Integrated audit: 'SAS 70: het verlengstuk van internal control over financial reporting'

Drs. ing. S.R.M. van den Biggelaar RE, drs. S. Janssen RE en drs. G.J.L. Lamberiks

Het uitbesteden van een proces ontslaat het management niet van zijn eindverantwoordelijkheid. Maar hoe krijg je zekerheid over processen die je hebt uitbesteed en welke invloed heeft dit op het internal control statement en de integrated audit? Met het van kracht worden van de Sarbanes-Oxley Act hebben we opnieuw kennisgemaakt met een oude bekende. Maar wat staat ons te wachten?

Inleiding

Het van kracht worden van de Sarbanes-Oxley Act, met name sectie 404, vereist van het management van aan de Amerikaanse beurs genoteerde organisaties dat het een statement afgeeft over de interne beheersing rondom de financiële verslaglegging. De getrouwheid van deze verklaring moet worden getoetst door de externe accountant. In grote multinationale organisaties is het vaak zo dat één of meer processen zijn uitbesteed. De vraag is dan hoe zekerheid kan worden verkregen over de beheersing van processen die wel van invloed zijn op het financiële verslaggleggingsproces maar die buiten het zichtveld van zowel het management als de externe accountant plaatsvinden.

Specifiek voor die gevallen waarin delen van interne beheersing zijn uitbesteed, is in de Verenigde Staten een uitvoeringsstandaard gedefinieerd, Statement on Auditing Standards Nr 70 of kortweg SAS 70. Hoewel deze standaard en het hieruit voortvloeiende rapport in principe bedoeld zijn als een auditor-to-auditor rapport, heeft het rapport sinds de publicatie van PCAOB II een breder bereik gekregen. Ook het management mag voor zijn 'assessment on internal control over financial reporting' gebruikmaken van een SAS 70-verklaring.

In dit artikel staan de gebruikers van het SAS 70-statement centraal, de gebruikersorganisatie en haar accountant. In het bijzonder zal dit artikel ingaan op de voorbereiding en uitvoering van een SAS 70-onderzoek, het gebruik van een SAS 70-statement zelf en de kosten die met een SAS 70-onderzoek gepaard gaan. Aangezien het gebruik van een SAS 70-statement in het kader van jaarrekeningcontrole niet nieuw is, wordt SAS 70 in dit artikel vooral belicht vanuit de 'integrated audit'. De 'integrated audit' bestaat uit een gecombineerde controle op de jaarrekening en het internal control statement van de organisatie. Voor de invloed van de Sarbanes-Oxley Act

Drs. ing. S.R.M. van den Biggelaar RE
is partner bij KPMG Information Risk Management en docent aan het Tilburg Institute of Advanced Studies. Hij is verantwoordelijk voor diverse SAS 70-trajecten bij zowel ICT- als overige service providers. Daarnaast heeft hij veel ervaring op het gebied van ERP-systemen en HR Shared Service Centers.

vandenbiggelaar.stephen@kpmg.nl

Drs. G.J.L. Lamberiks
is adviseur bij KPMG Information Risk Management. Hij heeft ervaring opgedaan met een breed scala van advies- en auditopdrachten. Hij is betrokken geweest bij meerdere SAS 70-onderzoeken in zeer complexe IT-omgevingen, en heeft zich voorts gespecialiseerd in informatiebeveiliging en IT-audit tooling.

lamberiks.gideon@kpmg.nl

Drs. S. Janssen RE
is als senior manager werkzaam bij KPMG Information Risk Management en docent aan het Tilburg Institute of Advanced Studies. Hij heeft meerdere SAS 70-onderzoeken in complexe IT-omgevingen geleid. Tevens heeft hij adviesopdrachten geleid die gericht waren op het opzetten van internal control frameworks in relatie tot Sarbanes-Oxley.

janssen.stephan@kpmg.nl

en SAS 70 op leveranciers van het SAS 70-statement verwijzen we naar [Bigg06].

Voorbereiding en uitvoering

Het uitbesteden van een proces ontslaat het management niet van de plicht en de verantwoordelijkheid om zijn interne huishouding op orde te hebben ([PCAO04]). Het is dan ook de verantwoordelijkheid van de gebruikersorganisatie om haar dienstverlener aan te sturen en te controleren. Een verzoek om een SAS 70-onderzoek wordt vaak geïnitieerd door de gebruikersorganisatie(s) en/of haar accountant. In de praktijk zien we vaak dat er wordt gebeld naar de serviceorganisatie met het verzoek: 'Doe mij even een SAS 70'.

De externe accountant van de gebruikersorganisatie, ofwel de user auditor, is van oudsher de ontvangende partij. In principe heeft de user auditor slechts een beperkte rol in de voorbereiding en uitvoering van het SAS 70-onderzoek. Echter, in de praktijk zien en stimuleren de auteurs dat de user auditor juist wel wordt betrokken in de voorbereiding van het onderzoek, voornamelijk bij het bepalen van de scope en planning van het SAS 70-onderzoek.

Het verzoek 'Doe mij even een SAS 70' heeft vaak meer voeten in de aarde dan op het eerste gezicht wellicht lijkt

De serviceorganisatie is leverancier van het SAS 70-statement en is opdrachtgever van de service auditor. De serviceorganisatie is verantwoordelijk voor het opstellen van een dienstbeschrijving, het definiëren van beheerdoelstellingen (control objectives) en het beschrijven van internecontrolemaatregelen (control descriptions) die zij heeft getroffen voor het realiseren van de beheerdoelstellingen. In de praktijk zien we dat de beheerdoelstellingen zoals deze terugkomen in het SAS 70-statement vaak in overleg tussen de serviceorganisatie en de userorganisatie worden bepaald en afhankelijk zijn van contractafspraken en dienstverlening.

Daarnaast heeft de serviceorganisatie in de uitvoering van het onderzoek nog een aantal verantwoordelijkheden, maar hiervoor verwijzen de auteurs graag naar een uitgave van het American Institute of Certified Professional Auditors ([AICP05]).

De service auditor geeft een verklaring over de mate waarin de beheerdoelstellingen worden gerealiseerd. De service auditor is ervoor verantwoordelijk auditwerkzaamheden uit te voeren rondom de getrouwheid van de dienstbeschrijving, de opzet van het raamwerk van interne controle en het bestaan en eventueel de werking van de beschreven controlemaatregelen.

Generieke versus specifieke SAS 70-rapporten

Het verzoek 'Doe mij even een SAS 70' heeft vaak meer voeten in de aarde dan op het eerste gezicht wellicht lijkt. In de praktijk zien de auteurs dat elke gebruikersorganisatie deze vraag op een andere manier beantwoord wil zien.

In het ene uiterste neemt men genoegen met een generiek SAS 70-rapport, waarin het grootste deel van de inhoud wordt bepaald door de serviceorganisatie. In een generiek SAS 70-rapport beschrijft de serviceorganisatie de standaarddienstverlening, beheerorganisatie en controlemaatregelen. Het generieke rapport is een afgeleide van de standaarddienstverlening zoals deze is vastgelegd in haar dienstenportefeuille.

In het andere uiterste is een specifiek rapport gewenst. Aangezien het management van de userorganisatie het SAS 70-rapport wil gebruiken als verlengde van zijn eigen internal control framework, ontvangt het graag een rapport dat direct aansluit op dat framework.

Een overzicht van de belangrijkste verschillen tussen een generiek SAS 70-rapport en een specifiek SAS 70-rapport is opgenomen in tabel 1.

Een generiek rapport biedt in veel situaties voldoende zekerheid voor zowel de gebruikersorganisatie als haar auditor en is ook goedkoper dan een specifiek rapport. In principe gaat het hierbij dan om een standaard en ondersteunend proces, bijvoorbeeld pensioenadministratie of salarisverwerking. Naarmate de mate van standaardisatie afneemt en de complexiteit toeneemt, neemt ook de behoefte aan een specifiek statement toe.

Het SAS 70-rapport

Het resultaat van een onderzoek uitgevoerd volgens de SAS 70-standaard is een SAS 70-rapport. Het rapport kent in principe vier secties:

- de accountantsverklaring (sectie I);
- de beschrijving van controls door de serviceorganisatie (sectie II);
- informatie van de service auditor (sectie III);
- overige informatie van de serviceorganisatie (sectie IV).

Het is echter mogelijk dat u SAS 70-rapporten tegenkomt met minder secties.

Onderwerp	Generiek SAS 70-statement	Specifiek SAS 70-statement
Dienstbeschrijving	– Afgeleide van de standaardservice-portfolio – Generieke beschrijving	– Afgeleide van het contract met de gebruikersorganisatie – Specifieke beschrijving van de feitelijk geleverde dienst(en)
Control Objectives	– Bepaald door de serviceorganisatie – Afgeleide van de standaard-dienstverlening	– Overeengekomen tussen de serviceorganisatie en de gebruikersorganisatie – Eén op één afgeleide van raamwerk van de gebruikersorganisatie
Controls	– Aanwezig in de standaard-dienstverlening voor elke klant	– Opname van specifiek overeengekomen controlemaatregelen, bijvoorbeeld directe rapportage van security-incidenten
Testwerkzaamheden	– Klantonafhankelijk	– Klantafhankelijk – Aanvullende tests op verzoek van de gebruikersorganisatie
Auditperiode	– Zesmaandsperiode	– Overeengekomen tussen serviceorganisatie en gebruikersorganisatie (minimaal zes maanden)
Afsluiting	– Aanbieding van het rapport door de serviceorganisatie	– Aanbieding van het rapport door de serviceorganisatie – Bespreking van de rapportage en belangrijkste bevindingen tussen gebruikersorganisatie, serviceorganisatie, service auditor en user auditor

Tabel 1. Verschillen tussen een generiek en een specifiek SAS 70-rapport.

Sectie III is alleen verplicht indien het SAS 70-rapport een uitspraak doet over een bepaalde werkingsperiode, ofwel een SAS 70 type II. PCAOB-standaard 2 vereist dat de internecontrolemaatregelen op werking worden getoetst ([PCAO04]), vandaar dat u in het kader van de integrated audit in principe altijd een sectie III zult tegenkomen.

Een sectie IV wordt slechts dan gebruikt indien de serviceorganisatie informatie aan de gebruikersorganisatie wil verstrekken die buiten de scope van het onderzoek valt. Denk hierbij aan op stapel staande ontwikkelingen, of de wijze waarop de serviceorganisatie omgaat met bevindingen.

Hoewel u door de nummering van secties wellicht verwacht dat de secties ook in deze volgorde worden opgenomen in het SAS 70-statement, is er geen verplichte volgorde. In de praktijk zien we dan ook dat de verschillende secties nog wel eens in een andere volgorde worden gezet om de leesbaarheid van het rapport te vergroten.

Het moge duidelijk zijn dat het in ontvangst nemen en archiveren van een SAS 70-rapport niet voldoende is voor de integrated audit of voor het management assessment on internal control. Maar hoe ga je daar als user auditor of user management mee om? Het ligt voor de hand om vooraan te beginnen, de ervaring leert echter dat dit niet altijd de beste manier is.

Zoals eerder in dit artikel is vermeld, kan er sprake zijn van een generiek of een specifiek SAS 70-rapport. De wijze waarop een SAS 70-rapport moet worden gelezen door het management is hiervan afhankelijk en heeft ook veel te maken met het verwachtingsmanagement dat in de voorbereiding en uitvoering door de serviceorganisatie heeft plaatsgevonden.

Bij een generiek rapport dient het management zichzelf onder andere de volgende vragen te stellen:

- Sluit de scope van het onderzoek aan op ons eigen internal control framework? Worden alle relevante processen en deelprocessen die wij hebben uitbesteed, door het SAS 70 geraakt? In de meeste gevallen is dat neergelegd in de beschrijving van controls door de serviceorganisatie (sectie II).
- Welke control objectives hanteert de serviceorganisatie? Hoe passen deze control objectives op de binnen de organisatie gehanteerde control objectives? Control objectives zijn terug te vinden in sectie II en III. Om redundantie in het rapport te voorkomen, wordt er vaak voor gekozen om de control objectives alleen in sectie III te vermelden.

In het kader van de integrated audit is het niet voldoende een SAS 70-rapport in ontvangst te nemen en het te archiveren

- Heeft de service auditor een gekwalificeerde opinie op de voor de gebruikersorganisatie relevante control objectives (sectie I, de accountantsverklaring)? En zo ja, wat betekent dit dan, wat is de omvang en heeft de geconstateerde tekortkoming betrekking op onze organisatie? Deze informatie is opgenomen in sectie III.

Bij een specifiek rapport is in principe alleen de laatste vraag nog relevant. De eerste twee zijn in principe al in

de voorbereiding beantwoord. Vanzelfsprekend dient het management nog altijd wel kennis te nemen van het rapport en vast te stellen dat het rapport aansluit op wat was afgesproken in de scopingsletter.

SAS 70 voor de user auditor

Voor de user auditor dient het SAS 70-rapport twee doelen. In eerste instantie het traditionele doel: het verkrijgen van een redelijke mate van zekerheid over opzet, bestaan en werking van controlemaatregelen binnen de serviceorganisatie. Op deze controlemaatregelen wil de user auditor steunen bij het plannen van controlewerkzaamheden bij de gebruikersorganisatie en het bepalen van het controlerisico.

Voorts is het rapport een onderdeel van het toetsen van het management assertion op de interne beheersing rondom de financiële verslaglegging. Bijzonder hieraan is dat de uitvoering van testwerkzaamheden niet door het management zelf heeft plaatsgevonden maar door de service auditor.

In dit kader is het voor de user auditor niet alleen relevant om te verifiëren en evalueren of er in sectie I opmerkingen zijn opgenomen die potentieel tot een 'material weakness' leiden, maar ook hoe het management is omgegaan met het SAS 70-statement zelf. De vraag die hierbij bijvoorbeeld gesteld kan worden, is: 'Heeft het management zelf het SAS 70-statement op een juiste manier beoordeeld en indien nodig corrigerende maatregelen getroffen?'

Een gekwalificeerde opinie door de service auditor hoeft niet per definitie te leiden tot een 'material weakness'

Voor het traditionele gebruik van een SAS 70-rapport door de user auditor zijn specifieke richtlijnen opgenomen in de SAS 70-standaard (zie [AICP05]). Bijvoorbeeld:

- Een ongekwalificeerd oordeel in sectie I betekent niet dat de user auditor alleen op basis hiervan het controlerisico omlaag kan brengen. Ook 'deficiencies' op individuele controls kunnen invloed hebben op de planning en het controlerisico. Uiteindelijk zijn het werkende controls op basis waarvan de user auditor een lager controlerisico kan rechtvaardigen (zie onder meer ook [PCAO04]).
- Melding van zogenaamde 'user organisation control considerations' moeten worden meegenomen in het plannen van de audit (zie hierna).
- De werkingsperiode die wordt getest door de service auditor moet zoveel mogelijk aansluiten op de auditperiode van de user auditor. Een SAS 70 die slechts een deel van de auditperiode afdekt is minder waardevol.

Kort gezegd komt het erop neer dat de user auditor in het kader van de controle op de jaarrekening moet bepalen welke elementen van het SAS 70-rapport voor zijn controle van belang zijn en of het SAS 70-rapport op die elementen voldoende zekerheid biedt voor werking van controles.

De impact van een gekwalificeerde opinie

Indien de service auditor concludeert dat één of meer beheerdoelstellingen niet worden gehaald, leidt dit tot een gekwalificeerde opinie. De betreffende beheerdoelstelling wordt in dat geval expliciet uitgesloten in sectie I. Een gekwalificeerde opinie door de service auditor hoeft niet per definitie te leiden tot een 'material weakness' in het internal-controlraamwerk van de gebruikersorganisatie, noch hoeft dit te leiden tot een afkeurende verklaring bij de jaarrekening.

Een gekwalificeerde opinie is voor het raamwerk van interne controle in eerste instantie niets anders dan een geconstateerde tekortkoming, ook wel 'deficiency' genoemd. Aangezien het SAS 70-statement in principe een integraal onderdeel is van het internal-controlraamwerk, dient een 'deficiency' bij de serviceorganisatie in principe ook op eenzelfde manier te worden beoordeeld en geëvalueerd.

Het kan best zo zijn dat op grond van een kwalificatie de user auditor tot de conclusie komt dat er sprake is van een 'material weakness' in de interne beheersing over financiële verslaglegging. Dit betekent niet automatisch dat er ook een gekwalificeerde opinie bij de jaarrekening wordt gegeven. Door het bestaan van de 'material weakness' dient de user auditor bij het plannen van zijn controlewerkzaamheden meer gegevensgerichte werkzaamheden te plannen. Op basis van die werkzaamheden kan alsnog worden geconcludeerd dat de jaarrekening een getrouwe weergave is van de werkelijkheid.

De 'user organisation control consideration'

Tijdens het doornemen van het SAS 70-rapport kan het zijn dat op enig moment een 'user organisation control consideration' wordt gegeven. Kort gezegd komt dit erop neer dat de serviceorganisatie er bij het inrichten van een dienst rekening mee heeft gehouden dat ook de gebruikersorganisatie bepaalde controls heeft ingericht. Een goed voorbeeld is het verwerken van personeelsmutaties door een salarisverwerker. De serviceorganisatie kan deze mutatie slechts tijdig verwerken indien de gebruikersorganisatie deze ook bijtijds doorgeeft. De serviceorganisatie zal om die reden aangeven dat zij van

de gebruikersorganisatie verwacht controlemaatregelen te hebben ingericht die tijdig een signaal afgeven aan de serviceorganisatie.

Wat betekent een dergelijke 'user organisation control consideration' voor het management van de gebruikersorganisatie en de user auditor? Het management dient er zich van te vergewissen dat het dergelijke controlemaatregelen heeft geïmplementeerd, heeft gedocumenteerd en heeft getest in het kader van het 'assessment on internal control over financial reporting'. De user auditor zal in zijn controle van het management assertion moeten verifiëren of het management de user control consideration zelf heeft gesignaleerd bij het doornemen van het rapport, een soortgelijke control heeft gedocumenteerd en getest, en vervolgens zal hij zelf nog een paar waarnemingen moeten doen om de werking van de control zelfstandig vast te stellen (zie ook [PCAO04]). Dit laatste is wederom van belang voor het management assertion in het kader van het SOX 404-statement en in de tweede plaats om op het moment dat deze test faalt de werkzaamheden in het kader van de jaarrekeningcontrole hierop aan te passen.

Waarom kost een SAS 70-statement zoveel geld?

Deze vraag wordt ons in de praktijk vaak gesteld zowel door service providers die voor een generiek statement in de praktijk vaak de kosten dragen, als door de gebruikersorganisatie die voor specifieke SAS 70-rapporten de rekening moet betalen. De relatief hoge kosten zijn een gevolg van de benodigde inspanning om een SAS 70-rapport op te leveren. Hieronder wordt een aantal oorzaken toegelicht waardoor deze inspanning zo groot is:

Een SAS 70 type II-verklaring geeft een redelijke mate van zekerheid (reasonable assurance) over een minimale periode van zes maanden. Reasonable assurance betekent dat de auditor niet alleen kan afgaan op bijvoorbeeld interviews maar ook feitelijke waarnemingen moet doen in de vorm van inspections, observations, reperformance, etc. Bovendien betekent een type II met een werkingsperiode van minimaal zes maanden in de praktijk dat er minimaal tweemaal wordt getest gedurende de zes maanden.

In 2004 zijn de richtlijnen van de PCAOB op het gebied van dossiervorming verschenen (zogeheten PCAOB-richtlijn 3). Deze richtlijn is in beginsel van toepassing op integrated audit-activiteiten. Voorzover bekend hebben de meeste auditfirma's die SAS 70-rapporten afgeven deze richtlijn ook van toepassing verklaard voor SAS 70-onderzoeken. De consequentie hiervan is een vergrote werklast om de dossiers in orde te maken. Zo moet bijvoorbeeld elk dossierstuk (werkpapieren, en ontvangen bewijsmateriaal) tweemaal worden beoordeeld: eenmaal door de auditor en eenmaal door een reviewer van gelijk of hoger ervaringsniveau. Voorts moet elk dossierstuk worden gedateerd en geparafeerd door auditor en reviewer.

Maar vergeet ook niet dat ook de service auditor, conform sectie 102 van de Sarbanes-Oxley Act, moet zijn ingeschreven bij de PCAOB (www.pcaobus.org/Registration/) wil de rapportage bruikbaar zijn voor SOX 404-werkzaamheden. Als gevolg hiervan moet de service auditor voldoen aan alle richtlijnen van de PCAOB. Een voorbeeld daarvan is dat de PCAOB vanuit Amerika het recht heeft om dossiers te reviewen bij de service auditors in Europa. Inmiddels zijn de eerste tickets door de PCAOB besteld om dossierreviews uit te voeren.

De relatief hoge kosten zijn een gevolg van de benodigde inspanning om een SAS 70-rapport op te leveren

In de praktijk zien we veelal bij de eerste bespreking tussen de vier betrokken partijen dat de eisen van de user organisation en user auditor hoog zijn. Niet alleen worden er veel control objectives gedefinieerd, maar ook het aantal objecten in scope is groot. Daarnaast zien wij in de praktijk vaak specifieke eisen op het gebied van bijvoorbeeld de steekproeven, tussenrapportages, besprekingen, early warnings, mate van detail van sectie III, etc. Vanzelfsprekend heeft dit een grote invloed op de benodigde inspanning.

Er wordt steeds vaker gevraagd om zekerheid over een langere periode. Eind jaren negentig is het begonnen met de eerste TPM-verklaringen die met name gericht waren op opzet en bestaan. Dit werd gevolgd door SAS 70 type I-verklaringen. Met de SOX-wetgeving is het bijna vanzelfsprekend opgerekt naar type II-rapportages over een periode van zes maanden en inmiddels vragen de eerste user auditors SAS 70-statements over een periode van negen of twaalf maanden. We zien dit met name gebeuren bij userorganisaties die in hoge mate afhankelijk zijn van IT en/of bijvoorbeeld geen fysieke goederenstromen hebben (telco's, banken). Hoewel een langere auditperiode niet automatisch betekent dat de selection size van de tests moet worden uitgebreid, dient deze wel beter gespreid te worden over de auditperiode. In de praktijk betekent dit al snel dat er drie of vier keer moet worden getest.

Wat nu als er geen SAS 70-statement is?

In de praktijk hebben we al een paar keer meegemaakt dat het ontbreken van een SAS 70-statement tot grap-

pige maar ook frustrerende situaties kan leiden. Indien er geen SAS 70 beschikbaar is (bijvoorbeeld omdat serviceorganisatie en userorganisatie het niet eens worden over wie wat gaat betalen), betekent dit met een strikte interpretatie van de SOX 404-wetgeving dat het management van de userorganisatie zelf de key controls bij de service provider moet gaan testen. Vervolgens, maar natuurlijk niet gelijktijdig, moet de user auditor reperformancewerkzaamheden uitvoeren om vast te stellen of de testwerkzaamheden door het management goed zijn uitgevoerd. Hij staat dus ook weer op de stoep bij de service provider. Als service providers meerdere klanten hebben die SOX-plichtig zijn, leidt dit al snel tot ongewenste situaties die voor alle partijen maar beter kunnen worden voorkomen. Dit is overigens ook vaak de conclusie van serviceorganisaties en hun klanten na één jaar werken zonder SAS 70-statement.

Tot slot

Met het van kracht worden van de Sarbanes-Oxley Act is het begrip SAS 70 weer uit de kast gehaald en van zijn stofmantel ontdaan. Dit artikel is voornamelijk geschreven vanuit het perspectief van de gebruikers. Duidelijk moge zijn dat je er met het verzoek 'Doe mij even een SAS 70' niet bent.

Is het een hype? De toekomst zal het leren. Vandaag de dag zien we in ieder geval dat steeds meer organisaties assurance willen over een uitbesteed proces, ook niet (grote) beursgenoteerde organisaties. In enkele gevallen heeft het zelfs helemaal niets te maken met financiële verslaglegging of integrated audit. De vraag aangaande assurance komt dan vanuit een heel andere hoek, bijvoorbeeld FDA, OPTA of andere toezichthoudende instanties.

Is er nog meer over SAS 70 te schrijven? Ja, zeer zeker. Denk maar eens aan situaties waarin delen van één proces zijn uitbesteed aan meerdere service providers. Hoe sluit je al die rapporten op elkaar aan? Hoe ga je als serviceorganisatie om met grote veranderingen in aangeboden diensten? Bijvoorbeeld de implementatie van een nieuw systeem, transities, offshoring van activiteiten, of situaties waarin de standaardset van controls simpelweg nog niet is geïmplementeerd. Wellicht dat we in toekomstige artikelen nog op deze vragen terugkomen.

Literatuur

[AICP05] American Institute of Certified Public Accountants, *AICPA Audit and Accounting Guide: Service Organizations: Applying SAS 70, as Amended*, 2005.

[Bigg06] Drs. ing. S.R.M. van den Biggelaar RE, drs. S. Janssen RE en drs. G.J.L. Lamberiks, *SAS 70 in een ICT-fabriek: Accessoire, fabrieksoptie of onderdeel van de standaard?*, Compact 2006/1.

[PCAO04] Public Company Accounting Oversight Board, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*, 2004.