Toepassing van de monitoring-component van het COSO-raamwerk

Betere interne beheersing voor organisaties én belangrijke innovatie in het accountantsberoep

Cees Klumper

SAMENVATTING In dit artikel wordt aangegeven hoe toepassing van de nieuwe COSO-richtlijnen met betrekking tot de monitoringcomponent van interne beheersing tot belangrijke structurele verbeteringen in de efficiëntie en effectiviteit kan leiden. Dit is relevant voor organisaties zelf en tevens voor hun interne en externe accountants. Door monitoringactiviteiten te onderscheiden van de overige interne beheersingsmaatregelen en ze vervolgens te evalueren en te verbeteren kan de beheersing van risico's effectiever en efficiënter worden gemaakt en kan ook de *assurance* die daarover gewenst is effectiever en efficiënter worden verkregen. Aan de hand van de ervaringen bij de invoering van processen om te voldoen aan de bepalingen van de Amerikaanse Sarbanes-Oxley wetgeving, paragraaf 404, wordt dit geïllustreerd.

RELEVANTIE VOOR DE PRAKTIJK Monitoring heeft tot nu toe in veel organisaties onvoldoende aandacht gehad, met als gevolg dat interne beheersing én de benodigde assurance daarover, niet zo effectief en efficiënt zijn als zou kunnen; hier is veel winst te behalen. Dit is relevant voor iedereen die zich met interne beheersing bezighoudt, zoals managers, interne en externe auditors, *risk managers* en *compliance officers*.

1 Inleiding

De Committee of Sponsoring Organizations of the Treadway Commission (COSO)[1] houdt zich sinds haar oprichting in 1985 bezig met het ontwikkelen en wereldwijd verspreiden van *frameworks* en richtlijnen voor ondernemingen om hun operaties effectiever, efficiënter en ethischer te maken. De commissie doet dit volgens haar website aan de hand van onderzoek, analyse en *best practices*. Al sinds 1992 moedigt COSO organisaties aan om hun interne beheersing volgens het door haar gepubliceerde raamwerk in te richten. Ondernemingen die aan de Amerikaanse Sarbanes-Oxley wetgeving[2] moeten voldoen, moeten in hun jaarverslag melding maken van welk framework zij hanteren voor hun interne beheersing. In bijna alle gevallen blijkt dit COSO te zijn. Ook in de Nederlandse praktijk[3] wordt COSO veel toegepast voor risicomanagement en interne beheersing.

Recentelijk[4] heeft COSO daar een schepje bovenop gedaan door met betrekking tot de monitoringcomponent met aanvullende richtlijnen te komen. COSO's reden om met deze aanvullende richtlijnen te komen was de constatering dat, volgens COSO, monitoring nog onvoldoende wordt begrepen en toegepast:
'COSO initiated this project based on observations that many organizations were not fully utilizing the monitoring component of internal control. This fact became most clear as COSO witnessed the efforts of many companies to meet certain internal control assertion requirements around the world.'[5]

'Met name de worsteling die veel ondernemingen hebben gehad om aan de bepalingen van de Sarbanes-Oxley Act van 2002 te voldoen, en dan met name Section 404, die onder andere van het management een uitspraak vraagt of de *internal control over financial reporting* effectief was per jaareinde, hebben COSO aan het denken gezet. Sinds de start van de implementatie van SOX-404 *compliance*-processen wordt er met name door ondernemingen veel geklaagd over de kosten van deze processen, die volgens hen vaak niet in verhouding staan tot de baten. Dit wordt ook onderkend door de regelgevers, waaronder de U.S. Securities en Exchange Commission (SEC, 2007) en de U.S. Public Company Accounting Oversight Board (PCAOB, 2007b). Een belangrijke oorzaak van die ongunstige kosten-batenverhouding is dat veel ondernemingen redundante testwerkzaamheden uitvoeren in plaats van te steunen op de in de processen veelal reeds aanwezige monitoringactiviteiten.

De voordelen van het wél in de praktijk toepassen van de principes, zoals aangemoedigd door COSO (2008), zijn groot. Feitelijk vervult COSO (2008) een *missing link* in het denken en handelen met betrekking tot interne beheersing. Zonder deze *missing link* is het niet goed mogelijk om op de meest efficiënte wijze:

- externe accountantscontroles uit te voeren;
- SAS 70-trajecten[6] uit te voeren;

- SOX-404 beoordelingen te doen, zowel door het management als door de controlerende accountant;
- de internal audit functie uit te voeren;
- 'in control' statements af te geven.

In het vervolg van dit artikel zal ik aantonen hoe interne beheersing beter kan door toepassing van de nieuwe COSO-richtlijnen (2008). Dit illustreer ik aan de hand van het doorsnee SOX-404-compliance-proces. In paragraaf 2 ga ik in op SOX-404 en geef ik aan hoe de kosten om aan deze bepaling te voldoen substantieel verlaagd kunnen worden. In paragraaf 3 behandel ik het fundamentele onderscheid tussen monitoringactiviteiten en controls. Er kan gebruik worden gemaakt van de binnen processen reeds aanwezige monitoringactiviteiten, wat wordt aangeduid met 'embedded testing' en wordt besproken in paragraaf 4. In paragraaf 5 behandel ik de toepassing van *embedded testing* op andere terreinen van interne beheersing en in paragraaf 6 beantwoord ik de vraag wat embedded testing betekent voor de werkzaamheden van de externe accountant. Ik sluit af met enkele conclusies in paragraaf 7.

2 SOX-404: een revolutionaire testbenadering

Toen ondernemingen en hun accountants zich bogen over de wijze waarop de bepalingen van Section 404 van de Sarbanes-Oxley Act moesten worden geïmplementeerd, schrok men doorgaans van de omvang van de werkzaamheden die dit met zich meebracht. En niet alleen de kosten van de implementatie waren onverwacht hoog, ook de kosten van de ieder jaar terugkerende noodzakelijke *compliance* gaven (en geven nog steeds) aanleiding tot veel discussie en klachten (zie o.a. Van Leeuwen, 2005).

Eén van de grootste kostenposten vormt hierbij het vaststellen dat de voor de *internal control* over financial reporting als relevant geïdentificeerde beheersmaatregelen al dan niet effectief hebben gewerkt (het zogenaamde *managementtesten* door de organisatie zelf); die kosten kunnen tot 50 procent of zelfs meer van de totale SOX-404-compliance-kosten bedragen, zo is in de praktijk gebleken (met enige regelmaat worden er *benchmarks* gepubliceerd door de 'Big 4' en anderen die inzicht geven in de kosten). Reden voor veel ondernemingen om het aantal van de belangrijkste van deze beheersmaatregelen (de zogenaamde *key controls*) dan maar zo klein mogelijk te maken, teneinde zodoende op deze testkosten te kunnen besparen (zie o.a. Van Beurden en Hartjes, 2006). Daarmee wordt echter het zicht op de interne beheersingsmaatregelen die een rol spelen met betrekking tot de financiële verslaggeving wel navenant minder.

De vraag is of er een andere manier is om de kosten substantieel te verlagen, maar dan zonder dat het zicht op de afdekking van de risico's minder wordt. Die manier blijkt er te zijn: steunen op de monitoringcomponent van interne beheersing (zie paragraaf 3), zoals COSO sinds 1992 aanbeveelt en in de meest recente *guidance* (COSO, 2008) inzake monitoring krachtig herhaalt.

Aangezien bijna alle ondernemingen die SOX-plichtig zijn aangeven het COSO-framework voor interne beheersing te hanteren, rijst de vraag waarom dit steunen op monitoring niet al gebeurt (het maakt bijvoorbeeld geen onderdeel uit van de standaardbenaderingen die door de 'Big 4' en vergelijkbare organisaties aan ondernemingen geadviseerd worden).[7] Daar ga ik in paragraaf 4 verder op in.

3 Een fundamenteel onderscheid tussen monitoring activiteiten en controls

Interne beheersingsmaatregelen zijn er in verschillende soorten. Er zijn bijvoorbeeld detectieve en preventieve *controls*, handmatige en geautomatiseerde, en *entity-level* en *process-level controls*. Maar er is ook nog het onderscheid tussen monitoring-controls en overige controls. Liever praat ik zelf trouwens over monitoringactiviteiten en controls om aan te geven dat het om activiteiten gaat die wezenlijk van elkaar verschillen. Namelijk, waar 'gewone' controls ten doel hebben om fouten in processen, financiële verantwoordingen of wat ook maar de controledoelstelling is te voorkomen of tenminste te detecteren, hebben monitoringactiviteiten ten doel om vast te stellen of de onderliggende controls die zij monitoren naar behoren werken, hetgeen iets fundamenteel anders is. Dit laatste, vaststellen of controls naar behoren werken, is precies de doelstelling van het SOX-404-managementtesten dat in de praktijk tot zulke hoge kosten leidt. Het is dan ook mogelijk om deze monitoringactiviteiten, mits adequaat uitgevoerd en gedocumenteerd, als onderdeel van het testen te beschouwen (embedded testing) dat het management moet (laten) uitvoeren om aan het einde van het jaar een onderbouwd oordeel uit te kunnen spreken over de effectiviteit van de *internal control over financial reporting*. Dit kan in de praktijk besparingen opleveren tot wel 90 procent van de testinspanningen die momenteel nog worden uitgevoerd in het kader van SOX-404. In de meeste organisaties worden monitoringactiviteiten namelijk al sinds jaar en dag uitgevoerd als normaal onderdeel van de managementcyclus (het is de '*check*' in de *plan-do-check-act*-cyclus). Feitelijk is het meeste managementtestwerk dat momenteel in het kader van de jaarlijkse SOX-404-attestatie nog wordt gedaan door de meeste organisaties dan ook overbodig en het kan zelfs contraproductief werken. Dat ondernemingen dit zelf ook vinden, blijkt onder andere uit het feit dat ondernemingen die van de Amerikaanse beurs afgaan, in de regel het managementtesten vrijwel direct (nagenoeg) geheel afschaffen omdat ze er te weinig toegevoegde waarde van ervaren. Of ze vervangen het door embedded testing.

4 Embedded testing

Embedded testing is een term die door de auteur van dit artikel in 2005 is bedacht om aan te geven hoe gebruik kan worden gemaakt van de binnen processen vaak reeds aanwezige (*embedded*) monitoring (*testing*) activiteiten teneinde de aanvullend uit te voeren testwerkzaamheden tot een minimum te kunnen beperken (zie b.v. Klumper en Geuzebroek, 2007 en KPMG, 2006[8]).

Enkele definities:

Managementtesten: het vaststellen *door de organisatie zelf* dat de voor de internal control over financial reporting als relevant geïdentificeerde beheersmaatregelen al dan niet effectief hebben gewerkt.

Controls: deze hebben ten doel om fouten in processen, financiële verantwoordingen of wat ook maar de controledoelstelling is, te voorkomen of ten minste te detecteren.

Monitoringactiviteiten: deze hebben ten doel om vast te stellen of de onderliggende controls die zij monitoren, naar behoren werken. Monitoringactiviteiten, mits adequaat uitgevoerd en gedocumenteerd, kunnen als onderdeel van het managementtesten worden beschouwd.

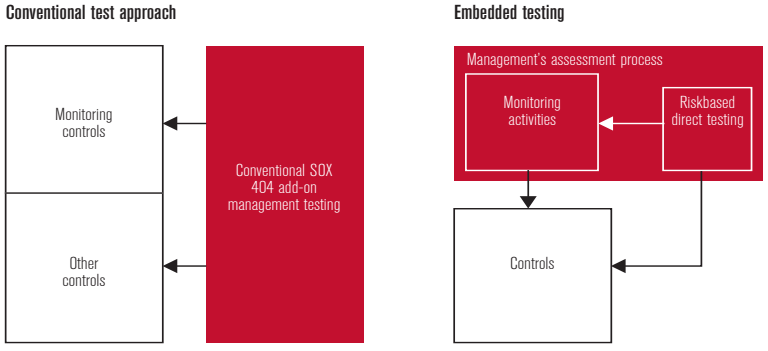
Embedded testing: gebruikmaken van de binnen processen vaak reeds aanwezige (embedded) monitoring (testing) activiteiten teneinde de aanvullend uit te voeren testwerkzaamheden tot een minimum te beperken.

Baselining: het expliciet maken en evalueren van de *on-going* monitoringactiviteiten, zodat men weet in hoeverre de on-going monitoringactiviteiten adequaat zijn ingericht en worden uitgevoerd.

4.1 Embedded testing: een voorbeeld

Om duidelijk te maken wat embedded testing is, gaan we terug naar de manier waarop de meeste ondernemingen SOX-404 hebben geïmplementeerd. Deze manier is in eerdere nummers van het MAB uitgebreid beschreven (Emanuels, Van Leeuwen en Wallage, 2004; Van Leeuwen, 2005; Van Nieuw Amerongen en De Jager, 2006; Diekman, 2005). Het komt erop neer dat in één van de implementatiefases de belangrijkste key controls worden gedocumenteerd en dat ze vervolgens, na op toereikendheid in opzet te zijn beoordeeld, op hun praktische werking worden getest door onafhankelijke testers, zoals bijvoorbeeld internal auditors. Neem het voorbeeld van de reconciliatie van een grootboekrekening die eens per maand door persoon A wordt opgesteld. Vervolgens voert afdelingshoofd B er een beoordeling op uit. Niet zelden zijn deze twee beheersingsmaatregelen beide als *key control* aangemerkt. Vervolgens is er in de standaard SOX-404 benadering een tweetal *tests of operating effectiveness* op uitgevoerd, vaak door internal auditors of door voor deze gelegenheid ingehuurde externe krachten: één op het maken van de reconciliatie en één op de door het afdelingshoofd uitgevoerde review. Nu is er op zich weinig mis met het driemaal testen van dezelfde control (het afdelingshoofd, die de reconciliatie-control doorlopend, in de normale procesgang, test, de internal auditor of extern ingehuurde kracht die dat nogmaals doet als hij of zij de reconciliatie-control test, en vervolgens de internal auditor of extern ingehuurde kracht, die de review control test, vaak middels *reperformance* zodat de reconciliatiecontrol wederom wordt bekeken). De vraag dringt zich echter op of éénmaal niet al voldoende zou zijn. Ook al omdat vervolgens de externe accountant langs komt (die zelfstandig het nodige bewijsmateriaal over de werking van de belangrijkste controls moet verzamelen) om vervolgens de werking van de bewuste reconciliatie-control een vierde en vijfde keer vast te stellen. Vijf tests van dezelfde control dus; geen wonder dat er klachten zijn over de efficiëntie van het SOX-proces en geen wonder dat gedeliste ondernemingen daarmee stoppen zodra ze hun kans schoon zien. Maar ook over de effectiviteit van dit proces zijn twijfels: doordat er zoveel tijd en energie wordt gestoken in het zo vaak vaststellen van de werking van een zo beperkt mogelijk aantal key controls, blijft er wellicht niet genoeg aandacht over voor sommige belangrijke risico's, zoals die van (senior) managementfraude, waar SOX wel door is ontstaan.

Figuur 1 Conventional test approach versus embedded testing



4.2 Conventional test approach versus embedded testing

In 2005 heeft de auteur van dit artikel in zijn functie als Vice President Internal Control van Ahold geconstateerd dat er aldus een grote hoeveelheid testwerk drie- of zelfs vierdubbel werd gedaan. Dat moest stoppen. Dat vond ook de Securities and Exchange Commission (SEC), want in de in de zomer van 2007 gepubliceerde *Interpretive Guidance for Management* wordt uitgebreid stilgestaan bij de mogelijkheden die het management heeft om optimaal gebruik te maken van de in de processen aanwezige, zogenaamde ongoing monitoringactiviteiten, zodat de eventueel nog noodzakelijk geachte *direct testing*-inspanningen (het conventionele SOX-managementtesten) zoveel mogelijk beperkt kan blijven, hiertoe overigens mede aangezet door een *comment letter* op de *concept-guidance* (Klumper en Shepherd, 2007b) en een hierover door Klumper en Shepherd gevoerd gesprek met de SEC in Washington in 2007.[9] Zie figuur 1.

Eén en ander betekent dus dat SOX-compliant ondernemingen, anders dan overigens eerder bepleit door Van Nieuw Amerongen en De Jager (2006)[10] in hoge mate kunnen steunen op de on-going monitoringactiviteiten die binnen processen doorlopend uitgevoerd worden. Dit is groot nieuws voor ondernemingen en voor hun externe accountants die tot nu toe van die mogelijkheid zelden op de hoogte zijn en er derhalve ook geen gebruik van maken. Nu is het helemaal niet zo vreemd dat de SEC zo duidelijk in de Interpretive Guidance for Management heeft aangegeven dat ondernemingen gebruik kunnen maken van ongoing monitoring. De SEC heeft namelijk eerder al ondernemingen verwezen naar het interne beheersingsraamwerk zoals dat door COSO is gepubliceerd, en daar wordt, al sinds de oorspronkelijke publicatie in 1992 (COSO 1992), vastgesteld dat on-going monitoring voor organisaties een uitstekende manier is om zekerheid te verkrijgen over de werking van belangrijke beheersingsmaatregelen: zoals al opgemerkt het doel van managementtesten. Wat wel bevreemdt en daarom nadere studie verdient, is dat er ondanks deze twee gezaghebbende publicaties en de te behalen efficiëncy- en effectiviteitswinsten, nog steeds maar heel weinig organisaties gebruikmaken van deze mogelijkheid. Waarmee we terug zijn bij hetgeen in de inleiding op dit artikel is aangehaald over de reden waarom COSO nu, in 2008, is gekomen met aanvullende *guidance,* specifiek over de monitoringcomponent van het COSO-raamwerk. Monitoring wordt volgens COSO onvoldoende begrepen en toegepast. Het feit dat ondernemingen tot op de dag van vandaag, teneinde aan SOX-404 te voldoen, doorgaan met het niet gebruikmaken van het COSO-framework, terwijl ze dat niet zelden tot wel 50 procent aan kostenbesparingen zou kunnen opleveren, illustreert deze constatering van COSO op wel heel indringende wijze.

5 Toepassing van embedded testing op andere terreinen van interne beheersing

Volgens COSO zijn er twee manieren om monitoring in te richten: *on-going* en *separate evaluations* waarbij de *separate evaluations* primair ten doel hebben om vast te stellen of de on-going monitoring nog steeds adequaat functioneert. Daarbij geldt dat de kwaliteit van de on-going monitoring omgekeerd evenredig is aan de mate waarin separate evaluations moeten worden uitgevoerd om in totaliteit de vereiste assurance te verkrijgen over de werking van de beheersmaatregelen. Oftewel, hoe robuuster de on-going monitoring, hoe minder de noodzaak om separate evaluations uit te voeren: communicerende vaten dus, tot op zekere hoogte.

Het is dus noodzakelijk om vast te stellen hoe robuust de on-going monitoring is, alvorens het juiste niveau van de separate evaluations kan worden bepaald. Zoals COSO heeft geconstateerd wordt het monitoringconcept nog onvoldoende begrepen en toegepast. Dit uit zich onder andere in het feit dat maar weinig organisaties het onderscheid hebben gemaakt tussen hun monitoringactiviteiten en overige controls. Dat heeft dan onder andere als consequentie dat ze niet goed in staat zijn om te bepalen in welke mate er separate evaluations, bijvoorbeeld door hun internal audit-afdeling, dienen plaats te vinden. En dat ze (mede daardoor) niet weten in hoeverre de on-going monitoring adequaat wordt uitgevoerd. Uiteindelijk weten ze niet goed in hoeverre ze daadwerkelijk in-control zijn. Het is dus noodzakelijk, wil een organisatie haar interne beheersing en risicomanagement verbeteren, dat ze de aanwezige on-going monitoring expliciet maakt en evalueert. COSO noemt dit het creëren van de monitoring *baseline*. Vervolgens kunnen er eventueel geconstateerde leemtes worden geadresseerd en, zolang dit nog niet is gebeurd, de nodige separate evaluations worden uitgevoerd teneinde het resterende risico tot een aanvaardbaar niveau terug te brengen.

6 Wat betekent embedded testing voor de externe accountant?

Ook voor de externe accountant kan er veel voordeel behaald worden middels de toepassing van de monitoring guidance en het stimuleren dat hun cliënten dat ook doen. Zo verandert menig monitoring control hierdoor in een managementtest waarop, zeker sinds de publicatie van de Public Company Accounting Oversight Board (PCAOB, 2007a) Auditing Standard No. 5, door de externe accountant tot op zekere hoogte gesteund kan worden (Klumper en Shepherd, 2007a). De monitoringactiviteit verandert van controleobject in een hoeveelheid bewijs dat de werkelijke key controls effectief zijn; een beweging die dus 'dubbel voordeel' oplevert. Dit met betrekking tot de rol van de externe accountant bij SOX-compliant ondernemingen.

Maar ook bij niet SOX-compliant ondernemingen geldt dat zonder goede baselining er onvoldoende zicht is op de in-control status van de organisatie en kan de internal auditor geen adequate auditplanning maken. Maar is er ook geen goede dialoog mogelijk met de externe accountant, want als de onderneming ten slotte zelf niet goed weet hoe de risico's worden beheerst (middels controls, ongoing monitoring en ten slotte separate evaluations en hoe dit alles op elkaar is afgestemd) dan is het voor de externe accountant ook erg moeilijk om de werkzaamheden die hij nog dient uit te voeren optimaal af te stemmen op hetgeen er in de organisatie zelf gebeurt. Dit geldt niet alleen bij de reguliere jaarrekeningcontrole, maar ook bij onder andere SAS 70-trajecten, subsidieverklaringen en andere situaties waarin externe assurance gewenst is over de kwaliteit van interne beheersing.

Het voert te ver om in dit artikel in te gaan op de aspecten

van objectiviteit en deskundigheid, de wijze waarop organisaties de voorgestelde 'kanteling' door zouden kunnen voeren, hoe hun interne en externe accountants daarop zouden kunnen reageren alsook de vele andere praktische aspecten van embedded testing. En los van de potentieel flinke kostenbesparingen levert toepassing van embedded testing nog een aantal andere belangrijke, meer kwalitatieve, voordelen op, waar dit artikel ook niet op in zal gaan. Deze aspecten en voordelen zijn reeds grotendeels beschreven in eerdere publicaties (Klumper en Geuzebroek, 2007; COSO, 2008) en *webcasts* (voor onder andere *Compliance Week* en het *SOX 404 Institute* door de auteur van dit artikel).
Wat wel interessant is om in dit kader te vermelden, is dat Diekman (2005) heel dichtbij het concept van embedded testing is gekomen in zijn artikel in het MAB middels verwijzingen naar theorieën van Ramos[11] en Winters[12]. Vervolgens beschrijft hij helaas toch weer het conventionele SOX-404-proces waarin dus geen gebruik wordt gemaakt van monitoring, althans niet zoals het door COSO bedoeld was en is.

7 Samenvatting en conclusies

Managementtesten, in de SOX-404-context, is het vaststellen *door de organisatie zelf* dat de voor de internal control over financial reporting als relevant geïdentificeerde beheersmaatregelen al dan niet effectief hebben gewerkt. Om de kosten van dit 'managementtesten' te reduceren, kozen veel ondernemingen ervoor om het aantal van de belangrijkste beheersingsmaatregelen (de key controls) zo klein mogelijk te maken. Dit is de verkeerde weg. Er is een andere manier om de kosten substantieel te verlagen, zonder dat het zicht op de afdekking van de risico's kleiner wordt, namelijk: steunen op de monitoringcomponent van interne beheersing, zoals COSO sinds 1992 aanbeveelt en in de meest recente guidance (COSO, 2008) inzake monitoring krachtig herhaalt. Fundamenteel is het onderscheid tussen controls en monitoringactiviteiten. Controls hebben ten doel om fouten in processen, financiële verantwoordingen of wat ook maar de controledoelstelling is, te voorkomen of ten minste te detecteren. Monitoringactiviteiten hebben ten doel om vast te stellen of de onderliggende controls die zij monitoren, naar behoren werken.
Ondernemingen kunnen steunen op on-going monitoringactiviteiten die, mits adequaat uitgevoerd en gedocumenteerd, als onderdeel van het managementtesten kunnen worden beschouwd. Dit kan belangrijke kostenbesparingen opleveren: het meeste managementtesten dat in het kader van SOX-404-compliance-attestatie wordt uitgevoerd is overbodig en kan zelfs contraproductief werken.
Baselining, het creëren van de monitoring baseline, biedt zicht op de in-control status van de organisatie. Het betreft het expliciet maken en evalueren van de on-going monitoringactiviteiten, zodat men weet in hoeverre de on-going monitoringactiviteiten adequaat zijn ingericht en worden uitgevoerd. Voor zover dat niet al gebeurt, dienen separate evaluations te worden uitgevoerd die afgestemd worden op de mate van robuustheid van de on-going monitoringactiviteiten.
Bestudering van de nieuwste COSO-richtlijnen over monitoring is zeer de moeite waard voor eenieder die zich bezighoudt met interne beheersing. Toepassing ervan in de praktijk kan leiden tot een structureel betere interne beheersing tegen meestal lagere kosten. ■

C. Klumper RA MBA CIA is partner in KPMG's advisory praktijk, gespecialiseerd in interne beheersingsvraagstukken. Van 2005 tot 2006 was hij verantwoordelijk voor de wereldwijde internal control functie van Ahold.

Literatuur

■ Beurden, B.C.J.M. van, en S.J. Hartjes (2006), 'Integrated audit'. Efficiënte combinatie controleren jaarrekening en testen interne beheersingsmaatregelen, *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 80, no. 1/2, januari/februari, pp. 55-63.

■ Committee of Sponsoring Organizations of the Treadway Commission (1992): *Internal Control – Integrated Framework*, september; zie: www.coso.org.

■ Committee of Sponsoring Organizations of the Treadway Commission (2008): Exposure draft: *Internal Control – Integrated Framework: Guidance on Monitoring Internal Control Systems*, juni; zie: www.coso.org.

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

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

■ Klumper, C. en S.G.J. Geuzebroek (2007), Cure for SOX-testing blues at Royal Ahold, *Compliance Week*, 30 januari 2007, pp. 1-3.

■ Klumper, C. en Geuzebroek, S.G.J. (2007), Het middel tegen SOx Blues, *De Accountant*, april 2007, pp. 34-37.

■ Klumper, C. en M. Shepherd (2007), *Comment letter to the United States Public Company Accountanting Oversight Board on the proposed Auditing Standard "Considering and Using the Work of Others in an Audit"*, 26 februari 2007, zie: www.pcaob.org.

■ Klumper, C. en M. Shepherd (2007), *Comment letter to the United States Securities and Exchange Commission on the proposed interpretive guidance for management regarding its evaluation of internal control over financial*

reporting, 23 januari 2007, zie www.sec.org.
- KPMG (2006), SOx 404 Today: Alles onder controle?; pp. 4-5.
- Leeuwen, O.C. van (2005), Column: Sarbanes Oxley en Tabaksblat: dat valt tegen!, *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, no. 7/8, juli/augustus, pp. 324-325.
- Nieuw Amerongen, C.M. van, en N.G. de Jager (2006), SOx-404 en steunen op de testwerkzaamheden van de gecontroleerde onderneming, *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 80, no. 12, december, pp. 601-611.
- Public Company Accounting Oversight Board (2007a), *Auditing Standard No. 5, An audit of internal control over financial reporting that is integrated with an audit of financial statements and related independence rule and conforming amendments*; zie: http://www.pcaob.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf.
- Public Company Accounting Oversight Board (2007b), PCAOB Release No. 2007-005A, June 12, 2007, on *Auditing Standard No. 5, An audit of internal control over financial reporting that is integrated with an audit of financial statements and related independence rule and conforming amendments*; zie: http://www.pcaob.org/Rules/Docket_021/2007-06-12_Release_No_2007-005A.pdf.
- Ramos, M. (2004), Evaluate the control environment, *Journal of Accountancy*, vol. 197, no. 5, May, pp. 75-78.
- Securities and Exchange Commission (2007), *New Guidance for Compliance with Section 404 of Sarbanes-Oxley*; zie: www.sec.gov/news/press/2007/2007-101.htm.
- Winters, B.I. (2004), Choose the Right Tools for Internal Control Reporting, *Journal of Accountancy*, vol. 197, no. 2, February, pp. 34-40.

Noten

1 COSO is de Committee of Sponsoring Organizations of the Treadway Commission, een commissie samengesteld uit *live* vertegenwoordigers van de American Accounting Association, het American Institute of Certified Public Accountants (in veel opzichten de Amerikaanse variant van het Nederlandse NIVRA), Financial Executives International, het Institute of Management Accountants, en het Institute of Internal Auditors, dat ook een Nederlands chapter kent).

2 De Sarbanes-Oxley-wetgeving is in 2002 tot stand gekomen in respons op een aantal spraakmakende *deconfitures* van grote Amerikaanse ondernemingen, zoals Enron en Worldcom. Doelstelling was om regels te stellen waarmee de kans dat dergelijke problemen zich weer zouden voordoen, aanmerkelijk kleiner zou worden. Alle ondernemingen met een notering aan een Amerikaanse beurs, dus ook ondernemingen die in het buitenland gevestigd zijn, vallen onder de werking van deze wetgeving. De uiterste datum om aan de bepalingen van de Sarbanes-Oxley wetgeving te voldoen, is mede afhankelijk van de omvang van de onderneming.

3 De Code Tabaksblat (2003) stelt in Best Practice Bepaling II.1.4 dat het bestuur van een onderneming in het jaarverslag een beschrijving geeft van de voornaamste risico's gerelateerd aan de strategie, een beschrijving van de opzet en werking van de interne risicobeheersings- en controlesystemen en een beschrijving van eventuele belangrijke tekortkomingen, doorgevoerde verbeteringen en geplande verbeteringen. Ook Nederlandse ondernemingen refereren hiervoor aan het COSO-raamwerk.

4 Zie Committee of Sponsoring Organizations of the Treadway Commission: *Internal Control – Integrated Framework: Guidance on Monitoring Internal Control Systems* dat op 4 juni 2008 als *exposure draft* is gepubliceerd en waarop commentaar kon worden gegeven tot en met 15 augustus 2008.

5 COSO Guidance on Monitoring Internal Control Systems, Volume I, Executive Summary, par. 3.

6 Statement on Auditing Standards (SAS) 70 'Service Organizations' (AU Section 324) is een controlestandaard van de Auditing Standards Board van het American Institute of Certified Public Accountants (AICPA). In PCAOB Auditing Standard (AS) No. 5 'An audit of internal control over financial reporting that is integrated with an audit of financial statements' staat beschreven hoe een accountantscontrole met betrekking tot SOX dient plaats te vinden.

7 De auteur van dit artikel heeft in 2007 en 2008 een aantal SOX-congressen in de Verenigde Staten geleid en als onderdeel daarvan workshops gegeven over hoe monitoring zou kunnen worden toegepast zoals in dit artikel omschreven, en in geen van deze congressen of workshops was er een onderneming die aangaf al gebruik te maken van monitoring zoals in dit artikel omschreven.

8 Hierin is een verslag opgenomen van de presentatie die de auteur van dit artikel in november 2005 op een KPMG SOX-congres over embedded testing heeft gegeven.

9 Op 9 februari 2007 vond in Washington een gesprek plaats over de inhoud van de comment letter van de auteur van dit artikel en Matthew Shepherd, op de concept guidance van de SEC voor het management van ondernemingen met betrekking tot SOX-404. Dit gesprek is door de SEC gedocumenteerd in een openbaar *Memorandum to the File* van dezelfde datum; in de definitieve guidance verwijst de SEC expliciet naar de comment letter als één van de aanleidingen om de guidance aan te passen.

10 Van Nieuw Amerongen en De Jager (2006): 'Naar onze mening verdient het, om verwarring te voorkomen, aanbeveling om als uitgangspunt te nemen dat de werknemer van de gecontroleerde onderneming slechts testwerkzaamheden uitvoert ten aanzien van processen waar deze werknemer in het geheel niet in operationele zin bij betrokken is. Naar onze mening heeft het zelfs sterke voorkeur wanneer de tester slechts testwerkzaamheden uitvoert met betrekking tot beheersingsmaatregelen van een andere afdeling.'

11 Diekman (2005, p. 515) stelt: 'Ramos (2004) geeft aan dat in dit verband zou kunnen worden gestreefd naar een optimaal model van interne beheersing. Bij een optimaal model worden de interne controlemaatregelen on line en real time aangepast aan de veranderende (omgevings)factoren.'

12 Diekman (2005, p. 515) stelt: 'Winters (2004) stelt dat het om een continu proces van 'monitoring' van de interne controles gaat dat moet leiden tot een optimale structuur van interne beheersing. Met andere woorden: de beoordeling door het management van de interne controles is niet een proces dat eens per jaar wegens een wettelijke eis moet plaats hebben, maar moet worden ingebed als een continu proces dat leidt tot voortdurende aanpassing van de structuur van interne beheersing aan nieuwe omstandigheden.'