



# ISAE 3402: een nieuw hoofdstuk voor de IT-auditor

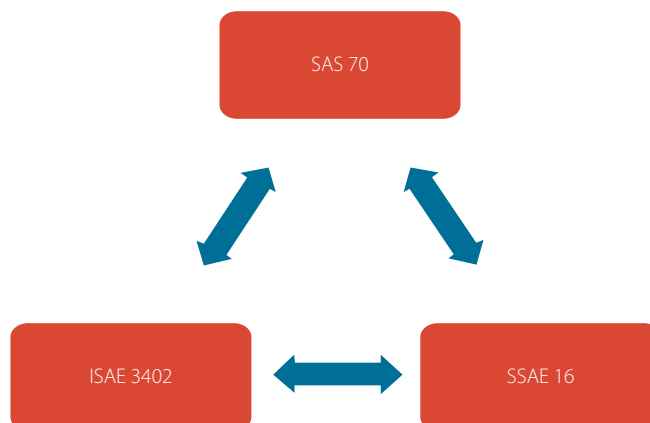
De SAS70-standaard is sinds jaar en dag dé internationale standaard voor het geven van zekerheid over uitbestede processen. Door de IAASB is eind december 2009 een nieuwe wereldstandaard opgesteld, ISAE 3402, die de SAS70-standaard vervangt. Deze nieuwe standaard is duidelijk gebaseerd op SAS70, maar brengt wel een aantal veranderingen met zich mee, zowel inhoudelijk als voor de IT-auditor specifiek. In dit artikel wordt ingegaan op de overeenkomsten en verschillen tussen de bestaande SAS70-standaard en de nieuwe ISAE 3402-standaard.

Het uitbesteden van (delen) van bedrijfs- of ondersteunende processen aan serviceorganisaties is een strategie die door veel bedrijven wordt gehanteerd. Met de invoering van de *Sarbanes Oxley* wet- en regelgeving zijn bestuurders zich echter meer bewust geworden van het feit dat zij toch eindverantwoordelijk blijven voor de uitbestede diensten. Daar uitbestede diensten ook belangrijk kunnen zijn voor de financiële verantwoording van de uitbesteder, is door de *American Institute of Certified Public Accountants* (AICPA) in 1992 een standaard opgesteld, waarin auditors aan auditors een verantwoording gaven over de kwaliteit van de uitbe-

stede processen. Dit werd de inmiddels zeer veel gebruikte SAS 70-standaard.

Op 18 december 2009 heeft de IAASB de nieuwe TPA-standaard gepubliceerd; de ISAE 3402 (*International Standard for Assurance Engagements*) [ISAE3402]. De publicatie van ISAE 3402 is niet de enige wijziging die doorgevoerd is rondom bestaande TPA-standaarden. Ook de SAS 70-standaard is inmiddels aangepast op de eisen zoals opgenomen in de ISAE 3402. De nieuwe Amerikaanse standaard heet *Statement on Standards for Attestation Engagements 16* (SSAE 16) en is in januari 2010 geaccordeerd door de ■

RENÉ EWALS



Figuur 1: Overzicht TPA-standaarden.



AICPA en gepubliceerd op 24 maart 2010 [SSAE16]. Zie ook figuur 1, waarin is aangegeven dat zowel de ISAE 3402 als SSAE 16 afstammen van SAS 70, doch dat de SSAE 16 is gebaseerd op de ISAE 3402-standaard.

In dit artikel wordt stilgestaan bij de achtergronden en invoering van ISAE 3402 en gaan we in op de verschillen met de bestaande en aankomende Amerikaanse standaarden. Hierbij wordt ervan uitgegaan dat de lezer basiskennis heeft van de huidige SAS 70-standaard. Voor een goed inzicht in de SAS 70-standaard wordt verwezen naar [EWAL09]. Achtereenvolgens komen aan de orde het tijdspad van invoering, de totstandkoming van ISAE 3402, de verschillen met bestaande SAS 70 en SSAE 16. Verder zullen we stilstaan bij de betekenis voor de bestaande praktijk en de IT-auditor. Tot slot volgt de conclusie.

### TIJDPAD VAN INVOERING

Hoewel de nieuwe ISAE 3402-standaard is gepubliceerd, is deze nog niet ingevoerd. De invoering van ISAE 3402 is verplicht voor perioden van onderzoek, waarin de datum 15 juni 2011 is inbegrepen. Het eerder conform ISAE 3402 rapporteren (*early adaptation*), wordt door de IAASB echter wel toegestaan.

De nieuwe ISAE-standaard moet eerst worden vertaald en geïntegreerd in de regelgeving voor auditors bij de leden van IFAC (*International Federation of Accountants*). Vanuit Nederland zijn hierbij NOREA en het NIVRA aangesloten. Voor de integratie in lokale regelgeving is vanuit NOREA en NIVRA aangegeven dat eind 2010 de definitief vertaalde tekst kan worden goedgekeurd op de algemene ledenvergadering. Door de nauwe samenwerking tussen de accountantsorganisaties in Nederland en België is het te verwachten dat er voor beide landen één vertaling beschikbaar komt.

### DE TOTSTANDKOMING VAN DE ISAE 3402

#### Van exposure draft naar finale standaard

De publicatie van deze nieuwe ISAE-standaard is niet de bekende donderslag bij heldere hemel. Al enige tijd wordt door de IAASB gewerkt aan deze standaard. Zie ook een eerder artikel over ISAE 3402 in de IT-auditor [HOUT09]. In 2008 is een zogenaamde *exposure draft* gepubliceerd, waarop kon worden gereageerd. Ook bevatte de exposure draft een aantal specifieke vragen waarop de IAASB een antwoord zocht. Van de mogelijkheid om te reageren, heeft een groot aantal organisaties gebruikgemaakt. Vanuit Nederland heeft een gecombineerde werkgroep van NOREA/NIVRA een reactie gestuurd en elk van de grote accountantskantoren (Big Four) heeft zelfstandig gereageerd, veelal via het internationale hoofdkantoor. Voorts heeft een aantal serviceorganisaties in Nederland van de gelegenheid gebruikgemaakt hun visie kenbaar te maken.

De reacties die IAASB heeft ontvangen, hebben geleid tot een aantal substantiële wijzigingen in de definitieve standaard. Hierdoor moet bijzondere voorzichtigheid worden betracht met het interpreteren van publicaties over ISAE 3402, als deze zijn opgesteld vóórdat de definitieve standaard is gepubliceerd. Relevant te noemen aspecten hierbij zijn:

- de reikwijdte van het rapport. Deze is nu veel strikter dan in de exposure draft en beperkt tot processen en beheersmaatregelen gerelateerd aan de jaarrekeningcontrole (*relevant for financial reporting*) voor de user organisatie;
- de zekerheid die wordt gegeven is nu alleen nog 'redelijke' zekerheid;
- het opnemen van een specifieke link met ISA 3000;
- werkzaamheden uitgevoerd door een Interne Audit-afdeling moeten expliciet zichtbaar worden gemaakt in het rapport;

- dat mededelingen niet meer tevens kunnen worden afgegeven over een zogenaamd interne *Shared Service Centre*.

Dit artikel is gebaseerd op de gepubliceerde definitieve tekst.

#### Aanpassingen aan de finale standaard

Op 29 januari 2010 heeft de IAASB in een persbericht laten weten, dat het woord *only* in de definitieve en gepubliceerde standaard in paragraaf 3b tot verwarring kan leiden bij de interpretatie. Met name rondom de door IAASB vastgestelde reikwijdte. Door IAASB-medewerkers is onderzoek gedaan en vastgesteld dat het betreffende woord inderdaad een fout is en niet in paragraaf 3b had moeten staan, doch in 3a [IAASB]. Hieronder staat de tekst met 'only' in *bold* op de juiste plaats en in doorgestreepte tekst de oorspronkelijk doch foute plaatsing.

3. *This ISAE applies only when the service organization is responsible for, or otherwise able to make an assertion about, the suitable design of controls. This ISAE does not deal with assurance engagements:*

- (a) To report **only** on whether controls at a service organization operated as described, or
- (b) To report *only* on controls at a service organization other than those related to a service that is likely to be relevant to user entities' internal control as it relates to financial reporting (for example, controls that affect user entities' production or quality control).

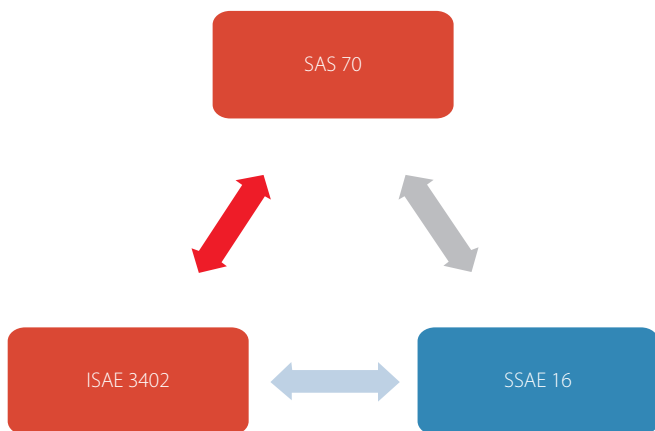
*This ISAE, however, provides some guidance for such engagements carried out under ISAE 3000.5 (Ref: Para. A2) [IAASB]*

Deze nieuwe tekst is inmiddels opgenomen in de definitieve tekst zoals te vinden op de website van IFAC. Niettemin zijn er nog foutieve teksten in omloop.

### VERSCHILLEN MET DE BESTAANDE SAS 70

#### Redelijke zekerheid

Binnen de structuur van de internationale regelgeving vanuit de IAASB worden twee soorten zekerheid gehanteerd: redelijke zekerheid en beperkte zekerheid. Bij een ISAE 3402 moet een positief verwoorde



Figuur 2: Verschillen met de bestaande SAS 70

conclusie worden gebruikt door de auditor en er kan derhalve alleen redelijke zekerheid worden gegeven, hetgeen ook zo specifiek in de standaard is opgenomen.

Voorts worden binnen de internationale regels twee wijzen van rapporteren gehanteerd: *direct reporting* en *assertion based reporting*.<sup>1</sup> In dit kader heeft de IAASB gemeend een specifieke mengvorm te moeten kiezen voor de ISAE 3402 rapportage, althans wat betreft de mededeling van de auditor. De nieuwe standaard maakt gebruik van de assertion based-rapportage, maar de mededeling zelf, de opinie, moet worden geformuleerd als een direct reporting-conclusie. Dat geldt ook voor de uitvoering van de werkzaamheden.

### Management mededeling

Een belangrijke wijziging is dat ook het verantwoordelijke management een mededeling (*management assertion*) moet opnemen in het ISAE 3402-rapport. In deze mededeling worden onder meer de volgende zaken opgenomen:

- Voor wie het rapport bedoeld is (reikwijdte).
- De beschrijvingen in het rapport zijn *fair* en gelden voor de transacties in de periode van onderzoek (bij een type 2), waarbij specifiek is

opgenomen welke services, transacties onderdeel zijn van het rapport. Voorts worden elementen opgenomen zoals de beheersomgeving, het risicobeheerproces, informatie en communicatie alsmede de *control activities*. Kortom, de relevante aspecten van het COSO-model.

- Dat de beheersmaatregelen die de bijbehorende beheersdoelstellingen afdekken, adequaat zijn ontworpen en hebben gewerkt in de periode. Hierbij zijn de volgende criteria in ogenschouwen genomen:
  - De risico's die een bedreiging vormen voor het behalen van de beheersdoelstellingen.
  - De beschreven beheersmaatregelen, indien die effectief hebben gewerkt, geven redelijke zekerheid dat de onderkende risico's het behalen van de beheersdoelstellingen niet verhinderen.
  - De beheersmaatregelen consequent zijn uitgevoerd door medewerkers met de vereiste vaardigheden en autoriteit.

De Engelse tekst van de mededeling door het management is opgenomen als bijlage 1 in de standaard. Deze verplichte toevoeging aan het rapport is mogelijk de meest zichtbare wijziging ten opzichte van een SAS 70-rapport en geeft goed invulling

aan de verantwoordelijkheid van het management en de transparantie die ermee wordt bereikt. Een mededeling van het management is overigens ook mogelijk bij een SAS 70-rapport, doch hiervan wordt in weinig gevallen gebruik gemaakt.

Ook is expliciet in de ISAE opgenomen dat, ondanks dat de auditor een opinie geeft over de effectieve werking, het management dat niet mag gebruiken om haar eigen opinie daarop te baseren. Van het management wordt verwacht, dat het monitoren van beheersmaatregelen plaatsvindt om de effectieve werking van beheersmaatregelen vast te kunnen stellen. Dit omvat onder meer dat rapportering van uitzonderingen plaatsvindt alsmede tijdige correcties plaatsvinden en dat de effectiviteit wordt beoordeeld. Monitoring kan plaatsvinden door continue activiteiten, door separate evaluaties of een combinatie van deze twee. De auditor zal ten behoeve van zijn werkzaamheden moeten vaststellen, op basis van welke elementen het management tot de conclusie is gekomen zoals verwoord in de management mededeling.

### De zogenaamde *suitable criteria*

In overeenstemming met ISAE 3000 moet de service auditor beoordelen of de serviceorganisatie de juiste criteria heeft gebruikt om de beschrijving van het systeem van interne controle op te stellen, of de beheersmaatregelen adequaat zijn ontworpen en of de beheersmaatregelen effectief werken (deze laatste uiteraard alleen voor een type 2-rapport). In de ISAE-standaard is daarbij opgenomen, welke minimumcriteria door de service auditor moeten worden beoordeeld. De door de auditor toegepaste minimumcriteria moeten ook in het rapport worden opgenomen. Waarschijnlijk worden deze criteria opgenomen in wat nu de sectie III van een SAS 70 rapport is, waarin de service auditor beschrijft welke



werkzaamheden zijn uitgevoerd en welke conclusies daaruit zijn getrokken. De volgende criteria worden genoemd:

- *Fairness of presentation*: dit moet omvatten alle elementen die relevant zijn voor de gebruikersorganisaties, zoals de reikwijdte van de inhoud van het rapport, en voldoende detailniveau in de beschrijvingen.
- *Suitability of design*: de beheersmaatregelen passen bij de beheersdoelstellingen en de beheersmaatregelen behalen de doelstelling. De opstelling van het management in het rapport moet op basis van een risicoanalyse tot stand zijn gekomen.
- *Effectieve werking*: toetsing over een periode dat de maatregelen effectief hebben gewerkt.

### Sub-serviceorganisaties

Indien een serviceorganisatie op zichzelf weer een deel van de processen heeft uitbesteed aan een andere partij, is er sprake van een sub-serviceorganisatie. Indien dat deel van de processen bij de sub-serviceorganisatie significant is voor de gebruikersorganisatie moeten deze worden opgenomen in het rapport. Dit wordt ook wel de *inclusive*-methode genoemd. Dat was althans de wijze waarop dit is verwoord in de SAS 70-standaard. In de nieuwe ISAE 3402-standaard wordt hiervan afgeweken, aangezien er niet wordt gesproken over de significantie van de processen bij de sub-serviceorganisatie voor de gebruikersorganisatie. Wat dit betekent voor het gebruiken van de *inclusive* methode of de *carve out*-methode (hierbij wordt de sub-serviceorganisatie niet meegenomen in het rapport) op basis van significantie voor de gebruikersorganisatie, is niet geheel duidelijk. Wel wordt door de IAASB in de toelichting op de ISAE 3402 aangegeven dat mogelijk de *inclusive* methode in de praktijk alleen kan worden toegepast indien de auditors van hetzelfde bureau zijn.

De ISAE 3402 stelt heel duidelijk dat, indien sprake is van de *inclusive* methode, de gehele beschrijving (niet alleen de beheersdoelstellingen en -maatregelen) van de sub-serviceorganisatie integraal moet worden opgenomen in het rapport. Dat geldt ook voor de mededeling van het management van de sub-serviceorganisatie. Voorts stelt ISAE 3402 dat, in geval van een *carve out* alle beheersmaatregelen die de serviceorganisatie heeft ingericht om zeker te stellen dat de relevante beheersmaatregelen bij de sub-serviceorganisatie effectief werken, in het rapport moeten worden opgenomen. Bijvoorbeeld dat de inhoud van een *assurance* rapport van de sub-serviceorganisatie wordt beoordeeld door de serviceorganisatie.

Voorbeelden van andere mogelijkheden zijn:

- dat eigen audits worden verricht;
- dat regelmatig overleg wordt gevoerd met de sub serviceorganisatie over de kwaliteit en beheersmaatregelen die worden uitgevoerd;
- de interne organisatie van de serviceorganisatie om de kwaliteit van de processen uitgevoerd door de sub serviceorganisatie te beheersen.

### Steunen op Interne Audit afdelingen

Onder de huidige SAS 70-standaard kan op twee wijzen gebruik worden gemaakt van de werkzaamheden van een Interne Audit afdeling [EWAL09]:

1. Met de zogenaamde *direct assistance*, waarbij de medewerker van de afdeling Interne Audit wordt ingezet alsof hij/zij onderdeel is van het auditteam.
2. Om de *nature, timing and extent* van de service auditor aan te passen op door Interne Audit uitgevoerde werkzaamheden.

In de nieuwe ISAE 3402-regelgeving wordt dat onderscheid niet genoemd en wordt alleen gesproken over de mogelijkheid, genoemd

onder punt 2. De reden waarom de *direct assistance* niet is opgenomen, is onbekend. Met dien verstande dat hierbij is aangesloten bij de huidige formuleringen van COS610 (ISA 610), waarin dit onderscheid momenteel ook niet wordt gemaakt. Inmiddels is in juli 2010 door de IAASB een exposure draft gepubliceerd "ISA 610 Using the work of Internal Auditors". In deze exposure draft is wel expliciet tekst opgenomen rondom de 'direct assistance' vanuit een afdeling Interne Audit. Deze nieuwe regelgeving wordt naar verwachting in definitieve vorm gepubliceerd in september 2011 en ingevoerd in december 2013.

Een ander belangrijk verschil met SAS 70 is dat de service auditor specifiek melding dient te maken van de werkzaamheden die zijn uitgevoerd door de Interne Audit-afdeling. Dit is bijvoorbeeld conform de huidige Britse AAF/01-standaard voor financiële instellingen, maar geheel anders dan onder SAS 70 het geval is. Wel is specifiek opgenomen, dat de tekenende auditor geheel en ongedeeld verantwoordelijk is voor zijn deel van het rapport. De verantwoordelijkheid voor de uitgevoerde werkzaamheden en de opinie wordt niet gedeeld met de Interne Audit afdeling.

In de nieuwe standaard is, evenals onder SAS 70, niet omschreven in welke mate gebruik mag worden gemaakt van de werkzaamheden van een afdeling Interne Audit. Hierbij doet zich de vraag gelden of de invulling hiervan aan individuele eindverantwoordelijken of aan kantoren wordt overgelaten of dat richtlijnen worden ontwikkeld door NOREA/NIVRA, waarin wordt opgenomen wat de minimum te verrichten werkzaamheden zijn door de service auditor. Over het algemeen moet de service auditor 'toereikende' *assurance*-informatie verzamelen om tot zijn oordeel te kunnen komen.

In de COS610 is hierover het volgende opgenomen [COS610]:

‘De aard, timing en omvang van de controlewerkzaamheden die worden uitgevoerd op specifieke werkzaamheden van de interne auditors zullen afhangen van de inschatting door de externe accountant van het risico van een afwijking van materieel belang, van de evaluatie van de interne auditfunctie, alsmede van de evaluatie van de specifieke werkzaamheden van de interne auditors.

Dergelijke controlewerkzaamheden kunnen omvatten:

- Het onderzoeken van items die reeds door de interne auditors zijn onderzocht.
- Het onderzoeken van andere soortgelijke items; het observeren van werkzaamheden die door de interne auditors zijn uitgevoerd.’

Voordat kan worden gesteund op de werkzaamheden uitgevoerd door de afdeling Internal Audit moeten de volgende aspecten worden beoordeeld:

- De kwaliteit van de afdeling.
- In welke mate de verrichte of te verrichten werkzaamheden relevant zijn.
- De impact van de werkzaamheden op de aard, timing en omvang van de werkzaamheden, waarbij in ogenschouw wordt genomen:
  - De aard en reikwijdte van verrichte of te verrichten werkzaamheden.
  - De significantie van de werkzaamheden voor de conclusies van de externe IT-auditor.
  - De mate van subjectiviteit die is toegepast bij de beoordeling van het bewijsmateriaal.

### Risico analyse

Nieuw ten opzichte van SAS 70 is dat beheersdoelstellingen moeten voortkomen uit een set van beheersmaatregelen die tot doel hebben een risico te vermijden. De serviceorganisatie is verantwoordelijk voor het tijdig onderkennen van risico's en het

nemen van de juiste en passende acties op de risico's. Hierbij kan de serviceorganisatie gebruikmaken van een formeel of informeel proces om relevante risico's te identificeren. Een formeel proces houdt mogelijk in dat de risico's worden ingeschat op basis van significantie, kans op voorkomen en het implementeren van maatregelen die de risico's afdekken. Voorts is specifiek opgemerkt in de ISAE-standaard, dat een degelijk proces om beheersdoelstellingen te formuleren op zichzelf reeds een informeel proces betekent om risico's in te schatten.

Vanuit de ISAE-standaard wordt een risicoanalyse zelf niet verplicht gesteld. Niettemin kan de IT-auditor de cliënt wel ondersteunen of adviseren indien de IT-auditor van mening is dat het uitvoeren van een (in)formele risicoanalyse belangrijk is. Uiteraard moet daarbij wel de blijvende onafhankelijkheid in acht worden genomen, indien de IT-auditor ook als externe auditor de ISAE 3402-mededeling gaat afgeven.

### Representatiebrief

Bij de huidige SAS 70-regelgeving is een representatiebrief die door het verantwoordelijke management van de serviceorganisatie wordt getekend en aan de auditor is geadresseerd niet verplicht. Sommige organisaties vereisen dat wel, andere niet. Bij de ISAE 3402 is een representatiebrief een verplicht onderdeel van de audit. Met deze brief, gericht aan de auditor, geeft het management aan alle informatie te hebben verstrekt aan de auditor die relevant is in het kader van zijn werkzaamheden. Tevens moet het management hierin de afgegeven management mededeling nogmaals bekrachtigen.

Specifiek in ISAE 3402 is opgenomen, dat ook een representatiebrief moet worden verstrekt door het management van een zogenaamde sub-serviceorganisatie aan de service auditor. Uiteraard alleen indien de

sub-serviceorganisatie binnen de reikwijdte van het onderzoek valt (inclusive methode).

De ISAE 3402 bevat zelf geen voorbeeld van een goede representatiebrief.

### Verspreiding van het rapport

Over de verspreiding van het rapport is opgenomen, dat de beoogde gebruikers het management van de serviceorganisatie, de user organisatie en de accountants van de user organisatie betreffen. Met de term 'beoogd' (*intended*) wordt mogelijk ruimte geschapen om de verspreiding ruimer op te vatten, dan onder de huidige SAS 70-standaard, hoewel in een toelichtende beschrijving door IAASB wordt aangegeven dat dit niet de bedoeling is. Met de beoogde gebruikers wordt bedoeld: die personen die de inhoud van het rapport op zijn merites kunnen beoordelen. Om die reden is in de mededeling ook opgenomen dat het rapport bedoeld is voor de gebruikersorganisatie en de auditor van deze organisatie. In alle gevallen is het verstandig van de tekenende service auditor om vooraf met de cliënt afspraken te maken over de verspreiding van het rapport (hetgeen ook conform bestaande NOREA-standaarden is).

De ISAE 3402-rapportage is derhalve niet bedoeld voor het maatschappelijk verkeer, zodat publicatie van het rapport met mededeling op bijvoorbeeld Internet niet is toegestaan.

### Mededeling auditor

De mededeling die door de IT-auditor wordt afgegeven, sluit nu beter aan op de formuleringen zoals die gebruikelijk zijn in accountantsverklaringen en is nu beter gestructureerd vergeleken met de bestaande SAS 70-standaard. De volgende elementen moeten worden opgenomen in de mededeling:

- Reikwijdte van het rapport.
- De verantwoordelijkheden van de serviceorganisatie.
- De verantwoordelijkheden van de service auditor. ▣



- De beperkingen die samenhangen met de beheersmaatregelen bij serviceorganisaties.
- De opinie.
- Een verwijzing naar de beschrijving van de beheersmaatregelen.
- Bedoelde gebruikers van het rapport.

De opinie zelf bestaat uit twee (type 1) of drie (type 2-mededeling) aspecten:

- De beschrijving is *fair*, zoals ontworpen en geïmplementeerd per [datum] of gedurende de periode.
- De beheersmaatregelen gerelateerd van de beheersdoelstellingen zijn adequaat ontworpen per [datum] of gedurende de periode.
- De beheersmaatregelen bieden redelijke zekerheid dat de beheersdoelstellingen worden bereikt gedurende de periode.

In de opinie wordt een uitspraak gedaan over de gehele beschrijving in het rapport (*presentation of the description*), over het gebruik van gepaste beheersdoelstellingen (*suitability of the objectives*), en of de gehanteerde criteria die door het management zijn gebruikt, passen bij het rapport (*suitability of the criteria specified by the service organization*).

Is dat anders dan bij de bestaande SAS 70? In de meeste opzichten niet, hoewel in de ISAE wordt gesproken over een ontwerp en implementatie gedurende de periode. Bij SAS 70 was dat altijd vanaf een bepaalde datum. Voorts werd in de SAS 70-mededeling niet gerefereerd aan criteria die zijn gebruikt bij het opstellen van het rapport.

#### De reikwijdte van ISAE 3402

De SAS 70-standaard was heel bewust opgesteld als *auditor to auditor*-rapportage met als reikwijdte de processen binnen de serviceorganisatie die relevant zijn voor de *financial reporting* van de user organisatie. De reikwijdte van de ISAE is in de definitieve versie niet anders, ondanks de tendens van verruiming in de *exposure draft*. Wel is door de IAASB de deur opengezet voor een grotere reikwijdte door in de ISAE-teksten op te nemen, waarin is aangegeven dat beheersmaatregelen rondom *operations* van de serviceorganisatie en *compliance* met wet- en regelgeving ook relevant kunnen zijn voor de financial reporting van de user organisatie. In de toelichting door de IAASB is daarbij aangegeven dat over enkele jaren (2013) zal worden geëvalueerd hoe deze opening is ingevuld in de praktijk. Zie voor de reikwijdte ook wat hierover eerder in

de tekstbox in de paragraaf 'De totstandkoming van de ISAE 3402' is vermeld.

#### VERSCHILLEN MET DE NIEUWE SSAE 16

Op 24 maart jongstleden heeft de AICPA de definitieve opvolger van de SAS 70-standaard gepubliceerd. De standaard is een Statement on Standards for Attestation Engagements en wordt in het kort aangeduid als SSAE 16 [SSAE16]. Deze opvolger van de SAS 70 is tot stand gekomen in nauw overleg met de *Task Force* van de IAASB die de ISAE 3402-standaard heeft opgesteld, SSAE 16 is sterk gebaseerd op ISAE 3402, maar heeft op punten een uitwerking gekregen die past binnen de Amerikaanse wet- en regelgeving.

Naar verwachting stappen in Nederland de meeste organisaties over naar ISAE 3402. Niettemin kunnen internationaal opererende organisaties, en dan zeker indien zaken worden gedaan met en in Amerika, overwegen om gebruik te maken van de SSAE 16 standaard.

De SSAE 16 standaard heeft heel veel overeenkomsten met de ISAE 3402, doch de volgende verschillen kunnen hier worden aangeduid [SSAE16]:

#### Intentional acts

Zowel binnen ISAE als SSAE moet de auditor de *nature* en *cause* onderzoeken van afwijkingen tussen beschreven beheersmaatregel en de vastgestelde uitvoering van controles. Echter, binnen de SSAE moet de auditor ook aandacht geven aan het risico, dat de beschrijving van de serviceorganisatie niet *fairly represented* is en of beheersmaatregelen mogelijk niet goed zijn ontworpen of effectief werken. Ook bevat de SSAE een vereiste dat het management van de serviceorganisatie schriftelijk aan de auditor verklaart dat alle bekende of vermoede *intentional acts* door medewerkers van de



Figuur 3: Verschillen met de nieuwe SSAE 16

serviceorganisatie zijn gemeld aan de service auditor.

#### *Anomalies*

De ISAE-standaard opent de mogelijkheid om een gevonden uitzondering (*deviation*) te betitelen als een anomalie, een gebeurtenis die ver buiten de verwachting ligt. Dit is mogelijk door nader onderzoek te verrichten naar de gevonden uitzondering en vervolgens met een hoge mate van zekerheid te concluderen, dat de gevonden uitzondering niet representatief is voor de populatie. De SSAE stelt, dat alle gevonden uitzonderingen moeten worden gezien en geëvalueerd door te kijken naar de aard (*nature*) en oorzaak (*cause*) van de uitzondering. Voorts is in de SSAE overwogen om bepaalde woorden en woordcombinaties niet over te nemen, daar deze in de verdere regelgeving in Amerika niet worden gebruikt.

#### *Direct Assistance*

Dit betreft directe ondersteuning door een Internal Auditor als ware hij een onderdeel van het audit team. Zoals eerder verwoord in dit artikel is dit momenteel niet opgenomen in de ISAE 3402-standaard.

#### *Subsequent events*

Indien relevante gebeurtenissen na de periode van onderzoek en vóór afgifte van het rapport niet door het management worden opgenomen in de beschrijving, neemt de auditor de gebeurtenis op in zijn mededeling. Tevens geldt, dat de auditor moet afwegen wat de invloed is op de eigen mededeling en de management assertions, indien gebeurtenissen bekend worden na afgifte van de mededeling, doch wel bestonden voor de mededeling werd afgegeven.

#### *Restriction of use*

SSAE is strenger en preciezer in de bewoordingen voor wie het rapport is bedoeld: management van de user organisatie alsmede de auditors van de user organisatie. ISAE gebruikt

de woorden *intended* in plaats van *restricted* zoals SSAE.

#### *Documentation completion*

Voor het completeren van de documentatie houdt ISAE geen specifieke termijn aan, terwijl de SSAE een termijn van zestig dagen na de datering van de mededeling hanteert.

#### *Engagement Acceptance & Continuance*

Een specifieke voorwaarde voor engagement acceptatie en continuïteit binnen SSAE is dat het management van de serviceorganisatie akkoord is met het afgeven van een representatiebrief aan het einde van de opdracht. ISAE heeft dit vereiste niet opgenomen.

#### *Disclaimer of opinion*

In de SSAE is specifiek opgenomen, dat de auditor afziet van een mededeling indien het management geen representatiebrief ondertekent. Ook kan de auditor de opdracht teruggeven. ISAE geeft aan, dat de weigering ertoe leidt, dat de auditor de opdracht teruggeeft. Als alternatieven zijn gegeven: het niet afgeven van de mededeling of het openbaar maken van de weigering in de mededeling. Welke van de twee alternatieven wordt gekozen, is mede afhankelijk van de lokale wet- en regelgeving.

#### *Elements in SSAE that are not required in ISAE 3402*

Enkele specifieke formuleringen moeten in een SSAE-rapport worden opgenomen, die een aanvulling zijn op de vereisten in een ISAE rapport. Zie voor de details [SSAE16].

In zijn algemeenheid geldt dat de SSAE in een aantal gevallen de auditor meer *guidance* geeft voor de uitvoering van de werkzaamheden. Daar staat tegenover, dat de ISAE de auditor iets meer vrijheid van handelen toestaat. Maar de verschillen zijn niet groot.

## BETEKENIS VOOR DE BESTAANDE PRAKTIJK EN DE IT-AUDITOR

### Verbeterde transparantie en uniformiteit

Met de invoering van de nieuwe ISAE 3402 wordt niet alleen een nieuwe standaard geïntroduceerd, maar ook meer uniformiteit gecreëerd. Hiervoor bestaat een aantal redenen:

- ♦ Een betere transparantie. In het rapport staat vermeld dat de directie ook verantwoordelijkheid neemt voor de beheersmaatregelen en zelfstandig tot een conclusie komt.
- ♦ Het uitsluiten van verwarring of een rapport een SAS 70- of een ISA 3000-rapport is. Nu zijn rapporten beschikbaar waarvan de serviceorganisatie meent, dat het een SAS 70, type 2-rapport is, maar als de mededeling goed wordt gelezen, dan blijkt sprake te zijn van een ISA 3000-rapport. Zie kader 'Voorbeeld SAS 70 rapport of toch ISAE 3000 rapport?'
- ♦ Een uniforme vertaling. De verwachting is dat met een uniforme vertaling van de standaard in het Nederlandstalige werkgebied, alle kantoren dezelfde tekst gebruiken voor de mededeling van de auditor en het management statement. Op dit moment hebben alle kantoren hun eigen versie van de Nederlandstalige SAS 70-mededeling.
- ♦ Het opnemen van criteria. De criteria die door de service auditor moeten worden gebruikt bij de beoordeling of de beschrijving door de serviceorganisatie, voldoen aan de eisen en zijn ook expliciet opgenomen in de standaard. Voorts moeten deze worden opgenomen in het rapport.

Bovenstaande voordelen leiden hopelijk ook tot een nog hogere acceptatiegraad bij serviceorganisaties alsmede user organisaties en hun auditors. Hierbij speelt mogelijk ook een rol, dat de bestaande



COS 402 vanuit het NIVRA recentelijk is aangepast en in werking treedt voor boekjaren vanaf 15 december 2009. In de COS 402 is opgenomen welke werkzaamheden de controlerend accountant moet uitvoeren indien de user organisatie activiteiten heeft uitbesteed. De nieuwe COS 402 is qua formuleringen, bewoordingen en beschrijvingen helemaal ingericht op ISAE 3402.

### Betekenis voor cliënten

Ook voor de ontvangers van de TPA-rapportage op basis van ISAE 3402 zijn de beschreven voordelen in de vorige paragraaf van toepassing. In aanvulling daarop kan nu het management ook zichtbaar maken dat zij verantwoordelijk zijn voor de adequate beheersing van de onderneming. Overigens was die mogelijkheid ook aanwezig binnen de bestaande SAS 70-rapporten, maar bestond geen gestandaardiseerde mededeling.

### Tekenbevoegdheid voor de IT-auditor

We gaan meer TPA-rapporten zien die worden getekend door de IT-auditor met de invoering van ISAE 3402. Immers, de ISAE 3402 wordt opgenomen in de standaarden voor de IT-auditor. Voorts is inmiddels in de Nadere Regelgeving van het NIVRA opgenomen dat een accountant kan en mag steunen op de werkzaamheden verricht door een Register IT-auditor (RE). Ook is de NOREA geassocieerd lid van IFAC.

Ten behoeve van de uitvoering van opdrachten onder ISAE 3402 is het wel vereist, dat de IT-auditor beschikt over de competenties om de opdracht uit te voeren. Dit geldt overigens voor alle opdrachten die door de RE worden uitgevoerd. Voorts geldt dit ook voor de accountant.

### Opleiding tot IT-auditor

De ISAE 3402-rapporten zijn weliswaar niet geschikt noch bedoeld voor het maatschappelijk verkeer,

wel zal door de nieuwe regelgeving meer zichtbaar worden, dat de IT-auditor een toegevoegde waarde kan leveren bij TPA-rapporten. Door zijn uitgebreide kennis van IT en de daaraan gekoppelde geautomatiseerde beheersmaatregelen in applicaties, kennis van risicobeheersing en administratieve organisatie en interne controle kan hij als geen ander de brug slaan tussen IT en de reguliere bedrijfsprocessen.

Doordat het belang van de IT-auditor toeneemt, zal de beroepsgroep ook goed moeten kijken in hoeverre de curricula van de postinitiële opleidingen tot IT-auditor voldoende aandacht besteden aan vakken als Audit-vaardigheden en Administratieve Organisatie/Interne Controle. Immers, door het toegenomen belang van de werkzaamheden van de IT-auditor, indirect ook binnen het maatschappelijke verkeer, zal hij vaker dan voorheen de eindverantwoordelijkheid moeten kunnen dragen. Daarbij horen voldoende prudentie en precisie bij de uitvoering van de werkzaamheden.

### CONCLUSIE

De belangrijkste praktische wijziging in ISAE 3402 is de verbeterde transparantie, door de toevoeging van een mededeling door het management in het rapport. Hierdoor wordt nog beter zichtbaar, dat het management verantwoordelijk is voor de beschrijving en de beheersdoelstellingen en -maatregelen in het rapport.

Daarnaast brengt deze ISAE standaard een belangrijke wijziging voor de IT-auditor teweeg. Door de aansluiting bij IFAC, kan de IT-auditor deze rapporten tekenen en door de aanpassing van de Nadere Regelgeving binnen het NIVRA wordt de beroepsgroep gezien als een op wiens oordeel kan worden vertrouwd. Dat is een belangrijke stap vooruit voor het beroep. ■

### Voorbeeld SAS 70 rapport of toch ISAE 3000 rapport?

Op de voorkant van het rapport staat het volgende:

#### STATEMENT ON AUDITING STANDARDS 70

Type II statement — Report on control activities placed in operation and test of operating effectiveness of [client] for the period January 1, 2009 — December 31, 2009

#### Report date: February 3, 2010

In de mededeling van het rapport staat het volgende:

#### Scope

We conducted our examination in accordance with the Dutch law, including Standard 3000, 'Assurance-engagements other than audits and reviews of historical financial information' and supplemented by the American Institute of Certified Public Accountants' Statement on Auditing Standards No. 70 Service Organizations, its interpretations and amendments and by other procedures deemed necessary in the circumstances. This law requires that we plan and perform our examination to obtain reasonable assurance that:

- (1) the description in section III of the accompanying SAS 70 report is adequate;
- (2) the internal controls were suitably designed for achieving the objectives set by management;
- (3) these controls were in operation on December 31, 2009;
- (4) the internal controls operate effectively over the period.

Hier lijkt sprake te zijn van een SAS 70 rapport en de kaft alsmede de bewoordingen suggereren dat ook, echter de werkzaamheden zijn uitgevoerd conform de COS 3000. Dus toch geen SAS 70 rapport, maar een Assurance rapport. Wat precies de rol van SAS 70 is geweest bij de uitvoering van deze opdracht is niet duidelijk. Met de invoering van ISAE 3402 zou deze onduidelijkheid tot het verleden moeten behoren.

## Literatuur

[AU322] AU Section 322, the auditor's consideration of the Internal Audit Function in an audit of Financial Statements (SAS 65).

[COS610] Gebruikmaken van de werkzaamheden van Interne Auditors.

[EWAL09] Drs R.Ch.T. Ewals RE, *Zekerheid bij uitbesteding*, Handboek IT-Auditing, februari 2009.

[HOUT09] Dennis Houtekamer en Remco de Graaf, *ISAE 3402: einde van SAS 70 in zicht?*, De EDP-auditor, nummer 1, 2009.

[IAASB] Memo IAASB staff, *Correction of Drafting Error in ISAE 3402*, 29 January 2010.

[ISAE3402] ISAE 3402, *Assurance Reports on Controls at a Service Organization*, International Auditing and Assurance Standards Board, December 2009.

[SAS 70] AICPA Audit Guide, *Service organizations: applying SAS No.70, as amended, with conforming changes as of May 1, 2009*.

[SSAE16] Statement on Standards for Attestation Engagements, Auditing Standards Board, AICPA, *Reporting on controls at a service organization*, March 2010.

## Noot

1 Direct reporting: de auditor formuleert de mededeling op basis van eigen uitgevoerde werkzaamheden en normenkader. Assertion based reporting: de auditor formuleert de mededeling op basis van door management uitgevoerde werkzaamheden en refereert aan normenkader management.



**Drs. R.Ch.T. (René) Ewals RE** is als directeur binnen ADEIA B.V. verantwoordelijk voor de dienstverlening rondom het geven van zekerheid ten behoeve van derde partijen (*Third Party Assurance*). Hiervoor was René binnen Deloitte de EMEA Leader Third Party Assurance. Hij heeft veel gepubliceerd over Third Party Assurance en is lid van de SAS 70-werkgroep van NOREA/NIVRA. René kunt u bereiken op [rene.ewals@adeia.nl](mailto:rene.ewals@adeia.nl).