Nut en noodzaak van SAS 70

Drs. S.R. van Bellen RA, drs. J.P. Hoogstra RE en drs. M.A. Francken RE RA CISA

De uitbesteding van processen in de financiële sector heeft ertoe geleid dat de toezichthouder wil dat de uitbestedende organisatie aantoont 'in control' te zijn over de uitbestede processen. Steeds meer ondernemingen verlangen daarom – en ook uit hoofde van hun SLA-management – een SAS 70-rapport van de serviceorganisaties. In dit artikel geven de auteurs op basis van hun praktijkervaring en aan de hand van de Nederlandse accountantscontrolestandaarden en de SAS 70 guidance aan wanneer een SAS 70 nodig is en welke alternatieven voorhanden zijn. Tevens wordt stilgestaan bij zaken waar de gebruiker en de opstellers op moeten letten bij het lezen en vervaardigen van een SAS 70-rapport.

Inleiding

De laatste jaren besteden steeds meer organisaties expliciete aandacht aan het 'in control' zijn, want zij moeten aan de buitenwereld kunnen aantonen dat zij grip hebben op de processen in hun organisaties. De buitenwereld komt daarbij met meer regelgeving, zoals Sarbanes Oxley (SOx) 404 en commissie-Tabaksblat.

Een andere trend die de laatste jaren in opkomst is, betreft de focus op kernactiviteiten. Als gevolg hiervan worden specifieke werkzaamheden uitbesteed die niet tot de primaire activiteiten behoren of werkzaamheden waarvan de kennis en/of capaciteit binnen de eigen organisatie onvoldoende aanwezig is. Voorbeelden van uitbesteding zijn legio, waaronder uitbesteding van vermogensbeheer, uitbesteding van de uitvoering van de pensioenregeling en uitbesteding van (delen van) ICT.

De uitbesteding van processen in bijvoorbeeld de financiële sector heeft geleid tot nieuwe wet- en regelgeving, waarbij de toezichthouder wil dat de uitbestedende organisatie aantoont 'in control' te zijn over de uitbestede processen. De uitbestedende organisatie legt deze eis inzake de aantoonbaarheid van het 'in control zijn' neer bij de partij waaraan is uitbesteed. Deze laatste partij laat in de praktijk vaak een verklaring opstellen door een onafhankelijke derde die door zowel het management van de uitbestedende organisatie, haar accountant als de externe toezichthouder gebruikt kan worden.

Waarschijnlijk kennen de meeste lezers van Compact wel de bekende Third Party Mededeling (TPM) waarbij een externe partij, veelal een auditor, een oordeel

Drs. S.R. van Bellen RA
is als manager werkzaam bij KPMG Accountants en is betrokken bij diverse SAS 70-audits.

vanbellen.sander@kpmg.nl

Drs. J. Hoogstra
is als manager werkzaam bij KPMG IT Advisory en heeft ervaring met diverse SAS 70-audits, zowel in een ontvangende als in een verstrekkende rol.

hoogstra.jan@kpmg.nl

Drs. M.A. Francken RE RA CISA
is als senior manager bij KPMG IT Advisory werkzaam binnen diverse SOx-trajecten, vanuit audit en advisory. Hierbij lag de nadruk op de IT-controles in relatie tot de financiële verantwoording. Daarnaast is hij actief betrokken bij IT Attestation (SAS 70) en External Audit support services binnen KPMG IT Advisory Nederland.

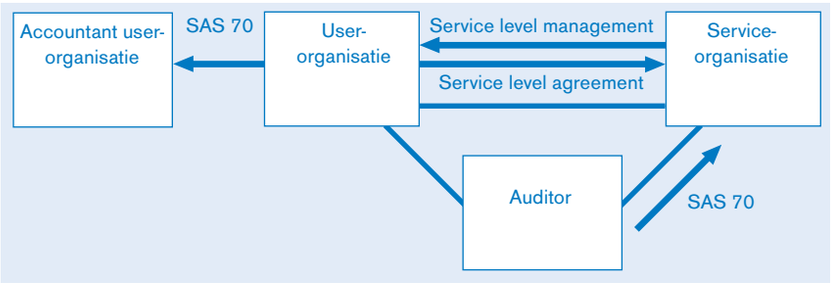
francken.marco@kpmg.nl

afgeeft over de dienstverlening van een organisatie. Deze TPM's worden van oudsher veel in de ICT gebruikt, waarbij de klant of een ICT-dienstverlener op verzoek van zijn klant een onderzoek laat verrichten door een onafhankelijke externe partij dat leidt tot een verklaring over de kwaliteit van zijn dienstverlening.

SAS 70-trajecten zijn over het algemeen erg kostbaar vanwege de verzwaring van de administratieve organisatie door de eisen aan aantoonbare vastlegging

Een nieuwe variant die, hoewel reeds langer aanwezig, de laatste jaren in Nederland steeds meer aandacht krijgt en wordt toegepast is de Statement of Auditing Standard No. 70 (SAS 70). Vooral veel pensioenuitvoerders en verzekeringsmaatschappijen zorgen met SAS 70-rapporten dat pensioenfondsbestuurders kunnen voldoen aan de Regeling Uitbesteding van De Nederlandsche Bank. Daarnaast wordt door Amerikaanse beursgenoteerde bedrijven die in Nederland dochterondernemingen hebben, veel gebruikgemaakt van deze standaard omdat strikte SOx-regelgeving dit vereist. Hierdoor wordt SAS 70 steeds meer als standaard gezien. In het verlengde hiervan nemen wij het fenomeen waar dat organisaties een SAS 70-rapport vaak als marketinginstrument gebruiken om aan te geven dat zij 'in control' zijn door met advertenties naar buiten te treden wanneer een SAS 70-rapport wordt uitgebracht.

1) Vermeldenswaardig is dat de Statement on Auditing Standards (SAS) No. 70, Service organizations, is geamendeerd en dat de werkelijke standaard (nu feitelijk de regelgeving) te vinden is in Professional Standards, vol. I, AU SEC 324. Toch spreekt men niet over SAS 324 omdat de term SAS 70 inmiddels is ingeburgerd.



Figuur 1. Relatie klant, serviceorganisatie en auditor.

SAS 70-trajecten zijn over het algemeen erg kostbaar vanwege de inhuur van externe projectmanagers en doordat de administratieve organisatie in veel gevallen fors verzwaard wordt aangezien er veel meer eisen worden gesteld aan de aantoonbare vastlegging van interne controles. Hierdoor is het van belang voor zowel de serviceorganisatie als de gebruikers van SAS 70-rapporten – iemand zal uiteindelijk deze kosten dienen te betalen – na te gaan of een SAS 70-traject met een SAS 70-rapport als product noodzakelijk is dan wel welke alternatieven er voorhanden zijn. Dit artikel probeert antwoord te geven op de vragen wanneer een serviceorganisatie een SAS 70-rapport moet opstellen en wanneer de accountant van de gebruikersorganisatie een SAS 70-rapport dient te verlangen. Ofwel: wat is het nut en de noodzaak van een SAS 70-rapport?

Als eerste wordt hiertoe de SAS 70-standaard uiteengezet, waarbij met name wordt ingegaan op de inhoud van het SAS 70-rapport. Vervolgens wordt aan de hand van de Nederlandse accountantscontrolestandaarden uiteengezet wanneer een SAS 70-verklaring nodig is en welke alternatieven voorhanden zijn. Daarna wordt stilgestaan bij zaken waar de gebruiker en opstellers op moeten letten bij het lezen en vervaardigen van een SAS 70-rapport. Ten slotte volgen er enkele alternatieven voor een SAS 70-rapportage.

SAS 70

De standaard

SAS 70[1] is een Amerikaanse richtlijn uitgevaardigd door het American Institute of Certified Public Accountants (AICPA). In deze richtlijn wordt primair beschreven hoe de externe accountant van de gebruikersorganisatie om dient te gaan met door de gebruikersorganisatie uitbestede processen, aan bijvoorbeeld een externe beheerder van vermogen of een automatiseringsorganisatie (de serviceorganisatie).

Essentie van het SAS 70-rapport is dat de gebruikersorganisatie ten behoeve van haar jaarrekeningcontrole meer inzicht en/of zekerheid wil hebben dat de prestaties van de serviceorganisatie voldoen aan door de gebruikersorganisatie gestelde normen. Een SAS 70-rapport richt zich vooral op de interne processen en beheersingsmaatregelen binnen de serviceorganisatie. In figuur 1 is de relatie tussen klant, serviceorganisatie en auditor weergegeven. Tussen de klant en de serviceorganisatie is een service level agreement afgesloten. Daarnaast geeft de auditor een SAS 70-rapport af aan de serviceorganisatie, die deze in het kader van service level management mag verstrekken aan de klant.

In een SAS 70-rapport wordt op basis van het *control framework* van COSO de control environment beschreven. In dit controleraamwerk worden de aanwezige beheersingsmaatregelen beschreven. De auditor moet hierbij aangeven of deze beheersingsmaatregelen in opzet toereikend zijn en bestaan (type I) dan wel gedurende een bepaalde periode hebben gewerkt (type II). Daarnaast moet de auditor vaststellen of de aanwezige beheersingsmaatregelen de door het management gedefinieerde beheersingsdoelstellingen afdekken.[2]

De standaard SAS 70 is voornamelijk gericht op de vorm van de rapportage en niet zozeer op de inhoud. Er wordt dus geen minimumset aan beheersingsdoelstellingen voorgeschreven. Dit is de verantwoordelijk-

2) Voor de jaarrekeningcontrole kan de accountant niet louter steunen op een type I-rapport, omdat de accountant de key controls over een jaar moet hebben getest.

heid van de serviceorganisatie. De auditor moet echter wel de toereikendheid van deze beheersingsdoelstellingen vaststellen. De guidance rondom SAS 70 geeft eisen aan de vorm van de rapportage.

Het SAS 70-rapport

De vorm van een SAS 70-rapport is uitgewerkt in de guidance van SAS 70 ([AICP06])[3], waarin tevens de verantwoordelijkheden voor de diverse partijen zijn uitgewerkt. De rapportage heeft een vast voorgeschreven indeling, die overigens in de Nederlandse praktijk nog niet in alle SAS 70-rapporten herkenbaar terugkomt:

- Sectie 1 bevat de mededeling van de auditor. Hierin geeft de auditor zijn oordeel over opzet en bestaan en/of werking van de beheersingsmaatregelen. Bij de opzet geeft de auditor tevens een oordeel of de maatregelen in algemene zin voldoen aan voorwaarden die de gebruikersorganisaties stellen in relatie tot de jaarrekening van de gebruikersorganisatie en specifiek de opzet van de beschreven beheersingsmaatregelen in sectie 2.
- Sectie 2 bevat een beschrijving van de organisatie, het gevoerde beleid en de geïmplementeerde procedures op hoofdlijnen door de serviceorganisatie. In sectie 2 staan ook de beheersingsdoelstellingen en de beheersingsmaatregelen beschreven.
- Sectie 3 is een sectie geschreven door de auditor, waarin hij een beschrijving kan geven van de uitgevoerde tests op de werking en de resultaten van deze tests.
- Sectie 4 is voor de serviceorganisatie. Dit hoofdstuk wordt in de praktijk vaak gebruikt voor een toelichting op de geconstateerde bevindingen door het management, dan wel een toelichting op bepaalde (toekomstgerichte) aspecten. In ieder geval dekt de mededeling van de auditor sectie 4 niet af.

Indien een type II-verklaring wordt afgegeven, wordt in sectie 1 expliciet de werkingsperiode beschreven. De werkingsperiode betreft minimaal zes maanden (veelal het eerste jaar), waarbij het gebruikelijk is om een werkingsperiode van één jaar te hanteren voor daaropvolgende jaren. In uitzonderingssituaties kan afgeweken worden van de minimale werkingsperiode van zes maanden, waarbij het minimum drie maanden is. Een SAS 70-rapport over een periode van zes maanden is in principe niet voldoende voor de jaarrekeningcontrole. Er dient ook *control evidence* te worden verkregen over de andere maanden. Theoretisch gezien is het uitgangspunt van SAS 70 dat alleen het eerste jaar een periode van zes maanden zal beslaan, daarna zal de verklaring een heel jaar bestrijken. In de praktijk zien we echter steeds meer dat organisaties meerdere jaren achter elkaar een SAS 70 over een periode van zes maanden afgeven. Dit betreft vaak het tweede en het derde kwartaal van het jaar. De gebruikersorganisatie heeft dan nog de tijd en ruimte om in het vierde kwartaal compenserende maatregelen in haar eigen organisatie en controleraamwerk te treffen bij eventuele geconstateerde tekortkomingen.

Een SAS 70-rapport over een periode van zes maanden is in principe niet voldoende voor de jaarrekeningcontrole

In tabel 1 is samengevat in hoeverre de secties verplicht of optioneel zijn in geval van een type I- of een type II-rapport.

3) De SAS 324-standaard is niet zo uitgebreid. De guidance daarentegen wel. Hierin staan veel voorbeelden en ook voorbeeldrapporten.

Sectie 4 wordt niet door de auditor beoordeeld, de inhoud hiervan is de verantwoordelijkheid van de serviceorganisatie. In sectie 3 hoeft de auditor geen gedetailleerde beschrijving te geven van de uitgevoerde tests, het gaat in die sectie met name om de soorten uitgevoerde tests (inspectie, waarneming ter plaatse, verificatie met documentatie en *reperformance*). Een uitzondering hierop betreft die gevallen waarin de geteste beheersingsmaatregelen niet effectief waren, dan is een nadere toelichting op de uitgevoerde test(resultaten) vereist.

Sectie	Type I	Type II
1 Rapport van de onafhankelijke auditor	Verplicht. Bevat conclusie en timing.	Verplicht, bevat conclusie en werkingsperiode.
2 Beschrijving organisatie, processen, beheersingsdoelstellingen en beheersingsmaatregelen	Verplicht. Verantwoordelijkheid serviceorganisatie.	Verplicht. Verantwoordelijkheid serviceorganisatie.
3 Informatie over uitgevoerde tests van de werking	Optioneel.	Verplicht. Verantwoordelijkheid auditor.
4 Overige informatie	Optioneel. Verantwoordelijkheid serviceorganisatie.	Optioneel. Verantwoordelijkheid serviceorganisatie.

Tabel 1. Sectie-indeling SAS 70-rapport.

Nut en noodzaak

De noodzaak voor het opstellen van een SAS 70-rapport door de serviceorganisatie wordt primair ingegeven doordat de klanten en de accountants van deze klanten dit eisen uit hoofde van de externe jaarrekeningcontrole. Om de noodzaak van deze eis bloot te leggen zullen wij derhalve de Nederlandse accountantscontrolestandaard COS 402 *De controleconsequenties van het gebruikmaken van serviceorganisaties*[4] ([NIVR07]) uiteenzetten. Waarna wij verder ingaan op het nut van een SAS 70-onderzoek.

4) Deze standaard is afgeleid van de Internationale Accountantscontrolestandaarden van het IFAC.

Jaarrekeningcontrole

Uit COS 402 is een aantal belangrijke afwegingen te herleiden die een externe accountant, en in zijn kielzog

het management van de gebruikersorganisatie, dient te maken in het geval bepaalde processen zijn uitbesteed aan een serviceorganisatie.

Verantwoordelijkheid extern

Artikel 2 geeft aan dat de accountant dient te beoordelen welke invloed het gebruikmaken van een serviceorganisatie door de gebruikersorganisatie heeft op de interne beheersing van de entiteit om het risico van een afwijking van materieel belang te kunnen onderkennen en in te kunnen schatten alsmede om aanvullende controlewerkzaamheden op te kunnen zetten en uit te kunnen voeren. In de reguliere jaarrekeningcontrole dient de accountant te bepalen in hoeverre de gebruikersorganisatie zelf de autorisatie van transacties uitvoert en/of voldoende effectieve maatregelen heeft getroffen. Indien de verantwoordelijkheid van de autorisatie van transacties bij de serviceorganisatie ligt kan de gebruikersorganisatie het noodzakelijk achten te moeten steunen op de voorschriften en procedures van de serviceorganisatie.

Invloed op de controle

In het laatste geval dient de accountant de betekenis van de activiteiten van de serviceorganisatie voor de gebruikersorganisatie en de invloed daarvan op de accountantscontrole vast te stellen (bijvoorbeeld de controleerbaarheid van de door de serviceorganisatie uitgevoerde werkzaamheden). In het geval dat de accountant concludeert dat de activiteiten van de serviceorganisatie belangrijk zijn voor de onderbouwing van de beweringen in de jaarrekening van de huishouding en dus relevant voor de controle zijn, dient de accountant voldoende inzicht te verkrijgen om risico's van een afwijking van materieel belang te kunnen onderkennen.

In het kader van een reguliere jaarrekeningcontrole is een SAS 70-rapport niet altijd noodzakelijk

Rapporten aanwezig

Daarvoor moet de accountant vaststellen of er rapportages aanwezig zijn voor het verkrijgen van informatie over de interne beheersing van de serviceorganisatie. Deze rapporten kunnen zowel zijn opgesteld door de (interne) auditor van de serviceorganisatie als door toezichthouders. COS 402 stelt geen eisen aan het 'format' of de inhoud van de rapportage. In deze rapporten dient wel een mededeling te zijn opgenomen door een externe auditor omtrent de effectieve werking van de interne beheersing van de serviceorganisatie met betrekking tot de activiteiten van de serviceorganisatie die voor de controle van belang zijn.

Hoewel COS 402 geen eisen stelt aan 'format' en inhoud, wordt in artikel 13 gesteld dat de accountant de reikwijdte, bruikbaarheid en toereikendheid van het verstrekte rapport dient te beoordelen. Daarnaast dient de accountant te beoordelen, indien het rapport de effectieve werking betreft, of de aard, het tijdstip van uitvoering en de diepgang van de tests toereikende controle-informatie verschaffen om het door de accountant ingeschatte risico van een afwijking van materieel belang te onderbouwen.

Aanvullende werkzaamheden

Concreet betekent het vorengenoemde dat als er geen rapporten aanwezig zijn dan wel de aanwezige rapporten onvoldoende zijn, de accountant zelf controlemaatregelen zal moeten uitvoeren teneinde een deugdelijke grondslag te verkrijgen voor zijn oordeel. Over het vaststellen van de effectiviteit stelt alinea 10 van COS 402 dat de accountant deze deugdelijke grondslag kan verkrijgen op twee alternatieve manieren:

- toetsen van de werking van de beheersingsmaatregelen binnen de gebruikersorganisatie op de activiteiten van de serviceorganisatie;
- bezoeken van de serviceorganisatie en het uitvoeren van systeemgerichte werkzaamheden.

Dit betekent dat, indien er geen SAS 70 of gelijkwaardig rapport aanwezig is, de accountant zelfstandig (aanvullende) werkzaamheden dient te verrichten. Dit is niet efficiënt wanneer de serviceorganisatie meerdere gebruikersorganisaties bedient.

Van belang bij het bepalen van de noodzaak van een SAS 70-rapport is de mate waarin de gebruikersorganisatie steunt op maatregelen die door de serviceorganisatie zijn getroffen. Dit is met name het geval als de beheersingsmaatregelen die door de gebruikersorganisatie zelf zijn getroffen inzake de uitbestede processen, niet alle risico's in hun geheel afdekken. Als de gebruikersorganisatie zelf voldoende beheersingsmaatregelen heeft getroffen, is een SAS 70-rapport niet noodzakelijk. Een voorbeeld in dit verband is de uitbesteding van de salarisverwerking door een onderneming. Indien deze onderneming voldoende 'input-output controls' heeft op de juist-, volledig- en tijdigheid van de aangeleverde data en daarnaast de ontvangen cijfers beoordeelt door middel van deelwaarnemingen en totaalverbanden op de verwachte brutoloonsom en fiscale afdrachten, zouden deze 'boundary controls' voldoende kunnen zijn. Is dat niet het geval, dan is een SAS 70-rapport een mogelijke oplossing, waarbij uiteraard wel alle keyprocessen en -risico's moeten zijn meegenomen.

Wel of geen SAS 70-rapport?

De gebruikersorganisatie dient vanuit haar verantwoordelijkheden een besluit te nemen over de noodzakelijkheid van een SAS 70-rapport.

Figuur 2 geeft een en ander kernachtig weer in een beslisboom.

Samenvattend kan gesteld worden dat in het kader van de reguliere jaarrekeningcontrole een SAS 70-rapport niet altijd noodzakelijk is. Wel kan een SAS 70-rapport, afhankelijk van het type en de beschreven beheersingsdoelstellingen, voldoen aan de informatiewensen van het management van de gebruikersorganisatie. In de praktijk komt het echter vaak voor dat de accountant een SAS 70-rapport alléén, onvoldoende controle-informatie vindt voor de jaarrekeningcontrole van de gebruikersorganisatie. Het SAS 70-rapport dekt met name de volledigheid van de transactieverwerking af, maar geeft onvoldoende informatie bijvoorbeeld over de waardering en het bestaan van de beleggingen die in beheer zijn bij een vermogensbeheerder, waardoor aanvullende gegevensgerichte werkzaamheden dienen te worden verricht door de accountant op de beleggingsstanden per jaareinde.

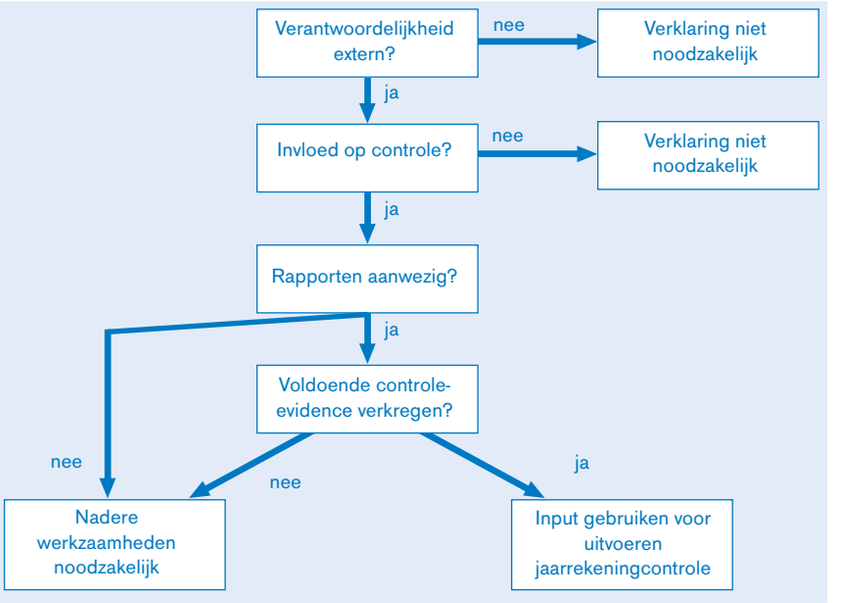
SAS 70 voor andere doeleinden

Naast de noodzaak die voortvloeit uit een externe jaarrekeningcontrole zien we in de praktijk regelmatig dat SAS 70-rapporten worden opgesteld ten behoeve van andere doeleinden, zoals:

- onderbouwing van het, onder SOx verplichte, in control statement, afgegeven door de CEO van de gebruikersorganisatie;
- nakoming van afspraken zoals vastgelegd in service level agreements;
- het kunnen voldoen aan de Regeling Uitbesteding van DNB;
- commerciële doeleinden in die zin dat men wil aantonen dat de processen worden beheerst.

Hoewel een SAS 70-rapport vaak wordt gebruikt voor commerciële doeleinden, geeft het geen zekerheid voor de toekomst. Een SAS 70-rapport gaat specifiek in op een bepaalde werkingsperiode in het verleden (type II), terwijl een ISO-certificaat bijvoorbeeld geldend is voor een bepaalde periode in de toekomst (tot einde geldigheidsduur). Een goedkeurend SAS 70-rapport zonder bevindingen geeft alleen aan dat de organisatie in de werkingsperiode de betreffende beheersingsmaatregelen had ingericht (afhankelijk van de type-verklaring).

Een SAS 70-onderzoek is echter volgens de verplichte formulering van de accountantsmededeling gericht op het verkrijgen van een redelijke mate van zekerheid dat de beschrijving een getrouw beeld geeft van die aspecten van beheersingsmaatregelen van de serviceorganisatie die van belang kunnen zijn voor de interne beheersing van een gebruikersorganisatie, voor zover een en ander betrekking heeft op de controle van de jaarrekening van de gebruikersorganisatie.



Figuur 2. Beslisboom in het kader van de jaarrekeningcontrole.

Attentiepunten bij gebruik van SAS 70

Indien de noodzaak van een SAS 70-rapport aanwezig is en een SAS 70-rapport wordt opgesteld en uitgebracht, zijn de volgende, in willekeurige volgorde behandelde zaken van belang voor zowel het management van de serviceorganisatie als van de gebruikersorganisatie.

Relevante scope voor eindgebruikers

Zowel voor het management van de gebruikersorganisatie als haar accountant is het van belang een SAS 70-rapport aandachtig te bestuderen. Een auditorsrapport met goedkeurende strekking (afkeurend komt zelden voor) betekent niet automatisch dat het rapport voldoet aan de verwachtingen. Het is van belang dat de gebruiker vaststelt welke beheersingsdoelstellingen zijn getest en welke beperkingen het rapport kent. De auditor van de serviceorganisatie zal in zijn rapportage duidelijk de scope van het onderzoek moeten omschrijven en in zijn mededeling dan ook verwijzen naar de bijlage in de rapportage waarin de overeengekomen beheersingsdoelstellingen worden beschreven en waarin hij aangeeft welke tests hij heeft uitgevoerd en wat zijn bevindingen waren. Het komt in de praktijk voor dat essentiële beheersingsdoelstellingen, van belang voor de uiteindelijke gebruikers, niet zijn opgenomen en getest. Om dit te voorkomen is het raadzaam om vooraf met de gebruikersorganisatie af te stemmen welke beheersingsdoelstellingen in het SAS 70-rapport worden afgedekt. Het is overigens tevens raadzaam voor de serviceorganisatie om, al dan niet in een specifieke paragraaf genaamd ‘gebruikerscontroles’, aan te geven welke controles de gebruikers zelf dienen te verrichten teneinde de beheersingsdoelstellingen af te dekken.

Reikwijdte verklaring in relatie tot de accountantscontrole

In principe hebben de werkzaamheden in het SAS 70-onderzoek directe raakvlakken met de werkzaamheden die de accountant van de gebruikersorganisatie in het kader van de jaarrekeningcontrole uitvoert. Zoals eerder is gesteld gaat bijvoorbeeld de formulering van het oordeel van de auditor specifiek in op de jaarrekeningcontrole.

Een essentieel verschil is echter dat het doel van een jaarrekeningcontrole is om een oordeel uit te spreken over de getrouwheid van de gepresenteerde cijfers ten behoeve van een brede groep gebruikers ('het maatschappelijk verkeer'). In het SAS 70-onderzoek geeft de auditor uitsluitend een oordeel over de afzonderlijk genoemde beheersingsmaatregelen voor een beperkte, vooraf gedefinieerde, verspreidingskring.

Afhankelijk van de gedefinieerde beheersingsdoelstellingen zal hij dus andere controlestappen uitvoeren: als de doelstelling is dat transacties tijdig moeten zijn verwerkt, dan zal hij van de geselecteerde transacties de tijdige verwerking vaststellen, terwijl hij in het kader van de jaarrekeningcontrole kan volstaan met vaststellen dat ultimo jaar de transacties zijn verwerkt door bijvoorbeeld afstemming met de bankafschriften.

Daarentegen wil een SAS 70-rapport ook niet direct zeggen dat alle zaken die in een SLA zijn opgenomen worden afgedekt, omdat de primaire scope van een SAS 70-rapport betrekking heeft op de jaarrekening.

De primaire scope van een SAS 70-rapport heeft betrekking op de jaarrekening

Ten slotte kan de eindgebruiker, c.q. haar accountant, vaststellen dat bepaalde belangrijke beheersingsmaatregelen niet zijn onderzocht en er kan, in onderling overleg tussen de gebruikersorganisatie, haar accountant en de serviceorganisatie, besloten worden tot aanvullend onderzoek.

Timing van een SAS 70-rapport

Een verklaring bij de jaarrekening wordt aan het einde van een boekjaar verstrekt, wat zou kunnen inhouden dat een SAS 70-verklaring dezelfde einddatum zou moeten hebben. Idealiter is dat ook zo, maar indien een SAS 70-rapport na einde boekjaar wordt ontvangen en er tekortkomingen zijn gesignaleerd, is er geen mogelijkheid om hier nog compenserende maatregelen voor te identificeren c.q. te implementeren door de gebruikersorganisatie. Met name om die reden worden SAS 70-rapporten veelal opgevraagd en opgesteld per einde derde kwartaal, zodat de uitkomsten kunnen worden geëvalueerd in het vierde kwartaal van het boekjaar van de betreffende gebruikersorganisatie. Een andere vraag die hierbij opkomt, is hoe moet worden omgegaan met dit laatste kwartaal. Uiteraard is dit afhankelijk van het belang van het SAS 70-rapport binnen het internecontroleraamwerk van de gebruikersorganisatie, maar ook van de aard en omvang van de geconstateerde tekortkomingen. De gebruikersorganisatie zal in elk geval moeten vaststellen dat de situatie in het laatste kwartaal niet significant is gewijzigd ten opzichte van het voorgaande kwartaal: wijzigingen in management, systemen, processen en andere omgevingsfactoren. Het kan wellicht zinvol zijn de serviceorganisatie te vragen om door haar auditor specifieke overeengekomen werkzaamheden te laten verrichten op dit laatste kwartaal met een beperktere scope en diepgang dan het SAS 70-rapport zelf. Daarnaast kan de gebruikersorganisatie ook zelf een beperkte follow-up geven bij de serviceorganisatie.

One size fits all?

Het is voor de serviceorganisatie het meest efficiënt indien zij één SAS 70-rapport opstelt voor meerdere gebruikers. Binnen de verplichte management assessment (in geval van SOx) zien we dat er strak voorgeschreven 'sample sizes' van toepassing zijn met betrekking tot de te testen beheersingsmaatregelen. Indien de serviceorganisatie bij haar tests de minimale 'sample sizes' evenredig verdeelt over de processen en data van al haar klanten, kan het zijn dat de data en processen van de betreffende ondernemingen slechts beperkt (of niet) in deze testscope vallen. Indien bijvoorbeeld de serviceorganisatie het wijzigingsbeheerproces over de IT-infrastructuur verricht voor diverse ondernemingen en hierbij dertig van de driehonderd doorgevoerde wijzigingen test, kan het heel goed zijn dat er ondernemingen zijn waarvan de wijzigingen niet in de test vielen. Betekent dit nu dat de betreffende beheersingsmaatregelen van deze ondernemingen niet zijn getest? Dat is een moeilijke vraag waar eigenlijk geen eenduidig antwoord op is te geven. Dit hangt wederom sterk af van het belang en de bijbehorende risico's van de uitbestede diensten. We zien in de praktijk dat ondernemingen die SOx 404-plichtig zijn, veelal specifieke testgevallen afdwingen voor de data die de serviceorganisatie onder haar beheer heeft, met name indien processen niet uniform verlopen of als systemen anders zijn ingericht voor verschillende gebruikersorganisaties.

Detailniveau beschreven tests

In een SAS 70-rapport behoeft het detailniveau van de uitgevoerde tests niet per test te worden vermeld, tenzij er afwijkingen zijn geconstateerd. Maar de AICPA SAS 70 audit guide (artikel 2.45) geeft in dit verband

ook het volgende aan: '... description of tests of operating effectiveness and the results of those tests:
- controls that were tested;
- control objectives the controls were intended to achieve;
- indication of nature, timing, extent, and results of the tests applied in sufficient detail to enable user auditors to determine the effect of such tests on their assessment of control risk ...'

Veel SAS 70-rapporten geven dit detailniveau nog niet aan bij effectieve beheersingsmaatregelen. Dit is akkoord indien er duidelijk, bijvoorbeeld in de inleiding bij sectie 3, is aangegeven welke testmethodiek is toegepast en welke 'sample sizes' daar doorgaans bij horen.

Uiteraard zijn er nog andere aspecten te benoemen, maar dat gaat voor de doelstelling van dit artikel te ver.

Alternatieven voor een SAS 70-rapport

In de praktijk zien we dat er een aantal alternatieven voor een SAS 70-rapport is. Deze alternatieven zijn van oudsher in gebruik, vaak nog van vóór de tijd van SAS 70. Deze alternatieven zijn:
- TPM, en
- overeengekomen specifieke werkzaamheden.

Beide alternatieven worden hieronder kort uitgewerkt.

TPM

Een Third Party Mededeling (TPM) is een schriftelijke uiting over de interne beheersing van de processen van een serviceorganisatie. Deze uiting wordt verstrekt door een onafhankelijke en onpartijdige auditor ten behoeve van één of meer gebruikers, zoals gebruikersorganisaties en (potentiële) klanten van een serviceorganisatie en hun externe auditor(s). Hierbij wordt met een redelijke mate van zekerheid gerapporteerd over een set van normen.

Een TPM gaat daarmee expliciet in op een gedefinieerd normenkader en niet zozeer op de controleomgeving en de beheersingsdoelstellingen van een serviceorganisatie. Een TPM is van oudsher veel in gebruik bij automatiseringsorganisaties.

De belangrijkste verschillen tussen SAS 70 en TPM zijn in tabel 2 aangegeven.

Eén van de voordelen van een TPM is dat deze vaak gerichter is, doordat alleen de normen beoordeeld worden en niet de control environment. Dat maakt dat dit soort onderzoeken vaak goedkoper is. Het grote verschil tussen de inspanning voor een SAS 70-rapport en een TPM-rapport zit in het opstellen van het rapport.

Overeengekomen specifieke werkzaamheden

Bij overeengekomen specifieke werkzaamheden voert de auditor werkzaamheden uit bij de serviceorganisatie. Dit is veelal de auditor van deze serviceorganisatie, die in opdracht van de klant werkzaamheden uitvoert. Bij overeengekomen specifieke werkzaamheden wordt geen totaalconclusie gegeven. Dit betekent dat deze onderzoeken ook geen zekerheid geven ten behoeve van de jaarrekeningcontrole.

Tabel 2. Verschillen tussen SAS 70 en TPM.

Onderwerp	TPM	SAS 70
Onderwerp	Norm	Control objectives
Opdrachtgever	Klantorganisatie of service-organisatie	Serviceorganisatie
Vorm	Vrij	Geadviseerde sectie-indeling
Oordeelsformulering	Conform Nederlandse accountantsrichtlijnen	Verplichte formulering conform SAS 70-standaard
Doelgroep	Vaak één specifieke klant	Bij voorkeur meerdere klanten
Nut voor de jaarrekening	Afhankelijk van scope en diepgang	Afhankelijk van scope en diepgang

Onderwerp	Overeengekomen specifieke werkzaamheden	SAS 70
Onderwerp	Norm	Control objectives
Oordeelsformulering	Geen oordeel	Verplichte formulering conform AICPA
Doelgroep	Eén specifieke klant	Bij voorkeur meerdere klanten
Nut voor de jaarrekening-controle	Beperkt, aangezien er beperkte zekerheid wordt gegeven	Afhankelijk van scope en diepgang
Betrokkenheid user auditor	Intensief, voor bepalen normen en uit te voeren werkzaamheden	Beperkt, alleen in voorfase

Tabel 3. Verschillen tussen overeengekomen specifieke werkzaamheden en SAS 70.

De auditor rapporteert per control bevindingen en of deze control wel of niet effectief is. Op basis hiervan kunnen de klant en diens accountant zelf hun conclusies trekken. De user auditor zal in dit verband veel betrokken zijn bij de uitvoering van de opdracht, om te kunnen waarborgen dat de uitkomsten van het onderzoek bruikbaar zijn.

De belangrijkste verschillen tussen SAS 70 en overeengekomen specifieke werkzaamheden zijn in tabel 3 aangegeven.

Conclusie

Het nut en de noodzaak van een SAS 70-rapport zijn afhankelijk van het doel van de verklaring, de inhoud

ervan (scoping) en de mate van uitbesteding. Elke gebruikersorganisatie dient, eventueel samen met haar accountant, te bepalen in hoeverre een verklaring voor de uitbestede dienstverlening noodzakelijk is. Dit zal afhankelijk zijn van het controleraamwerk bij de gebruikersorganisatie, alsmede van in hoeverre en in welke mate de werkzaamheden en de verwachte beheersingsmaatregelen van de serviceorganisatie daarin passen. Vervolgens moet bepaald worden op basis van effectiviteits- en efficiencyoverwegingen in hoeverre dit een SAS 70-rapport moet zijn of dat een TPM of overeengekomen specifieke werkzaamheden ook tot de mogelijkheden behoren. Tot slot zal de gebruikersorganisatie in samenspraak met haar accountant moeten bepalen of een SAS 70-rapport alleen voldoende is, mede gezien de werkingsperiode, of dat aanvullende werkzaamheden, bijvoorbeeld meer specifiek overeengekomen (andere) werkzaamheden, noodzakelijk zijn.

Literatuur

[AICP06] *Service Organizations: Applying SAS No. 70, as amended*, AICPA Audit Guide, American Institute of Certified Public Accountants, 2006.

[Bigg05] S.R.M. van den Biggelaar RE en P.C.V. Waldenmaier RE RA, *Praktijkervaringen binnen SAS 70-trajecten*, Compact 2005/2.

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

[NIVR07] *Controle en Overige Standaarden COS 402, de controleconsequenties van het gebruikmaken van serviceorganisaties*, Koninklijk NIVRA, 2007.