OPKOMST VAN EEN NIEUWE WERELDWIJDE ASSURANCESTANDAARD

ISAE 3402: einde van SAS 70 in zicht?

Dit artikel is geschreven om u te informeren over de ontwikkelingen op het gebied van *third party reporting*[1], met name op het gebied van SAS 70-verklaringen. Onderwerpen die aan bod komen zijn de mogelijkheden en beperkingen van de SAS 70-standaard, de ontwikkeling van de nieuwe ISAE 3402-standaard en de gevolgen daarvan voor de IT-auditor.

DENNIS HOUTEKAMER EN REMCO DE GRAAF

Het artikel is als volgt opgebouwd. We beginnen met een korte introductie van de belangrijkste begrippen in het artikel. Daarbij wordt ingegaan op de uitbesteding van dienstverlening en de beheersing daarvan. Vervolgens worden instrumenten toegelicht, die dienen om zekerheid te verkrijgen over de beheersing van uitbestede dienstverlening, waarbij nader ingegaan wordt op de SAS 70-standaard en de nieuwe ISAE 3402-standaard. Ten slotte wordt een vergelijking gemaakt tussen de SAS 70-standaard en de nieuwe ISAE 3402-standaard, waarbij vooral de gevolgen voor de IT-auditor worden toegelicht. Gezien het onderwerp en het soort wijzigingen, zijn deze gevolgen zowel relevant voor de IT-auditor van de serviceorganisatie als voor de IT-auditor van de gebruikersorganisatie.

Dit artikel is geschreven in januari 2009. Op dat moment had de nieuwe ISAE 3402-standaard nog de status *exposure draft*. De inhoud van de definitieve versie van de ISAE 3402-standaard (die in de loop van 2009 wordt verwacht) kan dus afwijken van wat in dit artikel wordt beschreven.

INTRODUCTIE

Uitbesteding

Uitbesteding[2] van diensten of productie is een van de instrumenten van ondernemingen en overheden om zich te focussen op de voor hen belangrijkste taak: het realiseren van de doelstellingen van de onderneming. Door het uitbesteden kunnen deze organisaties meer middelen overhouden voor zaken als innovatie, een snellere *time-to-market* en een meer flexibele organisatie. Het kostenbesparingsaspect is het meest gehoorde argument om tot uitbesteding over te gaan, naast andere argumenten zoals kwaliteitsverbetering, flexibilisering van arbeid en verbetering van de solvabiliteitspositie. De vraag of uitbesteding van processen inderdaad deze voordelen oplevert, is niet eenvoudig en eenduidig te beantwoorden. Feit is wel dat uitbesteding van processen geen voorbijgaande trend is en dus steeds meer bedrijven en hun medewerkers raakt. Daarnaast biedt uitbesteding ook mogelijkheden voor ondernemingen die in staat zijn de diensten te leveren die een andere partij wenst uit te besteden.

Verschillende soorten processen kunnen worden uitbesteed. Een voor IT-auditors bekende vorm is het uitbesteden van het beheer van rekencentra. Een andere vorm is het uitbesteden van ondersteunende bedrijfsprocessen (primair of bedrijfsondersteunend) zoals de afhandeling van vragen via een extern *call center* of het uitbesteden van (een deel van) de IT-organisatie. De meest verregaande vorm is de uitbesteding van (delen van) bedrijfsprocessen die vaak niet als *core business* worden gezien. Een voorbeeld van een dergelijke uitbesteding is het uitbesteden van de administratieve afhandeling van aandelentransacties bij een financiële instelling. Het beheersen van deze dienstverlening en het beheer van de afspraken omtrent de dienstverlening, bijvoorbeeld via Service Level Agreements (SLA's), aan zowel de leveranciers- als klantzijde, is een activiteit die ook voor de IT-auditor uitdagingen biedt.

Beheersing van uitbestede diensten

Het inregelen en beheersen van de uitbesteding kent niet alleen operationele uitdagingen, maar brengt ook voor de beheersing van de verschillende processen aandachtspunten met zich mee. Uitbesteding van processen is namelijk geen uitbesteding van alle verantwoordelijkheid, ook al zijn alle afspraken en *monitoring* daarvan nog zo goed vastgelegd in SLA's. Vanuit de principes van goed ondernemingsbestuur blijft de organisatie die de processen uitbesteedt eindverantwoordelijk voor de beheersing van deze processen. Vooral bij processen die een groot (materieel) financieel belang kennen, zal de uitbestedende

organisatie (de gebruikersorganisatie) een of andere vorm van toezicht op de partij aan wie wordt uitbesteed (de serviceorganisatie) moeten uitoefenen. Het uitoefenen van toezicht is niet alleen een wens van de uitbestedende partij, maar vaak ook vereist vanuit de wetgeving, zoals in het geval van de Amerikaanse Sarbanes-Oxley-wetgeving, die aangeeft dat het management van een organisatie aantoonbaar *in control* moet zijn van zijn onderneming. Het in control zijn geldt dus niet alleen voor de processen die binnen de eigen onderneming worden uitgevoerd, maar ook voor de processen die extern worden uitgevoerd en direct of indirect verband houden met de interne beheersing van de onderneming. De uitbestedende organisatie zal van de serviceorganisatie zekerheid moeten verkrijgen over de mate van beheersing over de processen die daar uitgevoerd worden.[3]

RAPPORTAGE OMTRENT BEHEERSING

Voor de gebruikersorganisaties die behoefte hebben aan een onafhankelijk en onpartijdig onderzoek en oordeel, is een interne verantwoordingsrapportage (bijvoorbeeld in de vorm van een SLA-rapportage) vaak onvoldoende. De gewenste onafhankelijkheid en onpartijdigheid ontbreekt als de verantwoordingsrapportage wordt opgesteld door de partij die ook de dienstverlening levert. Onafhankelijk onderzoek is voor gebruikersorganisaties dan ook noodzakelijk. Aangezien serviceorganisaties vaak werken voor meerdere opdrachtgevers, die elk hun eigen behoeften en eisen stellen aan beheersing, zal een serviceorganisatie van meerdere opdrachtgevers de vraag krijgen aan te tonen dat zij 'in control' is. Wanneer een rapportage over de interne beheersing volgens een algemeen geaccepteerde standaard wordt opgesteld en beoordeeld, is deze rapportage voor diverse gebruikers zinvol. Een SAS 70-verklaring is een rapportagevorm die in de praktijk veel wordt gebruikt om over de effectiviteit van de beheersingsmaatregelen bij de serviceorganisatie te rapporteren.

Iedere methode heeft zijn voor- en nadelen, maar in de praktijk is de SAS 70-verklaring een alom geaccepteerde standaard. Wij zullen de SAS 70-standaard hierna nader toelichten en ingaan op de toekomst van deze standaard. Daarnaast gaan wij in op de ISA 402-standaard en de potentiele opvolger van de SAS 70-standaard: de ISAE 3402-standaard. Omdat over de SAS 70-standaard in het verleden al voldoende is geschreven, zullen wij volstaan met een korte beschrijving.

SAS 70-standaard

In het begin van de jaren negentig van de vorige eeuw bracht de American Institute of Certified Public Accountants (AICPA) het Statement on Auditing Standards No. 70, Service Organizations (SAS 70) uit. De standaard was bedoeld om auditors van gebruikersorganisaties te ondersteunen bij de beoordeling van interne beheersingsmaatregelen. Hoewel ook andere, vergelijkbare standaarden of andere vormen van third party reporting kunnen worden gebruikt, is de SAS 70-standaard uitgegroeid tot een *de facto* standaard voor het rapporteren over beheersingsmaatregelen bij serviceorganisaties. Ook in Nederland is de SAS 70-standaard een veelgebruikte wijze om (auditors van) externe partijen (met name gebruikersorganisaties) zekerheid te verschaffen over de mate van interne beheersing. Het gebruik van een standaard als SAS 70 brengt een aantal voordelen met zich mee voor zowel de gebruikersorganisatie als de serviceorganisatie. De belangrijkste voordelen voor de gebruikersorganisatie zijn:

- het geeft de gebruikersorganisatie inzicht in en zekerheid over de wijze waarop de serviceorganisatie haar procesbeheersing heeft georganiseerd, waardoor de gebruikersorganisatie beter in staat is haar eindverantwoordelijkheid over de uitbestede processen te dragen; en
- de gebruikersorganisatie voldoet (indien van toepassing) aan de eisen die de diverse wet- en regelgeving haar stelt.

Toereikendheid van een SAS 70-rapport

Omdat de *scope* van een SAS 70-rapport wordt bepaald door de serviceorganisatie, moet de auditor van de gebruikersorganisatie altijd vaststellen of het rapport toereikend is om te voldoen aan de assurance-eisen die de gebruikersorganisatie heeft. De gebruiker van het SAS 70-rapport moet onder andere vaststellen: ▶

Opbouw en typen SAS 70-rapportages

Een SAS 70-rapport bestaat uit een aantal vaste onderdelen, afhankelijk van het type rapport dat wordt afgegeven. Het rapport zelf is opgebouwd uit het *assurance*rapport van de auditor, een algemene beschrijving van de organisatie en haar dienstverlening aangevuld met de wijze waarop zij de interne beheersing invult en een deel met doelstellingen van de interne beheersing met daaronder de gedetailleerde beschrijvingen van de beheersingsmaatregelen.
Er zijn twee typen rapportages mogelijk:

- Type I-rapport: de auditor van de serviceorganisatie beperkt zich tot de opzet en het bestaan van de beheersingsmaatregelen;
- Type II-rapport: de auditor van de serviceorganisatie toetst ook de werking van de maatregelen en beschrijft de wijze van toetsing en uiteraard de resultaten van de toetsing.

- in hoeverre de in het rapport beschreven beheersdoelstellingen overeenkomen met de beheersdoelstellingen van de uitbestedende partij;
- in hoeverre het afgegeven SAS 70-rapport bruikbaar is voor het gewenste doel (voor bepaalde doeleinden, zoals bij vereiste rapportering over effectieve werking, is alleen een Type II-rapport bruikbaar);
- wie de uitgevoerde testwerkzaamheden heeft uitgevoerd en of de testwerkzaamheden op een adequate wijze zijn uitgevoerd;
- of de diensten van subserviceorganisaties (geleverd aan de serviceorganisatie) zijn meegenomen in of uitgesloten van de rapportage (*carve-in/carve-out*).

In de praktijk is het uiteraard verstandig om voorafgaand aan de werkzaamheden de scoping af te stemmen op de assurancebehoefte van de gebruikersorganisatie.

Beperkingen van het SAS 70-rapport
De scope, structuur en toepasbaarheid van het SAS 70-rapport hebben in de loop der tijd aanleiding tot opmerkingen gegeven van diverse partijen (zoals van auditors en serviceorganisaties). Veel opmerkingen zijn inherent aan de oorspronkelijke doelstelling van het SAS 70-rapport: zekerheid geven over de interne beheersingsmaatregelen bij een serviceorganisatie voor zover van belang voor de jaarrekeningcontrole van een gebruikersorganisatie. Een belangrijk nadeel is de beperkte scope van de verklaring. Een SAS 70-verklaring bevat uitsluitend internecontroledoelstellingen en beheersingsmaatregelen die relevant zijn voor de betrouwbaarheid van financiële informatie. Het opnemen van interne controledoelstellingen en beheersingsmaatregelen op het gebied van continuïteit (voor zover dit toekomstgerichte doelstellingen betreft) en/of compliance (het voldoen aan wet- en regelgeving) is in principe niet toegestaan. Dit is in het bijzonder een nadeel in complexe, sterk gereguleerde sectoren, zoals het bankwezen waar toezichthouders van gebruikersorganisaties inzicht wensen in de mate van beheersing bij serviceorganisaties. Voor een gebruikersorganisatie zullen de beheersingsmaatregelen rond de continuïteit en compliance vaak een essentieel aandachtspunt zijn, waarover de gebruikersorganisatie met behulp van een onafhankelijke derde moet laten rapporteren. Vaak wordt dit probleem ondervangen door in Sectie IV van een SAS 70-rapport de serviceorganisatie de maatregelen te laten beschrijven die op continuïteitsgebied genomen zijn. De auditor van de serviceorganisatie mag deze maatregelen echter niet toetsen.

Een ander nadeel is dat de SAS 70-standaard een product is van de Amerikaanse AICPA-organisatie en dat in principe alleen door de AICPA gecertificeerde accountants (met de CPA titel) SAS 70-verklaringen mogen afgeven. Over dit punt ontstaat regelmatig onduidelijkheid en discussie. In de praktijk gaan de accountantskantoren/-organisaties hiermee verschillend om. De praktijk is dat in Nederland verklaringen worden afgegeven volgens Nederlands recht (COS 3000[4]) en conform de vormvereisten van SAS 70.

Herziening van de SAS 70-standaard
De AICPA is bezig met de herziening van de SAS 70-standaard. Doelstelling van de herziening is onder andere het laten aansluiten van de SAS 70-standaard op de ISAE 3402-standaard. Dit heeft als voordeel dat internationaal rapporterende serviceorganisaties een servicerapport kunnen uitbrengen dat in verschillende landen bruikbaar is. Het ligt in de lijn der verwachting dat de verbeteringen met name liggen bij de eerder genoemde beperkingen, en bij een betere aansluiting op lokale standaarden en verbreding van de doelgroep van het rapport. Op dit moment is de verwachting dat de opvolger van de SAS 70-standaard overeenkomstig de ISAE 3402-standaard zal zijn, met wellicht enkele kleine verschillen ten opzichte van deze standaard, die later in dit artikel nader wordt toegelicht.

ISA 402-standaard
Naast de SAS 70-standaard is in de jaren negentig van de vorige eeuw nog een standaard ontwikkeld die betrekking heeft op de omgang met serviceorganisaties. Dit betreft de ISA (International Standard on Auditing) 402-standaard van de International Auditing and Assurance Standards Board (IAASB) van de International Federation of Accountants (IFAC). De *ISA 402 – Audit Considerations Relating to Entities Using Service Organizations* beschrijft richtlijnen die een gebruikersorganisatie en haar auditors kunnen gebruiken bij het bepalen van de *impact* op de controle van de jaarrekening van de serviceorganisatie en het gebruik van rapportages gebaseerd op de SAS 70-standaard. De ISA 402-standaard geeft echter geen richtlijnen voor de serviceauditor (de third party-auditor die de verklaring afgeeft) voor het uitvoeren van beoordelingen van interne beheersingsmaatregelen bij de serviceorganisatie. Een voorstel van een standaard die de serviceauditor kan hanteren, is door de IAASB opgesteld in de vorm van een exposure

draft ISAE 3402-standaard, die in de volgende paragraaf nader wordt toegelicht.

ISAE 3402-standaard
De IAASB heeft in 2006 een onderzoek gestart dat twee doelstellingen had:
- het herijken van de ISA 402-standaard; en
- het ontwikkelen van een nieuwe wereldwijde standaard voor onderzoeksrapporten van serviceorganisaties. Deze standaard wordt voorlopig aangeduid als de *International Standard on Assurance Engagements (ISAE 3402) – Assurance Reports on controls at a Third Party Service Organization*.

De achterliggende doelstelling van de nieuwe standaard, die een volwaardig alternatief voor de SAS 70-standaard zal worden, is dat de onderzoeksrapporten bruikbaar zullen zijn voor een grotere groep belangstellenden en belanghebbenden. Bij de SAS 70-rapporten was de doelgroep beperkt tot het management en de auditor van de gebruikersorganisatie. Door het opnemen van meer typen interne beheersingsmaatregelen dan alleen de interne beheersingsmaatregelen gericht op financiële verslaglegging, zal een op ISAE 3402 gebaseerd rapport ook interessant zijn voor *die* serviceorganisaties waarvoor een SAS 70 tot op heden minder relevant was. Dit vanwege de nadruk op interne beheersingsmaatregelen gericht op financiële verslaglegging bij een SAS 70. Daarnaast is de ISAE 3402-standaard een internationale standaard die goed toepasbaar is binnen de al bestaande lokale controlestandaarden, zoals in Nederland de COS3000. Net zoals de SAS 70-standaard is de ISAE 3402-standaard *assertion based*, waarbij gebruikgemaakt wordt van controledoelstellingen ten aanzien van het object van onderzoek.

Het uitgangspunt bij het opzetten van ISAE 3402 is het behouden van de sterke punten van SAS 70 (zoals hiervoor beschreven in de subparagraaf 'SAS 70-standaard'). Dit betekent dat een rapport conform de ISAE 3402-standaard niet sterk zal afwijken van bestaande SAS 70-rapporten, omdat de meeste principes uit SAS 70 zijn overgenomen in het concept van ISAE 3402. Dit biedt zowel voor de gebruikersorganisatie als voor de serviceorganisatie een aantal voordelen, omdat de inspanning die voor de transitie van SAS 70 naar ISAE 3402 nodig is aan beide kanten beperkt kan zijn. Gezien de al genoemde beperkingen van de SAS 70-standaard is in ISAE 3402 een aantal aanvullingen op de SAS 70-standaard geformuleerd. De belangrijkste doelstellingen van de aanvullingen zijn ten eerste het doen toenemen van de bruikbaarheid van een rapport over de interne beheersingsmaatregelen van een serviceorganisatie en ten tweede het toevoegen van beheersingsmaatregelen die gerelateerd zijn aan de effectiviteit en efficiency van activiteiten/beheersingsmaatregelen – en door het toevoegen van beheersingsmaatregelen gerelateerd aan *compliance* met wet- en regelgeving. Door deze toevoegingen wordt de reikwijdte van het rapport vergroot.

De ISAE 3402-standaard kent twee typen rapporten die vergelijkbaar zijn met respectievelijk een SAS 70 Type I-rapport en een SAS 70 Type II-rapport:
- Type A-rapport;
- Type B-rapport.

In een Type A-rapport wordt alleen een oordeel gegeven over de opzet en het bestaan, terwijl in een Type B-rapport ook over de effectieve werking van de interne beheersingsmaatregelen gedurende een bepaalde periode een oordeel wordt gegeven. Er bestaat dan ook de verwachting dat een Type A-rapport in veel gevallen zal dienen als opstap naar een Type B-rapport. Uiteindelijk zal een Type B-rapport het meest voorkomen en zal deze voor de belanghebbenden het meest bruikbaar zijn.

Status ISAE 3402-standaard

Tot 31 mei 2008 had de ISAE 3402-standaard de status 'exposure draft' (conceptversie), wat betekent dat belangstellenden commentaar konden leveren op de conceptstandaard. Dit commentaar kan door de opstellers van de standaard worden gebruikt voor eventuele aanpassingen van de standaard. Het commentaar is op de website van de IAASB gezet. Wij hebben een korte selectie van de opmerkingen (van verschillende organisaties afkomstig) ten aanzien van de ISAE 3402-standaard op een rijtje gezet.

- De standaard geeft geen duidelijke richtlijnen over hoe dient te worden omgegaan met verschillende wetgevingen en jurisdicties, wat bijvoorbeeld bij *off shoring* van IT-dienstverlening van belang kan zijn.
- De ISAE 3402-standaard bevat mogelijkheden om materialiteit van belang te laten zijn bij het plannen en uitvoeren van de audit. Op zich is de toevoeging van materialiteit een verbetering ten opzichte van de SAS 70-standaard, waar een risicobenadering gebaseerd op risico's ten aanzien van financiële informatie of materialiteit ontbreekt. Materialiteit is echter een lastig begrip waarvoor nadere richtlijnen gewenst kunnen zijn.
- De criteria waaraan onder andere de beschrijvingen van de controls moeten voldoen, zijn (te) theoretisch van aard en sluiten niet aan bij de doelstellingen van het rapport. De SAS 70-standaard kent trouwens geen minimale set van criteria waaraan het internecontroleraamwerk moet voldoen.

De verwachting op het moment van dit schrijven is dat de IAASB het commentaar in maart 2009 heeft verwerkt en dat kort daarop de standaard definitief wordt uitgebracht. De verschillen en overeenkomsten tussen SAS 70 en ISAE 3402, zoals deze worden behandeld in dit artikel zijn dus gebaseerd op de voorlopige versie.

VERGELIJKING SAS 70- EN ISAE 3402-STANDAARD

Zoals aangegeven, komt ISAE 3402 op bepaalde punten sterk overeen met de SAS 70-standaard. We benoemen enkele overeenkomsten tussen SAS 70 en ISAE 3402.

Ondersteuning voor verschillende typen rapportages
Zowel de SAS 70-standaard als de voorgestelde ISAE 3402-standaard kent twee typen rapporten: een Type A-rapport over de *design* effectiviteit (opzet en bestaan) van controls en een Type B-rapport over de *operational* effectiviteit van controls (werking) over een bepaalde periode.

Gebruik van werkzaamheden internal audit
Beide standaarden maken het mogelijk gebruik te maken van een interne auditdienst bij het uitvoeren van de diverse procedures. Net als bij SAS

70, is het volgens ISAE 3402 niet toegestaan dat de auditor in het oordeel verwijst naar procedures die zijn uitgevoerd door internal audit. Het is wel toegestaan op werkzaamheden van internal auditors te steunen.

Toevoegen van steekproefomvang
Noch SAS 70, noch ISAE 3402 verplichten de serviceauditor de steekproefomvang toe te voegen, tenzij een relevante afwijking is vastgesteld.

Uiterlijk van het rapport
De opmaak en presentatie van een ISAE 3402-rapport is vergelijkbaar met een SAS 70-rapport.

Letter of representation
Beide standaarden verplichten het management tot het afgeven van een zogenoemde *letter of representation* aan de serviceauditor. Deze brief wordt niet ter beschikking gesteld aan de gebruikersorganisaties of de auditors daarvan.

Gebeurtenissen na afgifte van de verklaring
Beide standaarden verplichten de serviceauditor om zijn kennis over de beheersingsmaatregelen te actualiseren tot aan de datum van het uitbrengen van het rapport. Dit om vast te stellen of er gebeurtenissen zijn opgetreden die mogelijk het oordeel beïnvloeden of die om andere redenen zouden moeten worden gecommuniceerd met de gebruikers van het rapport.

We benoemen ook enkele verschillen tussen SAS 70 en ISAE 3402.

Verklaring van het management
Het ISAE 3402-rapport zal een verklaring van het management bevatten over het bestaan en effectief werken van de beheersingsmaatregelen. De verklaring wordt na het oordeel van de serviceauditor geplaatst. Momenteel bevatten SAS 70-rapporten alleen het oordeel van de serviceauditor en niet de verklaring van het management. Afhankelijk van de aard van de diensten die worden geleverd, kan de inhoud van de verklaring verschillen.

'De nieuwe ISAE 3402-standaard zal geen revolutie betekenen voor third party reporting'

Oordeel van de auditor
ISAE 3402 zal elke uitzondering in bestaan en werking samenvoegen in het uiteindelijke oordeel van de auditor. Terwijl SAS 70 deze concepten onderscheidt, is de IAASB van mening dat het samenvoegen van de twee begrippen bestaan en werking uiteindelijk meer bijdraagt aan het beoordelen van de interne beheersingsmaatregelen van de serviceorganisatie.

Beoordeling van de criteria
ISAE 3402 verplicht de serviceauditor om een beoordeling uit te voeren op de toereikendheid van de criteria die worden gebruikt door de serviceorganisatie voor het ontwikkelen van de omschrijving van het controleraamwerk, de beheersingsdoelstellingen en de gerelateerde beheersingsmaatregelen. De IAASB heeft voor een ISAE 3402-rapport in tegenstelling tot een SAS 70-rapport een minimale set van criteria gespecificeerd, waaraan het controleraamwerk moet voldoen. Het vaststellen van de controls, rekening houdend met deze *suitable criteria* blijft in de nabije toekomst dan ook complexe materie.

Verspreiding van het rapport
Het rapport is vertrouwelijk. Momenteel is de verspreiding van een SAS 70-rapport beperkt tot het management van de serviceorganisatie, de gebruikersorganisaties en de accountants van de gebruikersorganisaties. De IAASB heeft verdere beperkingen aangebracht, zodat de gebruikers van het rapport alleen de bestaande klanten van de serviceorganisatie zijn. Daarnaast moet de accountant van de gebruikersorganisatie voldoende kennis hebben van de wijze waarop de inhoud van het rapport wordt gerelateerd aan de beheersingsmaatregelen van de gebruikersorganisatie. Ten slotte wordt in ISAE 3402 in de auditorparagraaf een directe verwijzing gemaakt over het beoogde gebruik.

Relevantie van beheersdoelstellingen
In de huidige SAS 70-standaard is de eis opgenomen dat de beheersingsdoelstellingen in het rapport consistent zijn met beheersingsdoelstellingen die de serviceauditor relevant acht voor een jaarrekeningcontrole. De ISAE 3402-standaard bevat deze eis niet, waardoor het niet duidelijk is of de serviceauditor deze beoordeling moet gaan uitvoeren.

DE IMPACT OP EEN SERVICEORGANISATIE

Een serviceorganisatie die van plan is voor een of meer van de door haar uitgevoerde activiteiten een ISAE 3402-rapport te verstrekken, moet in de praktijk rekening houden met de hiervoor beschreven overeenkomsten en verschillen. Een belangrijk verschil met de SAS 70-standaard is dat in een rapport conform de ISAE 3402-standaard een verklaring van het management wordt opgenomen over het bestaan en effectief werken van de beheersingsmaatregelen. Deze door het management ondertekende verklaring is noodzakelijk alvorens het rapport uitgebracht kan worden. Afhankelijk van de aard van de diensten die worden geleverd, kan de inhoud van de verklaring verschillen. De IAASB heeft verschillende voorbeelden opgenomen in de voorlopige ISAE 3402-standaard. De ontwikkeling waarbij de gedachte dat compliance niet de primaire verantwoordelijkheid is van complianceafdelingen, interne auditdiensten en externe auditors, zet zich nu verder door in deze nieuwe standaard en maakt expliciet duidelijk dat het management van een organisatie verantwoordelijk is.

De serviceorganisatie gebruikt criteria voor het ontwikkelen van de omschrijving van het systeem, de beheersingsdoelstellingen en de gerelateerde beheersingsmaatregelen. Deze moeten voor de beoogde gebruikers van de rapportage specifiek, meetbaar en relevant zijn. Dit is een punt waarop veel commentaar is gekomen, omdat de minimale set van criteria die zijn gespecificeerd door de IAASB niet altijd toereikend lijken te zijn.

Ten slotte zal een internationale serviceorganisatie met meerdere locaties mogelijk een combinatie van SAS 70-rapporten en rapporten gebaseerd op lokale standaarden (zoals de Engelse AAF 01/06-standaard) moeten uitbrengen. Medewerkers van een serviceorganisatie die betrokken zijn bij dit rapportageproces zullen nauwkeurig de implementatie van de ISAE 3402-standaard binnen de eigen activiteiten moeten plannen.

GEVOLGEN VOOR SERVICE-ORGANISATIES EN IT-AUDITORS

Gezien de overeenkomsten tussen de SAS 70-standaard en de nieuwe ISAE 3402-standaard zullen de uiteindelijke werkzaamheden van de serviceorganisatie en de IT auditors van gebruikers- en serviceorganisaties niet wezenlijk veranderen. Net zoals vandaag de dag zullen risico's en beheersingsmaatregelen moeten worden geïdentificeerd, gedocumenteerd en getoetst worden door de IT-auditor die de verklaring afgeeft. Echter, er is geen vervanging voor het adequaat plannen van de auditactiviteiten; iedere serviceorganisatie die overweegt de ISAE 3402-standaard te implementeren, zal het implementatietraject moeten monitoren en de impact van de standaard moeten bespreken met haar auditor en interne auditafdelingen.

Een belangrijke wijziging ten opzichte van het SAS 70-rapport is de toevoeging van de beoordeling van de materialiteit. Zoals eerder aangegeven gaat het hier niet om de materialiteit van de jaarrekeningposten bij de gebruikersorganisatie, maar om de materialiteit ten aanzien van de informatie waarover wordt gerapporteerd. Hierbij moet het de auditor van de serviceorganisatie duidelijk zijn dat het assurancerapport informatie bevat die voor gebruikersorganisaties van (groot) belang is voor de betrouwbaarheid van financiële informatie van de gebruikersorganisaties.

Materialiteit (of risico-inschatting) ten aanzien van de beschrijvingen van de controls (opzet) is met name bedoeld om vast te stellen of de beheersingsmaatregelen meetbare criteria bevatten, waarmee beoordeeld kan worden of de opzet en het bestaan van de beheersingsmaatregel toereikend is. Van belang hierbij is onder andere dat geen belangrijke informatie in de controlebeschrijvingen wordt weggelaten waarmee de gestelde beheersdoelstellingen eventueel niet gehaald zouden worden. De belangrijkste opmerkingen in de commentaren op de exposure draft zijn gerelateerd aan de omschrijving van het begrip materialiteit; met name dat de omschrijving van materialiteit niet duidelijk genoeg was. De verwachting is dat het begrip 'materialiteit', zoals die wordt gebezigd in de definitieve versie van de ISAE 3402-standaard, dan ook nader (en beter) toegelicht zal worden.

CONCLUSIE EN AFSLUITING

Gelet op wat in de voorgaande paragrafen is besproken, zal de nieuwe ISAE 3402-standaard geen revolutie betekenen op het gebied van third party reporting. Het einde van SAS 70 is weliswaar in zicht, maar veel van de concepten en denkwijzen die in de SAS 70-standaard aanwezig waren, zien wij, al dan niet verpakt in een nieuw jasje, weer terug in de ISAE 3402-standaard. De verschillen die er zijn hebben met name te maken met het beter toepassen van de controls en het rapport daarover op de eisen vanuit de gebruikersorganisatie en het toevoegen van een *management assertion*. De verwachting is dus dat de transitie van de SAS 70-standaard naar de ISAE 3402-standaard geen wereldschokkende gevolgen met zich mee zal brengen. Desalniettemin zal deze transitie zorgvuldig uitgevoerd moeten worden en kunnen zowel de IT-auditors van de gebruikersorganisatie als van de serviceorganisatie hierbij een belangrijke rol vervullen om van deze transitie een succes te maken.

Kopieën van de uitgebrachte ISAE 3402- en ISA 402-standaarden zijn te vinden op de website: www.ifac.org. De informatie in dit artikel is gebaseerd op deze concepten. ■

Noten

1 Third party reporting wordt in deze context gezien als het proces van rapporteren door een onafhankelijke derde partij over de betrouwbaarheid van diensten en processen, uitgevoerd door een externe dienstverlener.
2 De beslissing van de gebruikersorganisatie om (ondersteunende) bedrijfsprocessen uit te laten voeren door een externe dienstverlener (serviceorganisatie).
3 Zie ook het studierapport *Normen voor de beheersing van uitbestede ICT-beheerprocessen* van de NOREA en het Platform voor Informatiebeveiliging.
4 COS 3000 is onderdeel van de 'Nadere voorschriften controle- en overige standaarden' van het NIVRA.

Drs. D. (Dennis) Houtekamer RE is als senior manager werkzaam voor Ernst & Young Advisory en heeft ruim ervaring met het uitvoeren en coördineren van onderzoeken die leiden tot *Third Party Reports*. Hij is het aanspreekpunt voor third party reporting binnen Ernst & Young in Nederland.

Drs. R.W. (Remco) de Graaf RE werkt als manager voor Ernst & Young Advisory en heeft ruime ervaring met third party-onderzoeken, zowel aan de uitvoerende kant als aan de klantzijde.