'Integrated audit'

Efficiënte combinatie controleren jaarrekening en testen interne beheersingsmaatregelen

Bart van Beurden en Steven Hartjes

SAMENVATTING De ontwikkelingen op het gebied van Corporate Governance, met name de Sarbanes Oxley Act, verlangen niet alleen van de ondernemingsleiding, maar ook van de externe accountant expliciete oordelen over de kwaliteit van de interne controle. Dit oordeel dient te worden gebaseerd op het testen van de werking van de interne controles. De praktijkervaringen van de auteurs bij SOx-projecten bij diverse grote internationale ondernemingen geven aan dat het bepalen van een effectieve teststrategie flink wat stuurmanskunst vereist om de kosten van het voldoen aan de regelgeving binnen aanvaardbare grenzen te houden en tegelijkertijd tot een verantwoord oordeel te komen. In dit artikel worden diverse knelpunten uit de praktijk aan de orde gesteld. Tot besluit wordt ingegaan op de vraag of dergelijke projecten een 'value for money' kunnen opleveren.

1 Inleiding

De schandalen die zich in de afgelopen jaren hebben voorgedaan inzake het publiceren van (al dan niet bewust) onjuiste of zelfs misleidende informatie heeft geleid tot een verscherpte aandacht voor Corporate Governance in het algemeen en meer specifiek tot het expliciet maken van de verantwoordelijkheid van het management voor voldoende interne beheersingsmaat-

regelen in de organisatie. Het management dient hiermee te waarborgen dat zij op de hoogte is van de mate waarin de strategische en operationele doelstellingen van de onderneming worden gerealiseerd; de in- en externe (financiële) rapportages betrouwbaar zijn; en de organisatie zich houdt aan de van toepassing zijnde wetten en regels.

Het meest in het oog springend zijn de vereisten van de Sarbanes Oxley Act uit 2002 (SOx). Met name de Secties 302 en 404 uit deze wet hebben aanleiding gegeven tot grootschalige projecten bij ondernemingen met een beursnotering in de Verenigde Staten. Deze moeten expliciet kunnen aantonen dat zij voldoende interne beheersingsmaatregelen in de organisatie hebben gerealiseerd, met name op het vlak van de externe verslaggeving. Ook in andere landen, zoals het Verenigd Koninkrijk (The combined code of Corporate Governance), Nederland (Corporate Governance Code of Code Tabaksblat), Frankrijk (Loi de Sécurité Financière) en in de vernieuwde Achtste EU Richtlijn is sprake van vergelijkbare ontwikkelingen.

Het unieke element in SOx is dat in aanvulling op de vereisten voor het management expliciete eisen zijn gesteld aan onderzoek en openbare rapportering door de externe accountant. De essentie hiervan is dat de accountant in aanvulling op zijn oordeel over de getrouwheid van de jaarrekening twee aanvullende onderzoeken en mededelingen doet. Eén is gericht op de kwaliteit van het proces dat het management van de onderneming heeft doorlopen om vast te stellen dat het voldoende interne beheersingsmaatregelen heeft gerealiseerd op het vlak van de externe verslaggeving. De ander is gericht op het verkrijgen en openbaar maken van een eigen oordeel over de toereikendheid van deze interne beheersingsmaatregelen. De Public Company Accounting Oversight Board (PCAOB) heeft in Auditing Standard No. 2 uitgebreide regels uitgevaardigd waaraan de externe accountant zich in dit kader dient te houden. In deze

Drs. B.C.J.M. van Beurden is directeur Capital Markets en verbonden aan het Directoraat Vaktechniek van Ernst & Young Accountants. Hij is specialist in Corporate Governance vraagstukken.

Drs. S.J. Hartjes is partner Financial Services bij Ernst & Young Accountants. Zijn specialiteit is procesbeheersing. Hij is coördinator van de SOX 404 werkzaamheden binnen Ernst & Young Nederland.

Dit artikel is geschreven op persoonlijke titel.

regels wordt aangegeven dat de externe accountant wordt geacht een 'integrated audit' uit te voeren. Dit houdt in dat de controlewerkzaamheden van de accountant zo worden ingericht dat zij zowel bijdragen aan de meningsvorming over de kwaliteit van de interne beheersingsmaatregelen op het vlak van de externe verslaggeving als bijdragen aan de meningsvorming over de getrouwheid van de jaarrekening. Hierna gaan wij in op de belangrijkste aspecten van de uitvoering van een integrated audit zoals vereist door SOx.

Eerst schetsen wij in paragraaf 2 de belangrijkste vereisten van SOx 404. Daarna wordt achtereenvolgens ingegaan op het bepalen van de scope van de werkzaamheden (paragraaf 3), het documenteren van processen en interne beheersingsmaatregelen (paragraaf 4), het evalueren van de opzet van de interne beheersingsmaatregelen (paragraaf 5), het toetsen van interne beheersingsmaatregelen (paragraaf 6) en het evalueren van de testresultaten (paragraaf 7). Wij sluiten af met een beschouwing waarin wij aangeven, dat naar onze mening, een SOx 404-project niet alleen kostenverhogend werkt, maar ook waarde toevoegt.

2 Belangrijkste vereisten van SOx 404

Er zijn twee secties in SOx die met name betrekking hebben op de kwaliteit van interne beheersingsmaatregelen op het vlak van de externe verslaggeving, te weten SOx 302 en SOx 404. De hoofdlijnen van deze secties zijn al eerder toegelicht door Emanuels, Wallage en Van Leeuwen (2004). Wij beperken ons daarom tot enkele essentiële elementen van SOx 404.

Sectie 404 heeft betrekking op interne beheersingsmaatregelen met betrekking tot de externe verslaggeving ('internal controls over financial reporting') en kan worden beschouwd als een verdieping van Sectie 302. Waar Sectie 302 zich vooral richt op de rapportagefunctie zelf en het proces voor totstandkoming van publieke informatie, richt Sectie 404 zich op het fundament dat hier noodzakelijkerwijs onder zit in de operationele organisatie: de interne beheersingsmaatregelen die de onderneming heeft gerealiseerd om er voor te zorgen dat alle transacties correct worden geregistreerd in de administratie van de onderneming en vervolgens adequaat worden verzameld en gerapporteerd in het 'Financial Statement Closing Process'. In dit laatste zitten de raakvlakken met Sectie 302. De consequentie van Sectie 404 is dat de reikwijdte van SOx wordt uitgebreid naar de overige functies buiten de financiële functie.

Het gaat echter niet om alle interne beheersingsmaatregelen, maar uitsluitend om de interne beheersingsmaatregelen die een relatie hebben met de externe verslaggeving. Evenals Sectie 302 vereist Sectie 404 dat CEO én CFO jaarlijks een publieke mededeling doen over de kwaliteit van de interne beheersingsmaatregelen van de externe verslaggeving. Voor de grootste ondernemingen in de Verenigde Staten (de zogenaamde 'accelerated filers') is Sectie 404 inmiddels in werking getreden. Voor de 'non-accelerated filers' uit de Verenigde Staten en de 'Foreign Private Issuers' (niet-Amerikaanse ondernemingen met een beursnotering in de Verenigde Staten) is inmiddels wederom uitstel verleend, waardoor de eerste publieke informatie uit hoofde van Sectie 404 voor de meeste ondernemingen wordt verwacht over het boekjaar 2006.

Kern van de verwachte mededeling van CEO én CFO is dat zij voldoende 'interne beheersingsmaatregelen van de externe verslaggeving' hebben gerealiseerd in de onderneming om materiële fouten in de jaarrekening te voorkomen dan wel intern tijdig te ontdekken. Indien de kans dat er materiële fouten in de jaarrekening terechtkomen niet voldoende is gereduceerd (er is dan sprake van een of meer 'material weaknesses'), worden CEO én CFO geacht te concluderen dat zij niet 'in control' zijn en moeten zij gericht aangeven op welke punten de interne beheersing tekort schiet.

Sectie 404 stelt daarenboven eisen aan rapportage door de externe accountant. De externe accountant dient vast te stellen dat het management van de onderneming een goed proces heeft ingericht om tot haar 'in control statement' te komen. Daarnaast dient de externe accountant zich ook zelf een oordeel te vormen over de kwaliteit van de interne beheersing inzake de externe verslaggeving. Naast de verklaring inzake de getrouwheid van de jaarrekening geeft de externe accountant onder Sectie 404 twee aanvullende mededelingen: één over de kwaliteit van de beoordeling door het management en één over de kwaliteit van de interne beheersingsmaatregelen van de externe verslaggeving. In de situatie dat de externe accountant tot het oordeel komt dat het management haar beoordeling onvoldoende heeft uitgevoerd (in accountantstermen: het management heeft geen deugdelijke grondslag voor haar uitspraken), moet de externe accountant een afkeurend oordeel geven over de beoordeling van het management. In die situatie is het niet toegestaan dat de externe accountant het onafhankelijk opgebouwde eigen oordeel alsnog vermeldt.

3 Bepalen van de 'scope' van de werkzaamheden voor de onderneming

Door de regelgevers in de Verenigde Staten wordt het COSO Internal Control Framework (1992) gesuggereerd als referentie voor de toetsing van de interne beheersing. Uit de nadere precisering van de regelgeving valt af te leiden dat van het totale toepassingsgebied van COSO de interne beheersing van strategische, operationele en 'compliance' risico's niet volledig worden afgedekt. De conclusie hierbij is dat SOx een smaller toepassingsgebied kent, maar, zoals uit het vervolg van dit artikel blijkt, daar wel een grote diepgang aan geeft.

Omdat de inrichting van de interne beheersing veelal volgens het COSO-model zal plaatsvinden, zullen veel van de termen en processtappen die hierin voorkomen in het navolgende worden gebruikt.

3.1 'Control Environment', de beheersomgeving, inrichten en evalueren

Voordat met de gerichte acties op de externe verslaggeving wordt begonnen, is een grondige evaluatie van de beheersomgeving voorgeschreven. Hierbij gaat het om de aandacht voor interne beheersing, ethisch gedrag, voorbeeldwerking, het hebben van deskundig en toegewijd personeel et cetera. Dit wordt ook wel aangeduid met het hebben van de juiste 'Tone at the top' zonder welke alle vervolgacties niet succesvol kunnen worden ingezet of na verloop van tijd kunnen verzanden.

3.2 Concretisering van de 'scope'

Veel niet-Amerikaanse ondernemingen die onderworpen zijn aan de vereisten van SOx 404 in verband met een beursnotering in de Verenigde Staten zijn grote multinationals met een vaak complexe organisatie. Het is ondoenlijk en ook niet noodzakelijk om alle interne beheersingsmaatregelen in de gehele organisatie te documenteren en te testen om tot het door SOx 404 vereiste oordeel te komen. Daarom begint ieder SOx 404-project met het afbakenen van de 'scope'. Bij de scope spelen vier factoren een bepalende rol:

- a posten van de jaarrekening;
- b bedrijfsprocessen;
- c bedrijfsonderdelen of entiteiten;
- d inherente risico's.

Ad a. Posten van de jaarrekening

Het vertrekpunt voor het bepalen van de 'scope' is de

jaarrekening zoals deze bij de Securities and Exchange Commission (SEC) wordt gedeponeerd in de 'Form 20-F'. In deze jaarrekening zijn posten van de balans en winst- en verliesrekening opgenomen alsmede relevante aanvullende 'disclosures' (bijvoorbeeld nadere toelichting en niet uit de balans blijken verplichtingen). In eerste instantie bepaalt de organisatie welke jaarrekeningposten significant zijn. Hiervoor wordt meestal een materialiteitsindicator gehanteerd welke wordt afgeleid van de winst voor belastingen. Als alternatief worden wel gehanteerd: balanstotaal, eigen vermogen of omzet.

De posten van de jaarrekening komen voort uit de administratieve vastleggingen binnen bedrijfsprocessen. De interne beheersingsmaatregelen zijn opgenomen binnen deze bedrijfsprocessen. Organisaties leggen de relatie tussen significante posten van de jaarrekening en de bedrijfsprocessen die bepalend zijn voor de totstandkoming van deze posten.

Ad b. Bedrijfsprocessen

Bedrijfsprocessen kunnen alleen worden getest binnen een consistente eenheid. Eenzelfde bedrijfsproces kan in verschillende bedrijfsonderdelen anders zijn ingericht. Soms kan zelfs één bedrijfsproces binnen een bedrijfsonderdeel verschillende implementatievormen hebben (bijvoorbeeld verkopen aan bedrijven naast verkopen aan particulieren). Een analyse van de significante jaarrekeningposten en de verschillende processen die hebben bijgedragen aan de totstandkoming van deze posten geeft een inzicht in de processen die in de scope moeten worden meegenomen om tot een dekkend oordeel te komen over de kwaliteit van de interne beheersingsmaatregelen.

Ad c. Bedrijfsonderdelen of entiteiten

In iedere organisatie zijn grotere bedrijfsonderdelen te onderkennen die voor sommige of zelfs alle posten van de geconsolideerde jaarrekening een substantieel gedeelte afdekken. PCAOB Standard # 2 geeft als regel dat qua testen tussen de 60 en 75% van de significante jaarrekeningposten moet worden afgedekt door individueel relevante bedrijfsonderdelen. Hiermee wordt een 80-20 scenario beoogd: 80% van de dekking wordt verkregen door 20% van de entiteiten. In de praktijk zijn grote verschillen waarneembaar tussen ondernemingen die een beperkt aantal grote bedrijfsonderdelen (waar de 80-20 regel opgaat) hebben en ondernemingen die juist een veelheid van individueel kleinere bedrijfsonderdelen kennen (waardoor meer bedrijfsonderdelen in de scope moeten worden meegenomen om voldoende dekking te verkrijgen).

De bedrijfsonderdelen kunnen in drie hoofdgroepen worden verdeeld (zie ook Diekman, 2005):

- individueel significante bedrijfsonderdelen: nagenoeg alle jaarrekeningposten zijn bij deze bedrijfs- onderdelen relevant qua omvang voor het totaal van de onderneming. Voor deze bedrijfsonderdelen worden (nagenoeg) alle processen in de scope van SOx 404 meegenomen;
- bedrijfsonderdelen met enkele significante posten: slechts enkele van de jaarrekeningposten zijn bij deze bedrijfs- onderdelen relevant, waardoor de scope zich zal beperken tot de processen die bij deze posten horen;
- individueel niet-significante bedrijfsonderdelen, die gezamenlijk wel een belangrijke invloed hebben op sommige jaarrekeningposten: voor deze onderdelen wordt doorgaans volstaan met het testen van de zogenaamde 'entity level controls'.

Deze 'entity level controls' bevatten onder andere ondernemingsbrede programma's zoals fraudepre- ventie, gedragscodes, centraal bepaalde beleidsregels en procedures, autorisaties en functiescheidingen, ge- centraliseerde gegevensverwerking, bewaking van de planning- en controlcyclus, activiteiten van de interne accountantsdienst, self-assessment programma's, be- waken van de realisatie van doelstellingen en moni- toring van financiële resultaten, bijvoorbeeld door middel van een planning & control-cyclus.

Ad d. Inherente risico's

De laatste dimensie die nog een rol speelt bij de 'scope' is het inherente risico. Hiermee wordt de kwalitatieve component in de 'scope' meegenomen. Waar de hier- voor genoemde elementen alle betrekking hebben op de kwantitatieve component (zichtbaar financieel effect) is het doel van de kwalitatieve factoren om die processen te signaleren die bij normaal verloop niet tot relevante financiële effecten leiden, maar in geval van tekort schietende interne beheersing wel degelijk relevante financiële gevolgen kunnen hebben. Fac- toren die bij de kwalitatieve risico-inschattingen een rol spelen zijn: eerder opgedane ervaringen, de ves- tigingsplaats, veel ongebruikelijke transacties, veel in- schattingsprocessen, cultuurbepaalde risico's (corruptie), frequente veranderingen in processen, personeel en systemen en ten slotte de noodzaak van frequente handmatige ingrepen in procedures of systemen.

Een simpel voorbeeld hiervan is het proces derivatenhandel bij banken, waar de impact van individuele transacties zo groot kan zijn dat deze directe gevolgen kunnen hebben voor de onder- neming, zoals de Barings-case ons heeft geleerd.

De uiteindelijke 'scope' voor SOx 404 levert een overzicht op van die bedrijfsprocessen binnen geïden- tificeerde bedrijfs- onderdelen die moeten worden gedocumenteerd en waarvan de relevante interne beheersingsmaatregelen moeten worden geïdentificeerd en getest.

4 Documenteren van processen en interne beheersingsmaatregelen

Bij gebrek aan nadere toelichting van de SEC of van de wetgever hanteren de meeste ondernemingen in onze praktijk de PCAOB Standard # 2 als leidraad voor hun interne documentatievereisten.

In deze op 9 maart 2004 definitief geworden standaard staan de randvoorwaarden van het documenteren van processen en interne beheersingsmaatregelen primair gericht op het mogelijk maken van het afgeven van een verklaring door de externe accountant.

De documentatie kan in twee hoofdgroepen worden verdeeld, die direct met elkaar te maken hebben:

- procesdocumentatie, die inzicht geeft in de trans- actieverwerking van begin tot eind, waarbij de PCAOB Standard # 2 in artikel 42 expliciet de fasen initiatie, autorisatie, registratie, verwerking en rap- portage onderkent;
- documentatie van interne beheersingsmaatregelen, die in de processen zijn opgenomen om er voor te zorgen dat alleen betrouwbare gegevens in de ad- ministratie worden opgenomen, die later worden gebruikt voor het opstellen van de jaarrekening.

Er zijn geen vormvoorschriften gegeven voor de docu- mentatie. In de meeste gevallen wordt de proces- documentatie gerealiseerd door een combinatie van stroomschema's en toelichtende teksten.

De interne beheersingsmaatregelen worden meestal opgenomen in 'control templates', die er voor zorgen dat naast de beschrijving van de interne beheersings- maatregel zelf tevens diverse aanvullende gegevens worden geregistreerd zoals de frequentie waarmee de beheersingsmaatregel wordt uitgevoerd, de verant- woordelijke functie/afdeling, de aard van de beheer- singsmaatregel (handmatig of geautomatiseerd of een mengvorm) en of de beheersingsmaatregel is gericht op voorkomen (preventie) of ontdekken (detectie) van fouten.

De essentie van SOx 404 is dat de scope zich beperkt tot 'interne beheersingsmaatregelen van de externe verslaggeving', oftewel die beheersingsmaatregelen die van belang zijn voor de jaarrekening. Bij de meeste projecten zijn de processen relatief gedetailleerd in

kaart gebracht door projectmedewerkers in samenwerking met de procesverantwoordelijken in het bedrijf. Vergelijkende onderzoeken naar de uitwerking van documentatie geven aan dat naast beheersingsmaatregelen over financiële verslaggeving meestal tevens tal van beheersingsmaatregelen hierin zijn opgenomen die operationeel van belang zijn voor een efficiënt procesverloop. Ervaringen in de Verenigde Staten (Ernst & Young, 2005) geven aan dat ondernemingen daar onder de tijdsdruk van de deadlines in het eerste jaar een groot aantal beheersingsmaatregelen in het testen hebben betrokken. Nagenoeg alle ondernemingen geven aan vanaf het tweede toetsingsjaar het aantal te testen controls flink te reduceren. Dit wordt gerealiseerd door het testen te beperken tot de 'key controls', zijnde die interne beheersingsmaatregelen die voor het management van belang zijn om te waarborgen dat er geen materiële onjuistheden in de jaarrekening worden opgenomen. In onze praktijk hebben wij voorbeelden gezien waar voor een inkoopproces in totaal meer dan honderd interne beheersingsmaatregelen waren onderkend. Vanuit het directe belang voor de jaarrekening kon het aantal relevante beheersingsmaatregelen welke gedocumenteerd en getest moeten worden tot circa vijftientig worden teruggebracht.

Het knelpunt dat zich in de praktijk het meeste voordoet is dat de beschrijvingen van individuele interne beheersingsmaatregelen erg uitgebreid zijn en feitelijk meer het procesverloop voor dat gedeelte weergeven dan de feitelijke beheersing. De elementen die in een goed beschreven beheersingsmaatregel terug moeten komen zijn:

- Welke functionaris heeft de beheersingsmaatregel uitgevoerd?
- Op welk moment/ met welke frequentie wordt de beheersingsmaatregel uitgevoerd?
- Wat houdt de beheersingsmaatregel precies in?
- Hoe wordt de beheersingsmaatregel uitgevoerd en hoe wordt zichtbaar gemaakt dat de beheersingsmaatregel is uitgevoerd?

Met name het duidelijk weergeven van de wijze waarop het functioneren van de beheersingsmaatregel achteraf kan worden vastgesteld, laat in de praktijk vaak te wensen over. Voorts is vaak sprake van 'samengestelde' interne beheersingsmaatregelen, dat wil zeggen dat er één beheersingsmaatregel wordt uitgewerkt, die feitelijk alleen effectief kan functioneren als een aantal stappen wordt doorlopen. Om de effectieve werking van deze beheersingsmaatregel te toetsen moeten verschillende

facetten apart worden belicht. Het verdient aanbeveling om er bij het uitschrijven van de beheersingsmaatregel alvast rekening mee te houden hoe deze beheersingsmaatregel later kan worden getest, zodat wordt voorkomen dat alle beschreven interne beheersingsmaatregelen opnieuw moeten worden bekeken.

De meeste ondernemingen in onze praktijk hebben meerdere versies van procesbeschrijvingen en control templates gemaakt alvorens de beheersingsmaatregelen zodanig waren beschreven dat deze ook effectief konden worden getest.

5 Evalueren van de opzet van de interne beheersingsmaatregelen

Een separate stap in het proces is het vaststellen dat de beschreven interne beheersingsmaatregelen adequaat en effectief zijn in hun opzet. Zodra de interne beheersingsmaatregelen voor een proces in opzet zijn beschreven, moet worden vastgesteld of er voldoende beheersingsmaatregelen zijn ontworpen om het uiteindelijke doel (geen materiële fouten in de jaarrekening) te realiseren. In de praktijk wordt dit aangeduid als 'design effectiveness' van interne beheersingsmaatregelen.

In veel projecten wordt de toetsing van 'design effectiveness' sterk gericht op de kwaliteit van de individuele interne beheersingsmaatregelen. De toetsing houdt in dat wordt geverifieerd of alle relevante elementen in termen van wie, wat, waar, wanneer en hoe in de beschrijving zijn opgenomen. Hiermee kan worden gewaarborgd dat de maatregel in de volgende fase zinvol kan worden getoetst.

Een voorbeeld uit de praktijk: een algemene statement zoals 'er is functiescheiding tussen inkoop, goederenontvangst en factuurbehandeling' kan op zich waar zijn, maar is onvoldoende specifiek hoe dit is gerealiseerd en kan worden waargenomen. Moet de toetser zich richten op het organigram? Is de functiescheiding wellicht vertaald in de toegangsprofielen tot de applicatie die het inkoopproces ondersteunt? Hoewel in eerste aanleg sprake lijkt te zijn van een goede interne controlemaatregel is nadere aanscherping nodig om tot een goede toets te komen.

Nog belangrijker dan het toetsen van een correcte beschrijving van individuele beheersingsmaatregelen is vast te stellen dat het hoger liggende doel, geen materiële fouten in de jaarrekening, wordt bereikt. Dit maakt het noodzakelijk alle beheersingsmaatregelen op te nemen in een heldere evaluatiestructuur.

Wij zijn sterk voorstander van een evaluatiestructuur waarbij iedere interne beheersingsmaatregel wordt gekoppeld aan de jaarrekeningposten en de kenmerken ('assertions', zoals bestaan, volledigheid, juistheid, juiste waardering, juiste presentatie) van deze posten die door deze maatregel worden geraakt. Voor iedere relevante combinatie van posten en kenmerken worden de gerealiseerde (en eventueel niet gerealiseerde) beheersingsmaatregelen in kaart gebracht. In de meeste gevallen zijn er meerdere beheersingsmaatregelen die bij kunnen dragen aan het realiseren van dit doel. De focus moet vooral zijn gericht op de vraag of de gerealiseerde interne beheersingsmaatregelen het doel al bereiken in plaats van de vraag of een mogelijke, maar niet gerealiseerde interne beheersingsmaatregel alsnog zou moeten worden getroffen. Deze wijze van evalueren biedt de mogelijkheid een efficiënte teststrategie in te richten door de meest effectieve interne beheersingsmaatregelen te selecteren.

6 Testen van interne beheersingsmaatregelen

De mededeling van zowel ondernemingsleiding als externe accountant uit hoofde van Sectie 404 van de Sarbanes Oxley Act heeft betrekking op de werking van de interne beheersingsmaatregelen met betrekking tot externe verslaggeving. Van belang hierbij is dat het niet over de werking over een bepaalde periode (bijvoorbeeld het boekjaar) gaat, maar dat de werking moet worden vastgesteld op de balansdatum. Een oordeel over de werking houdt in dat het daadwerkelijk functioneren van interne beheersingsmaatregelen moet worden getest.

In eerste aanleg zijn de meeste organisaties hun interne testwerkzaamheden gaan inrichten op basis van de PCAOB Standard #2. Belangrijke reden hiervoor is meestal om maximaal hergebruik door de externe accountant van intern verrichte werkzaamheden mogelijk te maken (Van Nieuw Amerongen en De Jager, 2005). Het is echter niet voorgeschreven dat voor het interne oordeel met dezelfde intensiteit moet worden getest. Zeker de recente uitingen van SEC en PCAOB van 16 mei 2005 geven aan dat de normen van PCAOB Standard #2 wat soepeler mogen worden toegepast op basis van een professionele risico-inschatting. Deze nadere instructies zijn uitgevaardigd op basis van de ervaringen opgedaan in de Verenigde Staten waaruit bleek dat zowel de projectkosten als de controlekosten explosief zijn gestegen. Het lijkt erop dat er een convergentie ontstaat tussen de meer materieelgeoriënteerde Europese benadering en de

meer formeelgeoriënteerde Amerikaanse benadering. Van groot belang is wel om de overwegingen inzake de aard en omvang van de testwerkzaamheden goed te documenteren, zodat verantwoording wordt afgelegd over de gemaakte keuzes.

Bij het bepalen van de omvang van de testwerkzaamheden wordt vooral onderscheid gemaakt naar de aard van de beheersingsmaatregel (handmatig of geautomatiseerd) en de frequentie van de beheersingsmaatregel (bij hogere, meestal dagelijkse frequentie heeft PCAOB bepaald dat minimaal 25 transacties moeten worden getest).

Bij de aanvang van de testfase realiseren veel ondernemingen zich dat het aantal gedefinieerde interne beheersingsmaatregelen te hoog is, hetgeen zou leiden tot onevenredige kosten voor het jaarlijkse testen. Daarbovenop komen dan nog de kosten voor het herstel en hertesten van niet goed functionerende interne beheersingsmaatregelen. Meestal is dan ook het begin van de testfase een moment van bezinning om tot een uitgebalanceerde set beheersingsmaatregelen te komen. Hierbij is van belang rekening te houden met de toereikendheid van de set van beheersingsmaatregelen zoals hiervoor beschreven in paragraaf 5.

Wat men zich moet realiseren is dat niet iedere gedocumenteerde en relevant geachte interne beheersingsmaatregel zich één op één vertaalt in een test. Het is zeer wel denkbaar dat testgevallen meerdere interne beheersingsmaatregelen afdekken. Een simpel voorbeeld ter illustratie. Beheersingsmaatregelen gaan vaak over verschillende stadia in de levenscyclus van een transactie (bijvoorbeeld een inkooporder of een lening), die in één dossier worden gearchiveerd. Het testen van alle beheersingsmaatregelen waarvan het bewijsmateriaal in dat dossier zit kan op basis van één gecombineerde steekproef worden uitgevoerd. Een ander voorbeeld zijn de toegangsrechten in IT-applicaties, die gecombineerd kunnen worden getest.

Eén van de lastigste testaspecten heeft betrekking op de integratie van informatietechnologie (IT) in de testaanpak. Enerzijds is het voordeel van maatregelen in geautomatiseerde systemen dat de constante werking hiervan zekerder is dan die van een handmatige procedure. De theorie stelt dan ook dat de geautomatiseerde beheersingsmaatregel slechts eenmaal hoeft te worden getest. Daarna beginnen echter de problemen. De randvoorwaarde hierbij is dat de zogenaamde IT 'general controls', die met name be-

trekking hebben op het gecontroleerd doorvoeren van wijzigingen in functionaliteit van IT-applicaties alsmede toegangsrechten, van voldoende kwaliteit zijn. Dit raakt aan een knelpunt in de controleaanpak van de accountant dat al jaren bestaat, namelijk de zichtbare relatie tussen de kwaliteit van IT 'general controls' en hun betekenis voor (geautomatiseerde) controles binnen processen. Als in het algemeen wijzigingen beheerst worden doorgevoerd, is dan daarmee de garantie verkregen dat een specifiek relevante beheersingsmaatregel binnen een applicatie goed functioneert terwijl die applicatie niet in de steekproef van het testen van IT 'general controls' is betrokken? Een ander knelpunt ligt in de keerzijde. In de meeste gevallen worden er leemtes geconstateerd in de IT 'general controls'. Betekent dit nu meteen dat er niet meer kan worden gesteund op de controles in IT-applicaties? Het primaat in de afweging ligt in een gebalanceerde set van beheersingsmaatregelen rond een bedrijfsproces. Idealiter moet het testen van IT 'general controls' worden toegespitst op die interne beheersingsmaatregelen waarvan de werking cruciaal is voor het oordeel en waarover niet op andere wijze voldoende zekerheid kan worden verkregen. Als een proces bestaat uit veel uniforme transacties met een hoge mate van voorspelbaarheid (bijvoorbeeld salarisverwerking of spaargelden) dan zullen over het algemeen de IT 'controls' niet cruciaal zijn om vast te stellen dat er geen materiële fouten in de salarissen of in de spaargelden zitten. Bij meer complexe toepassing (zoals de waardering van financiële producten) ligt dit duidelijk anders.

Een afgewogen aanpak voor het testen van IT 'controls' is derhalve noodzakelijk om enerzijds ongerechtvaardigde verwachtingen te voorkomen en anderzijds niet teveel onnodig testwerk te verrichten.

PCAOB #2 geeft duidelijk aan dat van de externe accountant een 'integrated audit' wordt verwacht. Dit betekent dat de werkzaamheden gericht op het verkrijgen van een oordeel over posten van de jaarrekening en de werkzaamheden gericht op het verkrijgen van een oordeel over de werking van de interne beheersingsmaatregelen zoveel mogelijk gecombineerd moeten worden. Naar Nederlandse maatstaven is dit al in belangrijke mate het geval, zeker voor de grote routinematige processen.

Er zijn twee gebieden die extra aandacht vereisen. Ten eerste zijn dit processen, waarbij de accountant van oordeel is dat een controle direct gericht op de jaarrekeningposten efficiënter is dan het toetsen van interne beheersingsmaatregelen. Dit wordt vaak ge-

hanteerd bij de controle van bijvoorbeeld de materiële vaste activa. In eerste instantie gaf de PCAOB aan dat ook bij deze posten de interne beheersingsmaatregelen moesten worden getoetst. In de recente richtlijnen wordt een meer genuanceerde benadering ook toegestaan.

Een grotere uitdaging zit in de controle van het afsluitproces van de jaarrekening. Bij de meeste ondernemingen is dat een proces dat onder hoge tijdsdruk van publicatiedeadlines wordt uitgevoerd. In de praktijk werkt de accountant schouder aan schouder met de onderneming en is er nauwelijks tijd om te wachten tot een onderneming alle interne beheersingsmaatregelen heeft uitgevoerd om die vervolgens te toetsen. Dit is een proces dat vaak minder goed is gedocumenteerd, zowel qua procesverloop als qua bewijs dat controles hebben plaatsgevonden. Denk hierbij bijvoorbeeld aan het navraag doen bij vreemde ontwikkelingen in de cijfers, die vaak onder tijdsdruk telefonisch of wellicht per e-mail worden afgewerkt. Een effectieve test van dit proces vraagt stuurmanskunst. Een deel van de oplossing kan worden gevonden in het feit dat het afsluitproces van de jaarrekening zeker bij grote ondernemingen allang niet meer een jaarlijks proces is, maar een proces dat grotendeels op maandbasis en wellicht voor sommige posten zoals voorzieningen op kwartaalbasis wordt uitgevoerd. Dit betekent dat de accountant het merendeel van zijn testwerk op andere momenten in het jaar dan tijdens de jaarafsluiting kan uitvoeren. De jaarafsluiting zelf kan dan een mix blijven van postgerichte (substantive) controlemaatregelen en het testen van interne beheersingsmaatregelen.

Naast het testen van de interne beheersingsmaatregelen in de processen (veelal de 'control activities' uit het COSO-model) dient de accountant zich ook een oordeel te vormen over de 'control environment' (de andere vier lagen uit het COSO-model). Gezien de aard van de vraagstelling (onder andere 'code of conduct', functioneren van het Audit Committee, functioneren van de Interne Accountant) is het testen van de 'control environment' niet zonder meer vergelijkbaar met het testen van de beheersingsmaatregelen in de processen. De gehanteerde teststrategieën maken meer gebruik van interviews en het vaststellen dat duidelijke beleidslijnen (Audit Committee Charter, Internal Audit Charter) aanwezig zijn. Voorts wordt hierbij vaak gebruikgemaakt van enquêtes om vast te stellen in welke mate bijvoorbeeld een 'code of conduct' ook in de praktijk wordt nageleefd.

7 Evalueren van de testresultaten

Sectie 404 vereist een expliciet, extern te publiceren oordeel van zowel ondernemingsleiding als externe accountant. Dit betekent dat voor belangrijk geachte interne beheersingsmaatregelen die niet blijken te werken een afweging moet worden gemaakt van het belang hiervan. De twee dimensies die hierbij de hoofdrol spelen zijn waarschijnlijkheid en impact. Bij de impact speelt de materialiteitsvraag een rol. Zou het niet functioneren van een interne beheersingsmaatregel kunnen leiden tot een materiële fout in de jaarrekening? Voor de externe accountant is dat vaak een afweging die wordt gemaakt en wordt gerapporteerd aan de ondernemingsleiding als bevinding bij de controle. De eerlijkheid gebiedt te zeggen dat het merendeel van deze posten geen betrekking heeft op geconstateerde fouten, maar op verschillen van inzicht, bijvoorbeeld over de hoogte van bepaalde voorzieningen. De component waarschijnlijkheid is wellicht nog moeilijker in te schatten. Een niet functionerende interne beheersingsmaatregel betekent niet dat er meteen fouten ontstaan. In de praktijk wordt daarom een schaal gehanteerd van onwaarschijnlijk via mogelijk tot bijna zeker. De combinatie van de factoren impact en waarschijnlijkheid zal leiden tot een overzicht van mogelijke fouten in de jaarrekening die kunnen duiden op een ontoereikende interne beheersingsmaatregel.

In de uitwerking zijn er twee belangrijke gradaties. Als er wel fouten kunnen ontstaan door ontoereikende interne beheersingsmaatregelen, maar deze kwalificeren niet als materieel voor het beeld van de jaarrekening, dan is er sprake van een 'significant deficiency'. Deze moeten worden gemeld aan ondernemingsleiding en Raad van Commissarissen/Audit Committee. Als er sprake van is dat de tekortschietende interne beheersingsmaatregelen kunnen leiden of zelfs hebben geleid tot materiële fouten in de jaarrekening dan is er sprake van een 'material weakness'. Een 'material weakness' kan ontstaan als de impact van een mogelijke fout relatief hoog is en de kans dat zich deze voordoet als gevolg van een niet functionerende beheersingsmaatregel aannemelijk is. De consequentie van de material weakness is dat de ondernemingsleiding en externe accountant moeten concluderen dat de interne beheersingsmaatregelen ontoereikend zijn en dit toelichten in de 404 statement. Dit heeft dus externe consequenties, die wellicht de status van de onderneming in de publieke opinie in gevaar kunnen brengen. Van belang is verder dat indien de onderneming meent dat er geen

'material weakness' gemeld hoeft te worden maar de externe accountant vindt dat deze wel aanwezig zijn, de laatste dit extern moet melden.

De beoordeling of een tekortkoming materieel is, is een inschattingsproces waarbij de PCAOB #2 dankbaar gebruik maakt van begrippen uit US GAAP. Bij de inschatting gaat het om het wegen van de kans (likelihood) dat de fout kan optreden en de omvang (magnitude) die de fout op de jaarrekening kan hebben. De grote accountantskantoren in de Verenigde Staten hebben een gezamenlijk document uitgebracht dat als leidraad wordt gehanteerd voor het evaluatieproces (Group of 9 large audit firms, 2004).

Naast de moeilijke afweging rond het trekken van grenzen tussen significant en materieel is een praktijkprobleem bij grote ondernemingen om het internationale bouwwerk zodanig te maken dat een verantwoorde afweging mogelijk is. Hierbij kan een regel uit het rekenen worden gehanteerd: afrondingen moeten zo laat mogelijk in het proces worden gemaakt om tot een goede uitkomst te komen. Dit wil zeggen dat niet iedere zelfstandige entiteit tot een eigen eindoordeel moet komen met achterwege laten van het rapporteren van mogelijke tekortkomingen, maar dat alle tekortkomingen boven bepaalde minimumgrenzen op centraal niveau moeten worden afgewogen. Hiermee wordt gewaarborgd dat individueel kleine fouten, die toevallig op dezelfde post van de jaarrekening betrekking hebben, niet worden veronachtzaamd.

8 Alleen kostenverhogend of ook waarde toevoegend?

Het overheersende gevoel is dat een SOx 404-project zeer veel tijd en geld kost. Het is moeilijk aan te tonen dat er ook waarde aan kan worden ontleend. De onderzoeken van Ernst & Young in de Verenigde Staten tonen aan dat bijna de helft van de onderzochte ondernemingen daadwerkelijke voordelen heeft gerealiseerd door hun 404-project. Waar zitten de mogelijke elementen van waarde? Allereerst zit dit in het expliciet maken van interne beheersingsmaatregelen rondom de externe verslaggeving, waar in de praktijk door de managementlagen veel impliciet werd aangenomen. Het opleveren van een beknopte beschrijving van de meest relevante processen van de organisatie helpt de managers om een goed beeld te krijgen van de mate van beheersing in hun processen/afdelingen. Hetzelfde inzicht helpt ook om mogelijke verbeteringen in processen door te voeren, zowel in

termen van efficiency (achterwege laten van overbodige handelingen) als in verhoging van kwaliteit (bijvoorbeeld door het vroegtijdig signaleren van ontwikkelingen en tijdige oplossing van issues, die anders in het gedrang komen van rapportage-deadlines).

Het grote bezwaar tegen SOx blijft het beperkte toepassingsgebied van interne beheersing, namelijk de externe verslaggeving, in combinatie met de enorme diepgang die daarbij moet worden betracht. Voor corporate governance-doeleinden is goed risicomanagement en interne beheersing op de andere gebieden (strategie, operationeel en voldoen aan wet- en regelgeving) essentieel. Ondernemingen die een begin hebben gemaakt met SOx kunnen wel gebruikmaken van de mechanismen en de opgedane ervaringen op het gebied van project management en op die wijze komen tot een integrale aanpak van risicomanagement en interne beheersing.

Om de vruchten te plukken van de initiële inspanningen moeten ondernemingen er voor zorgen dat de uitkomsten van de analyse worden verwerkt in de routinematige activiteiten van de lijnafdelingen en niet zonder meer terugvallen naar het oprichten van aparte interne controleafdelingen die meer kosten dan waarde toevoegen. Hoewel het moeilijk is aan te tonen, verwachten wij dat er zeker ondernemingen zijn die op deze wijze baat hebben bij een SOx 404-traject.

Voor de meeste Nederlandse ondernemingen en hun accountants is er nog een hoop werk aan de winkel en zullen er zeker nog de nodige discussies moeten plaatsvinden om tot een verantwoorde uitkomst te komen. Het optimaal integreren van het testen van de interne beheersingsmaatregelen in de uitvoering van de jaarrekeningcontrole leidt tot een efficiënt auditproces, zeker waar de selectie van relevante interne controlemaatregelen ook directe zekerheid geeft over de cijfers. Dit doel kan het best worden gerealiseerd door de evaluatie van de interne beheersingsmaatregelen te koppelen aan het oordeel per jaarrekeningpost en de kenmerken (assertions) bij deze post. ■

Literatuur

- Cadbury Code, (1992), *Report of the Committee on the Financial Aspects of Corporate Governance*, Burgess Science Press, London.
- Commissie Corporate Governance, (2003), *De Nederlandse Corporate Governance Code – Beginselen van deugdelijk ondernemingsbestuur en best practice bepalingen*, 9 december.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), (1992), *Internal Control Integrated Framework*, Jersey City, NJ.

Diekman, P.A.M., (2005), Rapporteren over interne controle. Sarbanes Oxley, section 404 en de rol van de interne accountant, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, no. 10, oktober, pp. 512-521.

Emanuel, J., O.C. van Leeuwen en Ph.Wallage, (2004), Internal Control volgens Sarbanes Oxley, Overzicht en praktische betekenis, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 78, no. 7/8, juli/augustus, pp 348-355.

Ernst & Young, (2005), *Emerging trends in internal controls, US-listed Foreign Private Issuers, Initial Survey*; www.ey.com, onder 'internal control reporting library'.

Ernst & Young (2005), *Emerging trends in internal controls, 4th Survey*; zie: www.ey.com, onder 'internal control reporting library'.

Group of 9 large audit firms (o.a. KPMG, PWC, Ernst & Young and Deloitte & Touche), (2004), *A framework for Evaluating Control Exceptions and Deficiencies*, version 3.

Nieuw Amerongen, C.M. van en N.G. de Jager, (2005), SOX-404 en steunen op de testwerkzaamheden van de gecontroleerde onderneming, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, no. 12, december, pp. 601- 611.

Public Company Accounting Oversight Board (PCAOB), (2004), *Auditing Standard 2 – An Audit of Internal Control over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*, March 9, zie: www.pcaobus.org.

Public Company Accounting Oversight Board (PCAOB), (2005), *Policy statement regarding implementation of Auditing Standard 2, An Audit of Internal Control over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*, May 16, zie: www.pcaobus.org.