren een hoger risico met zich meebrengen.

De foutgevoeligheid van informatie-elementen wordt mede beïnvloed door de vraag in hoeverre sprake is van aan het informatie-element ten grondslag liggende schattingsprocessen, of sprake is van transacties met verbonden partijen en of sprake is van kritieke grondslagen voor financiële verslaggeving. De omvang van het te vergaren bewijsmateriaal met betrekking tot de effectiviteit van interne beheersingsmaatregelen (op proces- of transactieniveau) is mede afhankelijk van de aard en omvang van het aanwezige bewijsmateriaal met betrekking tot organisatiebrede beheersingsmaatregelen.

Voor wat betreft de methode van het vergaren van bewijsmateriaal is het onderscheid tussen directe testprocedures en doorlopende monitoringactiviteiten ook van belang. Bij kleinere ondernemingen zal het bewijsmateriaal relatief meer focus hebben op doorlopende monitoringactiviteiten, terwijl het bewijsmateriaal bij grotere ondernemingen vaak meer is gericht op directe testwerkzaamheden. Doorlopende monitoringactiviteiten vinden veelal dagelijks plaats en kunnen daarom via de methode van self assessments worden gedocumenteerd. Bij directe testwerkzaamheden zal dat meer afhankelijk zijn van de aard van de control.

Een algemene blauwdruk is niet te geven van de hoeveelheid te verzamelen bewijsmateriaal en de vorm waarin dit bewijsmateriaal dient te worden samengesteld. In het algemeen verdient het wel aanbeveling om de strategie (de testmethoden en testwerkzaamheden) voor het vergaren van bewijsmateriaal goed te documenteren, bijvoorbeeld in de vorm van een alomvattend memorandum en e-mailinstructies aan het personeel. Wanneer het bewijsmateriaal in separate ordners wordt verzameld, vergemakkelijkt dat ook de toezichthoudende taak van audit committees.

Reflectie
Als zodanig bevat de conceptinterpretatie geen elementen die afwijken van bijvoorbeeld AS2. De focus van de conceptinterpretatie op bewijsmateriaal ten aanzien van *risico's*, is wel nadrukkelijk aanwezig. Voor gebieden met een laag risico hoeft minder gedocumenteerd te worden en voor gebieden met een hoger risico dient uitgebreid gedocumenteerd te worden. Voor wat betreft de hoeveelheid documentatie die minimaal aanwe-

zig dient te zijn, worden geen verdere concrete aanwijzingen verstrekt. Dat zal ook van geval tot geval kunnen verschillen. Wat echter wel van belang is, is de vraag óf en zo ja, hoe het management dient te bepalen en te documenteren dat sprake is van een laag dan wel hoog risico. Interessant is ook de vraag welke consequenties een verlaagde mate van documentatie onder de top-down, risk-based aanpak heeft voor de mate waarin de externe accountant zal willen steunen op de door de onderneming uitgevoerde testwerkzaamheden. Immers, de externe accountant kan op basis van AS2 (PCAOB, 2004) het meest steunen op door de onderneming uitgevoerde testwerkzaamheden in gebieden met een laag risico. Als deze risicogebieden nu minimaal zouden worden gedocumenteerd[1], zou dat met zich mee kunnen brengen dat de externe accountant alsnog besluit zelf aanvullende testwerkzaamheden uit te voeren, hetgeen de controlekosten juist zou verhogen in plaats van verlagen. Het antwoord op de gestelde vraag inzake een lagere mate van documentatie laat zich niet in een SEC interpretatie vangen. Toekomstige reviews door SEC en PCAOB op de SOx-aanpak en uitvoering van de onderneming en de externe accountant zullen hierin wellicht meer duidelijkheid verschaffen.

2.1.3 Meerdere locaties

Het merendeel van de in Amerika genoteerde ondernemingen heeft een organisatiestructuur waarbij de activiteiten van de onderneming op meerdere locaties plaatsvinden. Dit onderdeel van de conceptinterpretatie behandelt de samenloop van centraal ontworpen en uitgevoerde beheersingsmaatregelen versus lokale beheersingsmaatregelen. Het management kan bepalen dat het jaarrekeningrisico waaraan lokale beheersingsmaatregelen gekoppeld zijn, laag is. In een dergelijke situatie kan het management van mening zijn dat het bewijsmateriaal dat is verzameld middels doorlopende monitoringactiviteiten en het bewijsmateriaal dat beschikbaar is ten aanzien van centrale beheersingsmaatregelen voldoende zijn. Als op lokaal niveau sprake is van een hogere mate van complexiteit of van een hogere mate van vereiste oordeelsvorming, kan het management bepalen dat meer bewijsmateriaal nodig is over de effectieve werking van lokale beheersingsmaatregelen. Het management dient ('should') in ieder geval te overwegen in hoeverre sprake is van specifieke locatierisico's. Bij locatiespecifieke risico's kan men denken aan risico's ten aanzien van lokale wet- en regelgeving, de lokale bedrijfsomgeving enzovoort. Deze overweging kan niet plaatsvinden op basis van één oordeel omtrent alle beheersingsmaatregelen tegelijkertijd, maar dient te zijn

1 AS5 (PCAOB, 2006) laat hier overigens meer ruimte doordat het begrip 'principal evidence' is komen te vervallen. Tevens is meer ruimte voor de externe accountant gecreëerd in het steunen op testwerkzaamheden van de onderneming met betrekking tot de interne beheersingsomgeving.

toegesneden op de risicokarakteristieken van alle informatie-elementen van de financiële verslaggeving.

Reflectie
Het onderwerp 'meerdere locaties' is belangrijk omdat dit een variabele is die significante invloed heeft op de compliancekosten (zie bijvoorbeeld O'Brien, 2006, p. 28) en omdat de locatiestructuur veelal locatiespecifieke risico's met zich meebrengt die om zorgvuldig ontwerp van zowel lokale als centrale beheersingsmaatregelen vragen. Het is om die reden passend dat de conceptinterpretatie hieraan aandacht besteedt.

Het bespreken van een belangrijk onderwerp betekent echter niet zonder meer dat de bespreking ook concrete handvatten biedt aan het management van ondernemingen om op basis daarvan te komen tot een op risico gebaseerd intern beheersingssysteem. Het is opvallend te noemen dat een zo belangrijk onderwerp zo summier wordt uitgewerkt, zeker wanneer we dat vergelijken met de uitgebreide (kantoorspecifieke) richtlijnen die de grote accountantskantoren hanteren voor het bepalen van de controleaanpak voor ondernemingen met meerdere locaties (zie bijvoorbeeld PricewaterhouseCoopers, 2004). De controle van internationale ondernemingen wordt centraal aangestuurd op basis van controle-instructies aan lokale accountants. De opzet van een intern beheersingssysteem bij internationale ondernemingen heeft ook een primair centraal georganiseerd karakter, aangezien de beoordeling van tekortkomingen in de interne beheersingsmaatregelen uitmondt in één (geconsolideerd) managementrapport. Het is in de praktijk niet eenvoudig om de SOx-scoping bij een multilocatie omgeving goed uit te voeren en te monitoren. Het komt in de praktijk voor dat onder de moedermaatschappij meerdere joint ventures opereren waarop het management van de moedermaatschappij geen overwegende invloed kan uitoefenen. Het geven van interne richtlijnen kan daardoor in de praktijk op problemen stuiten.[1] Ook raakt het onderwerp 'multi-locations' direct de strategie van de onderneming daar waar het gaat om belangrijke acquisities. Het is bekend dat het doorgaans langer dan een half jaar in beslag neemt voordat een nieuw aangekochte onderneming is geïntegreerd met het moederbedrijf. Een dergelijke integratie geldt niet alleen voor bijvoorbeeld de overgang op centrale IT-systemen van het moederbedrijf, maar raakt de gehele bedrijfsvoering inclusief de toepassing van SOx.

1 AS5 (PCAOB, 2006, B17, p. A1-52) geeft overigens wel enige aanwijzingen voor de controle van de zogenaamde 'equity method investments'.

Het is opvallend dat het thema 'coverage'[1] niet wordt beschreven.[2] Het is begrijpelijk dat op dit terrein niet veel aanwijzingen worden gegeven doordat de focus van de conceptinterpretatie wordt gelegd op 'risico's'. De risico's van materiële fouten in de jaarrekening zullen van locatie tot locatie verschillen. De risico-identificatie is een activiteit die het management zelf zal moeten uitvoeren op basis van de beschikbare kennis van de (lokale) onderneming en haar omgevingsfactoren en het is dan ook lastig om meer specifieke aanwijzingen te verstrekken.

Gegeven het belang van methodologisch verantwoorde keuzes in een multilocatieomgeving is het te verwachten dat het management van multinationale ondernemingen aan de SEC meer concrete aanwijzingen zal vragen. Ook in dit geval zal een bespreking met de externe accountant van de mate van centrale beheersingsmaatregelen in verhouding tot lokale beheersingsmaatregelen plaats moeten vinden in een vroegtijdig stadium. Dergelijke besprekingen dragen bij aan uniformiteit van de SOx-aanpak van de gehele onderneming.

2.2 Rapportering

Het management evalueert elke tekortschietende beheersingsmaatregel die onder zijn aandacht wordt gebracht. Materiële tekortkomingen dienen te worden toegelicht in de jaarlijkse SOx-certificatie. Als er meerdere tekortkomingen zijn die elk raakvlakken hebben met hetzelfde informatie-element in de financiële verslaggeving, dient tevens hun gezamenlijke impact te worden geëvalueerd. Deze evaluatie is zowel kwantitatief (inschatting van de impact van de tekortkoming) als kwalitatief (inschatting van de mate van waarschijnlijkheid dat de tekortkoming leidt tot een materiële jaarrekeningfout[3]). Met name de relatie tussen beheersingsmaatregelen onderling dient in ogenschouw te worden genomen, bijvoorbeeld de relatie tussen algemene IT-beheersingsmaatregelen (bijvoorbeeld logische toegangsbeveiliging) en geautomatiseerde beheersingsmaatregelen in applicaties (bijvoorbeeld ingebouwde controles op rekenkundige juistheid) en IT-afhankelijke beheersingsmaatregelen.

Ten aanzien van de inschatting van de impact van tekortkomingen is zowel het saldo van een jaarrekeningpost per jaareinde van belang als het volume van transacties die ten grond-

1 'Coverage' impliceert een bepaalde minimumdekking van een jaarrekeningpost (op geconsolideerd niveau) die wordt verkregen door het aanwijzen van significante processen waarvoor interne beheersingsmaatregelen zijn geïmplementeerd en getest.
2 AS5 (PCAOB, 2006, p. 20) geeft expliciet aan dat de focus wordt verlegd van 'coverage' (zoals opgenomen in AS2 (PCAOB, 2004) naar risico.
3 Gelet op het adjectief 'materiële' bevat de evaluatie tevens de overweging wat een mogelijke tekortkoming betekent voor de gebruiker van de jaarrekening.

slag liggen aan de jaarrekeningpost. In het geval dat de tekortkoming een risico van 'overstatement'[1] behelst, is de impact van de tekortkoming per definitie gemaximeerd tot het bedrag van het balanssaldo of het transactietotaal. In het geval dat de tekortkoming een risico van 'understatement'[2] betreft, dan kan de impact veel groter zijn. In de meeste gevallen zal het waarschijnlijker zijn dat sprake is van een relatief kleine jaarrekeningfout dan van een relatief grote jaarrekeningfout. Het voorbeeld wordt gegeven van een reconciliatie die niet tijdig is uitgezocht. In het voorbeeld zou hoogstwaarschijnlijk wel tijdig een analyse zijn verricht, wanneer sprake was van grote verschillen.

Andere factoren die het management dient te betrekken in de evaluatie betreffen de aanwezigheid van compenserende beheersingsmaatregelen en de mate van detail en zekerheid die zorgvuldige bestuurders nodig zouden hebben om met een redelijke mate van zekerheid te kunnen beweren dat de jaarrekening is opgesteld overeenkomstig algemeen geaccepteerde grondslagen voor financiële verslaggeving.

De volgende indicatoren voor de aanwezigheid van een materiële tekortkoming worden opgesomd:
- Een ineffectieve beheersingsomgeving (bijvoorbeeld gesignaleerde fraude door senior management, niet-tijdig gerepareerde significante tekortkomingen en niet-effectief toezicht door het audit committee).
- Een herziening van een voorheen gepubliceerde jaarrekening die een correctie op een materiële fout bevat.
- Een materiële jaarrekeningfout die door de externe accountant wordt ontdekt en kennelijk niet door het bestaande beheersingsinstrumentarium aan het licht is gekomen.
- Een ineffectieve compliancefunctie. Deze indicator is vooral van belang voor complexe ondernemingen in zwaar gereguleerde bedrijfstakken.

Het management is verplicht materiële tekortkomingen expliciet te benoemen. Het is niet verplicht om reparatiewerkzaamheden te rapporteren die inmiddels in gang zijn gezet. Materiële tekortkomingen zijn lang niet altijd vergelijkbaar met door andere ondernemingen gerapporteerde materiële tekortkomingen. Transparantie naar de financiële markt is van groot belang en het management dient daarom te overwegen om per materiële tekortkoming expliciet toe te lichten wat de onderliggende reden van de tekortkoming is en wat de mogelijke impact van de tekortkoming is. Het is ondernemingen niet toe-

1 Het risico van een 'overstatement' is veelal gekoppeld aan het getrouwheidsaspect 'juistheid'.
2 Het risico van een 'understatement' is veelal gekoppeld aan het getrouwheidsaspect 'volledigheid.

gestaan om in de SOx-rapportering een beperking in de scope op te nemen.

Reflectie
Het onderwerp 'rapportering' is van groot belang aangezien daarin tot uitdrukking komt wat het samenvattende oordeel van het management is omtrent de effectiviteit van het interne beheersingssysteem met betrekking tot de financiële verslaggeving. Wanneer de onderneming materiële tekortkomingen niet op zorgvuldige wijze rapporteert, kan dat de beeldvorming van belanghebbenden bij de ondernemingen ernstig schaden. De aanwijzingen die worden gegeven in de conceptinterpretatie, verschaffen op een relatief hoog abstractieniveau inzicht voor het management van ondernemingen. Met name door het bespreken van indicatoren die aanleiding kunnen zijn voor een materiële tekortkoming, krijgt de aanwijzing meer handen en voeten.

In werkelijkheid is het evalueren van tekortkomingen een ingewikkeld proces waarbij effectiviteit veelal wordt onderverdeeld naar gradatie of aspect van (in)effectiviteit. In dat opzicht is het kort door de bocht wanneer wordt gesteld dat het management elke onder zijn aandacht gebrachte tekortschietende beheersingsmaatregel evalueert. In de praktijk kan sprake zijn van een aanzienlijk aantal tekortkomingen dat onmogelijk door het management op individueel niveau en qua samenhang kan worden geëvalueerd. Ondernemingen gebruiken daarom veelal een filtermechanisme om het geheel van tekortkomingen op verantwoorde wijze onder één noemer te scharen en als zodanig te evalueren. Het zou het management van ondernemingen aanzienlijk helpen wanneer meer aanwijzingen voor dit filterproces zouden worden verstrekt. Een verwijzing naar of een statement inzake de aanvaardbaarheid van het in december 2004 ontwikkelde raamwerk voor het evalueren van tekortkomingen ('A Framework for Evaluating Control Exceptions and Deficiencies', 2004) zou een korte route kunnen zijn voor deze nadere aanwijzingen.

3 Samenvatting en conclusies

Samenvattend kan worden geconcludeerd dat de conceptinterpretatie van de SEC meer eenduidigheid schept over begrippenkaders en in hoofdlijn aansluit op PCAOB controlestandaarden. In die zin is de conceptinterpretatie een goede uitwerking van de eerder uitgebrachte voorstellen voor een meer topdown, risk-based aanpak.

Tegelijkertijd laat de conceptinterpretatie veel ruimte voor on-

dernemingsspecifieke interpretatie en oordeelsvorming en is de conceptinterpretatie veelal op een hoog abstractieniveau uitgewerkt. Dit heeft alles te maken met het oogmerk van de SEC en de PCAOB, namelijk het verschaffen van een principle-based aanwijzing. Nederlandse ondernemingen die in 2007 de top-down, risk-based benadering willen toepassen en die tot op heden een bottom-up benadering hebben gevolgd, zullen in ieder geval veel werk hebben aan het aanpassen van de bestaande SOx-methodologie. Op de langere termijn zal deze risicobenadering evenwel naar verwachting leiden tot lagere compliancekosten.

4 Literatuur

A Framework for Evaluating Control Exceptions and Deficiencies, Version 3, December 2004, ontwikkeld door negen accountantsfirma's en W.F. Messier.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control Integrated Framework*, Jersey City, (NJ) 1992. Zie www.coso.org

DeFond, M.L. en J.R. Francis, Audit Research after Sarbanes-Oxley, *Auditing: A Journal of Practice and Theory*, Vol.24, Supplement, 2005, pp. 5-30.

Emanuels, J., O.C. van Leeuwen en Ph. Wallage, Internal Control volgens Sarbanes Oxley, Overzicht en praktische betekenis, *Maandblad voor Accountancy en Bedrijfseconomie*, jg.79, no. 7/8, juli/augustus 2005, pp. 348-255.

Gupta, P.P.G., Internal Control, *COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices*, Institute of Management Accountants, 2006.

Lander, G.P., *What is Sarbanes-Oxley?* McGraw-Hill, 2004.

Mock, T.J. en A.M. Wright, Are Audit Program Plans Risk-Adjusted? *Auditing: A Journal of Practice and Theory*, Vol.18, No.1, Spring 1999.

Nieuw Amerongen, C.M. van en N.G. de Jager, SOx-404 en steunen op de testwerkzaamheden van de gecontroleerde onderneming, *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, no. 12, december 2005, pp. 601-610.

O'Brien, P., Reducing SOX Section 404 Compliance Costs, A Top-Down, Risk-Based Approach, *The CPA Journal*, July 2006, pp. 26-28.

PricewaterhouseCoopers, *Sarbanes-Oxley Act: Section 404, Practical Guidance for Management*, July 2004, www.pwc.com

Public Company Accounting Oversight Board (PCAOB), Auditing Standard No. 2, *An Audit of Internal Control over Financial Reporting in Conjunction with an Audit of Financial Statements*, 2004. Zie http://www.pcaobus.org/

Public Company Accounting Oversight Board (PCAOB), *Proposed Auditing Standard, An Audit of Internal Control over Financial Reporting that is Integrated with Audit of Financial Statements*, 2006. Zie http://www.pcaobus.org/

Ramos, M., *How to Comply with Sarbanes-Oxley Section 404, Assessing the Effectiveness of Internal Control*, John Wiley & Sons Inc., 2004.

Securities and Exchange Commission, *SEC Staff Statement on Management's Report on Internal Control over Financial Reporting*, May 16 2005.

Securities and Exchange Commission, *SEC Commission Statement on Implementation of Internal Control Reporting Requirements,* May 16 2005.

Securities and Exchange Commission, *Internal Control over Financial Reporting in Exchange Act Periodic Reports of Non-Accelerated Filers and Newly Public Companies*, Release Nos. 33-8760/34-54942, 2006. Zie www.sec.gov

Securities and Exchange Commission, *Management's Report on Internal Control over Financial Reporting,* Release Nos. 33-8762/34-54976, 20 December 2006. Zie www.sec.gov

Smidt-van der Veer, R. en A.E. van der Slik, Nederlandse en Amerikaanse SOXA 404-ervaringen, *Handboek Management Accounting*, A1510, december 2006.

Wagner, S. en L. Dittmar, The Unexpected Benefits of Sarbanes-Oxley, *Harvard Business Review*, April 2006.