SOC 1-rapportages

Onderzoek naar ervaringen in de praktijk met een wereldwijde standaard

Anno Perk MSc, Stacy Warner CISA en drs. Marcel Fikke RE RA CISA

Het uitbesteden van processen heeft altijd impact op de beheersingsomgeving van de uitbestedende organisatie. Hoewel sommige controleactiviteiten niet meer hoeven te worden uitgevoerd, zal nog wel moeten worden vastgesteld in hoeverre de serviceorganisatie haar zaakjes op orde heeft. Gelukkig is er al weer enige tijd een wereldwijde standaard voor de beoordeling van de interne beheersing van serviceorganisaties. In dit artikel wordt aan de hand van een inventariserend onderzoek verslag gedaan van de eerste ervaringen met de nieuwe standaard en van de mogelijkheden voor global reporting.

A.L. Perk MSc
is adviseur bij KPMG Advisory.
perk.anno@kpmg.nl

A.M. Warner CISA
is senior manager bij KPMG Advisory.
warner.stacy@kpmg.nl

Drs. M.T. Fikke RE RA CISA
is manager bij KPMG Advisory.
fikke.marcel@kpmg.nl

Inleiding

Er kunnen verschillende oorzaken zijn waardoor het management van een organisatie zich voor de strategische keuze ziet gesteld om administratieve processen, het beheer van IT-systemen, gegevensverwerking of delen daarvan uit te besteden aan serviceorganisaties. Als de beslissing uiteindelijk is genomen, de serviceorganisatie is geselecteerd en de activiteiten zijn overgegaan, dan houdt de verantwoordelijkheid van het management voor deze processen echter niet op te bestaan. De uitbestedende partij (de gebruikersorganisatie) verwacht van de serviceorganisatie wel dat deze processen heeft ingericht om de risico's te beheersen die verband houden met de uitbestede activiteiten.

Om comfort te krijgen over de uitbestede activiteiten kan de gebruikersorganisatie bij de serviceorganisatie vragen om een assurancerapport, ook wel aangeduid als Service Organisatie Control (SOC)-rapport. De serviceorganisatie legt door middel van een SOC-rapport verantwoording af over het door haar geïmplementeerde systeem van interne beheersing over de aan haar klanten geleverde diensten. Het is daarbij belangrijk dat de serviceorganisatie vooraf afstemming heeft met de gebruikersorganisaties over de scope en inhoud van de SOC-rapportage.

Serviceorganisaties zoeken naar betere manieren om zekerheid te verschaffen over hun beheersingsomgeving

In het verleden werden SOC-rapporten veelal opgesteld op basis van de Amerikaanse SAS 70-standaard. Over de voorbereiding op de overgang van rapporten op basis van SAS 70 naar rapporten op basis van de internationale standaard ISAE 3402 of standaard ISAE 3000 is al veel geschreven, onder meer in [Beek11] en [KPMG10].

De standaard ISAE 3402 dient te worden gebruikt voor de beoordeling van de interne beheersing van processen die van belang zijn voor de financiële verantwoording. Voor de overige beheersingsmaatregelen (niet gerelateerd aan financiële verantwoordingsprocessen) kan gebruik worden gemaakt van de assurancestandaard ISAE 3000. De ISAE 3402-standaard is feitelijk een nadere concretisering van de ISAE 3000-standaard. Het stramien van ISAE 3402 kan echter in ISAE 3000 ook worden gevolgd om over de beheersing van andere processen te rapporteren ([Beek11], [KPMG12]).

SOC-rapportages

Om de herkenbaarheid en voorspelbaarheid van SOC-rapportages ten aanzien van IT-gerelateerde processen te bewerkstelligen heeft de Amerikaanse beroepsorganisatie voor accountants, het American Institute of Certified Public Accountants (AICPA), een drietal categorieën van SOC-rapportages gedefinieerd ([KLLP12]):

- *SOC 1*^{SM} – een rapportage over de beheersingsmaatregelen bij een serviceorganisatie die relevant zijn voor de interne beheersing van financiële verantwoordingsprocessen. SOC 1-rapporten worden in de Verenigde Staten uitgebracht in overstemming met SSAE 16 die valt onder de standaard AT 801 (zie ook tabel 1). Buiten de Verenigde Staten zouden deze rapporten onder de internationale standaard ISAE 3402 kunnen worden uitgebracht.
- *SOC 2*^{SM} – een rapportage over de beheersingsmaatregelen bij een serviceorganisatie die relevant zijn voor informatiebeveiliging, beschikbaarheid, integriteit van gegevensverwerking, vertrouwelijkheid of privacy. In de Verenigde Staten worden SOC 2-rapporten uitgebracht onder standaard AT 101. Buiten de Verenigde Staten zouden deze rapporten onder de internationale standaard ISAE 3000 kunnen worden uitgebracht.
- *SOC 3*^{SM} – een Trust Services rapportage voor serviceorganisaties. Evenals de SOC 2-rapporten kunnen deze onder AT 101 respectievelijk ISAE 3000 worden uitgebracht. Een SOC 3-rapport kan voor een breder publiek worden gebruikt dan een SOC 2-rapport.

Niveau	SOC 1^{SM}	SOC 2^{SM}	SOC 3^{SM}
Samenvatting	Gedetailleerd rapport voor gebruikers en hun auditors.	Gedetailleerd rapport voor gebruikers, hun auditors en gespecificeerde partijen.	Beknopt rapport dat meer algemeen mag worden verspreid, met als optie het opnemen van een trustzegel op de website.
Toepassing	Focus op financiële verantwoordingsrisico's en op beheersingsmaatregelen gerelateerd aan financiële verantwoordingsprocessen die door de serviceorganisatie zijn gespecificeerd. Van toepassing wanneer de serviceorganisatie financiële transacties verwerkt of transactie-verwerkende systemen ondersteunt.	Focus op de volgende principes: • Informatiebeveiliging • Beschikbaarheid • Vertrouwelijkheid • Integriteit van gegevensverwerking • Privacy Van toepassing op een breed scala van systemen.	

Tabel 1. **Verschillen en overeenkomsten tussen de SOC-rapportages.**

Deze drie verschillende rapportages adresseren een bredere set aan specifieke behoeften van gebruikers, zoals risico's met betrekking tot informatiebeveiliging, privacy of beschikbaarheid van systemen. Daarnaast zoeken serviceorganisaties naar betere manieren om zekerheid te verschaffen over hun beheersingsomgeving.

SOC-rapportages bieden de serviceorganisaties een gestructureerde manier van rapporteren. In tabel 1 zijn de verschillen en overeenkomsten van de drie SOC-rapportages opgenomen.

Wat is het effect geweest van de wijziging in de standaarden op het SOC-rapport?

Door het vervangen van de SAS 70-standaard dienden serviceorganisaties te heroverwegen op basis van welke standaard zij verantwoording zouden afleggen over de interne beheersing van de aan haar uitbestede processen. De keuze voor ISAE 3402 betekent dat de serviceorganisatie rekening zou moeten houden met een aantal nieuwe of gewijzigde elementen in het SOC-rapport, zoals de managementbewering, het omgaan met subserviceorganisaties en het gebruikmaken van werkzaamheden van internal audit.

Inmiddels hebben de serviceorganisaties en service-auditors in 2011 en 2012 ervaringen opgedaan met de assurancestandaarden. Reden om een inventariserend onderzoek uit te voeren naar de toepassing ervan in de praktijk en om te onderzoeken welke topics er nu spelen rond SOC-rapportages. Onderstaande uitkomsten zijn gebaseerd op een wereldwijde survey onder serviceauditors, gesprekken met serviceorganisaties in Nederland en uit eigen ervaringen met betrekking tot de servicerapporten over 2011 en 2012. In totaal zijn ruim 230 serviceorganisaties uit diverse sectoren (zoals pensioenfondsen, beleggingsinstellingen en IT-serviceproviders) in het onderzoek betrokken.

Type SOC-rapportage

De serviceorganisatie legt door middel van een SOC-rapport verantwoording af over het door haar geïmplementeerde systeem van interne beheersing over de aan haar klanten geleverde diensten. Het is daarbij belangrijk dat de serviceorganisatie vooraf afstemming heeft met de gebruikersorganisaties over de scope en inhoud van de SOC-rapportage.

Uit ons onderzoek is gebleken dat in veruit de meeste gevallen ervoor is gekozen om de SAS 70-rapportage te vervangen door een ISAE 3402. Ongeveer één op de zes serviceorganisaties heeft wel de overgang naar ISAE 3000 overwogen, maar heeft uiteindelijk toch gekozen voor ISAE 3402. De ondervraagde serviceorganisaties hebben aangegeven dat in veel gevallen de communicatie tussen serviceorganisatie en gebruikersorganisatie beperkt is geweest met betrekking tot de vorm van het rapport en dat is in onze ogen een gemiste kans. Beide partijen zijn immers gebaat bij een rapportage die het meest geschikt is voor de verantwoording over de processen die zijn uitbesteed en over de afspraken die daarover zijn gemaakt. Goede communicatie over de scope en vorm van het SOC-rapport vergroot de doeltreffendheid ervan. Wanneer informatiebeveiliging en beschikbaarheid van een specifiek systeem belangrijk zijn voor de diensten die een serviceorganisatie levert, dan is de gebruikersorganisatie het meest gebaat bij een SOC 2- of SOC 3-rapport. Uit de wereldwijde survey blijkt dat in de Verenigde Staten bijna 4% van de betreffende serviceorganisaties al bezig is met een SOC 2- of SOC 3-rapport en dat nog eens 36% geïnteresseerd is om een dergelijk rapport uit te brengen. Ook buiten de Verenigde Staten blijkt bij één op de drie serviceorganisaties interesse te bestaan in een SOC-rapport op basis van de ISAE 3000- in plaats van de ISAE 3402-standaard.

Managementbewering

De meest opvallende toevoeging aan het SOC-rapport is de opname van een managementbewering. In de managementbewering verklaart het management dat de in het rapport opgenomen beschrijving van de processen en systemen een getrouw beeld weergeeft. Tevens verklaart het management dat de interne beheersingsmaatregelen op afdoende wijze zijn opgezet en (bij een Type 2-rapport) gedurende de verslagperiode effectief werkten.

Het verantwoordelijke management baseert zijn uitspraken op de uitgevoerde management controls. Uit onze inventarisatie is gebleken dat veel serviceorganisaties al een proces hadden geïmplementeerd waarbij gebruik wordt gemaakt van rapportages van de eigen interne auditafdeling of van periodieke 'In Control'-statements door het lagere management. Het opnemen van een managementbewering is voor deze organisaties geen aanleiding geweest om meer monitoring controls toe te voegen aan het interne beheersingsraamwerk. De overige organisaties hebben wel in enkele gevallen monitoring controls specifiek aan het raamwerk toegevoegd.

De meeste organisaties hebben aangegeven dat zij de betreffende management controls hebben beschreven onder het hoofdstuk dat de interne beheersingsstructuur beschrijft. Zij hebben daarin echter niet aangegeven dat deze management controls zijn gebruikt om tot de managementbewering te komen. Transparantie op dit punt zou derhalve nog verder kunnen worden verbeterd.

Uit de interviews met de serviceorganisaties is verder gebleken dat geen enkele organisatie is afgeweken van de voorbeeldtekst in de standaard. De managementbewering is in de meeste gevallen ondertekend door één of meer C-level functionarissen. In ongeveer een kwart van de

Communicatie tussen serviceorganisatie en gebruikersorganisatie over de keuze van het type SOC-rapport is beperkt geweest

ISAE 3402 is geen aanleiding geweest om belangrijke wijzigingen door te voeren in het interne beheersingsraamwerk

gevallen is de managementverklaring getekend in naam van de serviceorganisatie. Het komt daarnaast bij ongeveer één op de zes serviceorganisaties voor dat de managementbewering niet is ondertekend.

Intern beheersingsraamwerk

Eén van de verplichte onderdelen van het SOC-rapport is de systeembeschrijving. Hierin beschrijft het management van de serviceorganisatie onder meer de soorten diensten en het interne beheersingsraamwerk. De verwachting bij de introductie van de ISAE 3402-standaard was dat de serviceorganisatie meer aandacht zou besteden aan het beschrijven van het risicomanagementproces, bijvoorbeeld door de risico-inschattingen op te nemen ter ondersteuning van de managementbewering of door het opnemen van meer monitoring controls in het beheersingsraamwerk. Uit de wereldwijde survey blijkt echter dat in slechts 34% van de gevallen sprake is geweest van een uitbreiding van de betreffende sectie in het rapport.

De ondervraagde serviceorganisaties hebben verder aangegeven dat de overgang naar ISAE 3402 geen aanleiding is geweest om belangrijke wijzigingen door te voeren in het interne beheersingsraamwerk, aangezien er meestal al een proces is waarbij de relevantie en de effectiviteit van het raamwerk ten minste jaarlijks worden beoordeeld. Wel hebben de organisaties aangegeven dat er nu meer aandacht is om de belangrijke wijzigingen in het raamwerk ook te vermelden in het hoofdstuk van het SOC-rapport waarin de beschrijving van het systeem van de serviceorganisatie is opgenomen, terwijl dat in het verleden misschien minder consistent werd gedaan.

Interne auditfunctie

In de ISAE 3402-standaard is de rol van de interne auditfunctie beter uitgewerkt dan bij SAS 70. Indien de serviceorganisatie beschikt over een interne auditfunctie, dient de serviceorganisatie inzicht te krijgen in de aard van de verantwoordelijkheden van de interne auditfunctie. Ook dient zij na te gaan welke werkzaamheden de interne auditfunctie uitvoert met betrekking tot het interne beheersingssysteem. De serviceauditor kan er onder bepaalde voorwaarden voor kiezen om gebruik te maken van de werkzaamheden van interne auditors. De serviceauditor blijft echter ook in deze gevallen de ongedeelde verantwoordelijkheid houden voor het oordeel in het SOC-rapport.

Ondanks de specifieke aandacht voor de interne auditor in de ISAE 3402-standaard is onze ervaring dat er in de praktijk nauwelijks sprake is van wijzigingen in de rol van de interne auditor bij SOC-rapportages.

Overige trends

Ondanks dat een wereldwijde standaard is geïmplementeerd voor SOC-rapportages, zien wij dat er nog steeds verzoeken worden gedaan om de rapportage op grond van de Amerikaanse standaard op te stellen. Een SSAE 16-rapport kan echter alleen door een CPA worden uitgevaardigd en dan alleen nog in het rechtsgebied waarin de CPA gecertificeerd is. De noodzaak voor een Amerikaans rapport is er door de wereldwijde standaard ook niet meer. De verschillen tussen ISAE 3402 en SSAE 16 zijn minimaal en daardoor is het SOC-rapport door de auditor van de Amerikaanse gebruikersorganisatie goed te gebruiken, ook indien deze gebruikersorganisatie onder de Sarbanes-Oxley wetgeving valt.

Tijdens de gesprekken met de serviceorganisaties hebben wij ook enige aandacht besteed aan het gebruik van tooling voor de vastlegging van interne beheersingsmaatregelen, managementtestactiviteiten en controleactiviteiten. Het beeld dat wij hebben aangetroffen bij de ondervraagde organisaties is erg diffuus. Alle smaken van uitsluitend beheersingsmaatregelen in een spreadsheet tot aan een volledig geïmplementeerde GRC-tool zijn wij tegengekomen. De komst van de nieuwe SOC-standaarden is in ieder geval geen trigger geweest voor serviceorganisaties om wijzigingen aan te brengen in de mate waarin zij gebruikmaken van tooling.

Wij hebben ook proberen te onderzoeken of de overgang naar ISAE 3402 een effect heeft gehad op de kosten per beheersingsmaatregel. Het blijkt echter dat, in ieder geval bij de ondervraagde serviceorganisaties, nauwelijks tot geen inzicht bestaat in de kosten op dat niveau.

Samenvatting

Uit ons inventariserende onderzoek blijkt dat de komst van ISAE 3402 niet heeft geleid tot grote verschillen ten opzichte van het SAS 70-tijdperk. De beoogde veranderingen, zoals meer aandacht voor risicomanagement en een bredere rol voor interne auditors, zijn nog niet over de gehele linie gerealiseerd door de serviceorganisaties. De nieuwe standaard heeft wel gezorgd voor meer duidelijkheid welk type rapport het meest geschikt is voor welke situatie. De communicatie daarover tussen gebruikersorganisatie en serviceorganisatie kan echter nog worden verbeterd, hetgeen de doeltreffendheid van het rapport ten goede zou komen. Wij zien derhalve nog een vrij groot potentieel voor verbeteringen in het rapporteren over uitbestede diensten.

Global reporting

Naast het verschaffen van helderheid over de vorm waarin serviceorganisaties verantwoording kunnen afleggen biedt ISAE 3402 nog een belangrijk voordeel, namelijk één wereldwijde standaard voor de beoordeling van de interne beheersing van serviceorganisaties. In het SAS 70-tijdperk was het nog zo dat deze van huis uit Amerikaanse standaard in verschillende delen van de wereld op andere manieren werd ingevuld. Met de ISAE 3402 heeft men één standaard waarvan men op globaal niveau gebruik kan maken. Dit biedt tevens perspectief voor wereldwijde gebruikersorganisaties die voor hun diensten op meerdere locaties vergelijkbare SOC-rapportages willen ontvangen.

In de afgelopen periode is niet alleen het management van serviceorganisaties druk bezig geweest om zijn begrip van SOC-rapportages te verbeteren om zo meer in control te raken, ook organisaties die overwegen om diensten uit te besteden zijn daarmee bezig. SOC-rapportages worden niet langer gezien als een kostenpost om met een aantal klanten zaken te kunnen doen; het is een vereiste geworden om werk te winnen, zeker bij de grote corporate organisaties. Deze organisaties hebben veelal vakkundige inkoopafdelingen of zelfs gespecialiseerde vendor-management-onderdelen die het hebben van een SOC-rapport als knock-out criterium stellen om überhaupt te worden meegenomen in (wereldwijde) proposaltrajecten. Bovendien kunnen deze vendor-managementafdelingen specifieke procedures ingeregeld hebben voor de beoordeling van SOC-rapportages, het opvolgen van eventuele tekortkomingen en het opnemen van specifieke beheersingsdoelstellingen en beheersingsmaatregelen.

Een SOC-rapport is naast een op de klant gerichte weergave van de serviceorganisatie en haar interne processen, een kans om klanten te herinneren waarom ze zaken doen met de serviceorganisatie en hoe de voortzetting van de dienstverlening waarde toevoegt aan de gebruikersorganisatie.

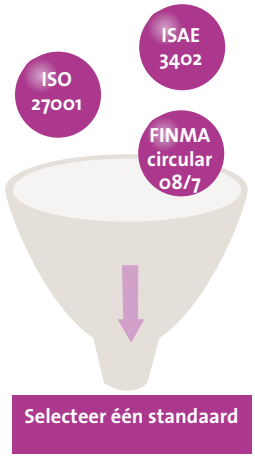
Wanneer grote wereldwijde organisaties processen hebben uitbesteed aan een serviceorganisatie met meerdere locaties dan kan het zo zijn dat voor elk van de locaties een apart rapport opgesteld dient te worden. Het is daarbij dan van belang dat deze rapportages beschikbaar zijn voor alle locaties, effectief zijn en – natuurlijk – betrekking hebben op dezelfde inhoud. Met andere woorden, de rapportages moeten identiek aan elkaar zijn met uitzondering van de locatie.

Onze ervaring dat er veel offerteverzoeken aan serviceorganisaties gedaan worden voor de wereldwijde portfolio van SOC-rapporten, volgt deze trend. We zien daarbij dat het noodzakelijk is dat de serviceorganisatie een passende serviceauditor heeft om effectieve rapportages te kunnen leveren die consistent zijn over de verschillende locaties. Deze serviceauditor beoordeelt niet alleen de SOC-rapportage en kan efficiencyvoordelen behalen door de leercurve, maar kan daarnaast ook additionele inzichten verschaffen in de samenhang en consistentie van de processen over de verschillende locaties heen.

Om een wereldwijde portfolio van SOC-rapportage te beheren is het voor een serviceorganisatie van belang een centre of excellence (COE) of vergelijkbaar onderdeel op te zetten. De COE is daarbij verantwoordelijk voor de volgende aspecten:

- *Awarenesstraining*. Voor een serviceorganisatie is het van belang dat niet alleen de mensen op de werkvloer vertrouwd zijn met het SOC-rapport, maar ook ondersteunende afdelingen als Marketing, Sales en Locatie Management dienen voldoende kennis te hebben.
- *Ondersteuning in proposaltrajecten*. Afdelingen als Marketing, Sales en zelfs Juridische Zaken zijn niet altijd

SOC-rapportages zijn een vereiste geworden om werk te winnen



Figuur 1. **Selectie van de juiste standaarden voor het wereldwijde beheersingsraamwerk[1].**

1 De circulaire 08/7 van de Financial Market Supervisory Authority (FINMA) beschrijft de voorwaarden voor de uitbesteding van bedrijfsactiviteiten binnen de bancaire sector.

bekend met de subtiele verschillen in SOC-rapportages en aanverwante zaken, zoals 'right-to-audit'-clausules en de verschillende mogelijke typen van SOC-rapporten. Tijdens proposaltrajecten kan het COE helpen met het uiteenzetten van de toegevoegde waarde die de SOC-rapportages bieden voor de potentiële klant.

- *Afhandelen van aanvragen voor het toepassen van de 'inclusive' methode.* Wanneer de serviceorganisatie wordt beschouwd als een subserviceorganisatie voor een klant die zelf ook weer een serviceorganisatie is, dan kan deze klant verzoeken om de diensten van de subserviceorganisatie onderdeel te laten zijn van zijn SOC-rapport (aangeduid als de 'inclusive' methode). Een voorbeeld hiervan is het geval dat een serviceorganisatie datacenter hosting services verleent aan een salarisverwerkende organisatie. De inclusive methode heeft specifieke eisen die moeten worden bewaakt om de subserviceorganisatie te beschermen.
- *Beheersing van de jaarlijkse controlecyclus.* Met elke rapportagecyclus moeten de systeembeschrijving en beheersingsmaatregelen worden beoordeeld en aangepast aan de huidige situatie. Dit in aanvulling op de coördinatie van het proces rond de managementbeweringen en van de logistieke details, waaronder tijd, resources en documentatie.

Het COE zal ook verantwoordelijk zijn voor de keuze welke rapportagestandaard de serviceorganisatie gebruikt om het interne beheersingsraamwerk op te baseren. Soms is het duidelijk welke standaard moet worden gebruikt en soms zijn er verschillende mogelijkheden die moeten worden geëvalueerd (zie figuur 1). In dit proces moeten ook lokale standaarden worden meegenomen die wellicht beter kunnen worden afgedekt door een internationale standaard.

Om te waarborgen dat de serviceorganisatie effectieve rapportages aan haar klanten kan verstrekken met dezelfde inhoud voor al haar locaties, dient de serviceorganisatie wereldwijd één beheersingsraamwerk te implementeren. Dit vereist dat het COE een raamwerk voorschrijft dat standaardeisen omvat, terwijl daarnaast een weloverwogen afweging moet worden gemaakt om eventuele lokale wet- en regelgeving mee te nemen.

Er zijn momenteel verschillende voorbeelden van serviceorganisaties die overgaan naar een wereldwijd raamwerk voor de SOC-rapportages. Dit proces (zie figuur 2) begint meestal met het combineren van de verschillende lokale kaders, hetgeen vaak een uitdaging is aangezien de lokale entiteiten een verschillende taal, lokale regelgeving of klantbehoeften kunnen hebben (zoals privacywetgeving, arbeidsrecht, milieuwetgeving). Bovendien kan de implementatie van de beheersingsmaatregelen tussen locaties verschillen door het gebruik van afwijkende ondersteunende IT-systemen.

In grotere organisaties is het onvermijdelijk dat er een aantal variaties tussen locaties bestaat. Deze variaties leiden tot verschillen tussen het wereldwijde beheersingsraamwerk en het beheersingsraamwerk van de verschillende locaties. Om te voorkomen dat dit resulteert in het rapporteren van deficiënties, moeten deze verschillen worden geanalyseerd en opgelost voorafgaand aan de rapportageperiode. Als alternatief kan het COE een vrijstellingsproces starten of compenserende controls implementeren.

Na elke implementatie van nieuwe beheersingsmaatregelen kan het enige tijd duren voordat deze maatregelen effectief werken. Om deficiënties van de effectieve werking van beheersingsmaatregelen zo vroeg mogelijk te detecteren kan een 'readiness assessment' worden uitgevoerd voor elk van de locaties. Een readiness assessment resulteert in een scorekaart waarop problemen per locatie worden aangetoond zodat het management een actieplan per locatie kan opstellen. Tevens wordt hiermee duidelijk welke locaties klaar zijn voor de audit op basis van het wereldwijde raamwerk.

Samenvatting

Wij zien dat de vraag vanuit de gebruikersorganisaties naar een wereldwijd raamwerk voor SOC-rapportages over verschillende locaties heen toeneemt. Het is daarbij voor de serviceorganisaties van belang dat ze op centraal niveau processen inrichten voor het aansturen van de audit, het creëren van awareness en om de variaties tussen de loca-

Figuur 2. **Proces naar een wereldwijd raamwerk voor SOC-rapportage.**

ties weg te nemen. Dit zal resulteren in een standaardaanpak en -raamwerk voor SOC-rapportages voor alle locaties om zo aan de wensen van de klanten te voldoen.

Conclusie

Met de implementatie van wereldwijde SOC-standaarden en de incorporatie daarvan in lokale standaarden hebben de regelgevende instanties de kaders geschapen voor transparante verantwoording over uitbestede dienstverlening. Uit het inventariserende onderzoek is naar voren gekomen dat de beoogde veranderingen van de nieuwe standaard in de praktijk nog niet in de gehele linie zijn opgepakt door serviceorganisaties. Er is daardoor nog een vrij groot potentieel voor verdere verbeteringen in het beheersingsraamwerk.

De nieuwe standaarden komen op het juiste moment, nu een trend ontstaat waarbij wereldwijde gebruikersorganisaties hun diensten voor meerdere locaties bij één serviceorganisatie willen onderbrengen en daarover vergelijkbare SOC-rapportages willen ontvangen. Het is daarbij voor de serviceorganisatie van belang dat zij een COE inregelt om het rapportageproces te coördineren en om de verschillen tussen locaties te beheersen. De trend richting global reporting in combinatie met het nieuwe palet aan wereldwijde standaarden voor SOC-rapportages biedt een extra kans voor communicatie tussen service- en gebruikersorganisatie en voor het beheersen van de risico's met betrekking tot de uitbestede diensten.

Literatuur

[Beek11] Drs. J.J. van Beek RE RA en drs. M.A. Francken RE RA CISA, *SAS 70 revised: ISAE 3402 will focus on financial reporting control procedures*, Compact 2011/0.

[KLLP12] KPMG LLP, *Effectively using SOC 1, SOC 2, and SOC 3 reports for increased assurance over outsourced operations*, 2012.

[KPMG10] KPMG Advisory N.V., *Praktijkgids SAS 70 deel III, SAS 70 verdwijnt: het moment voor herevaluatie*, 2010.

[KPMG12] KPMG Advisory N.V., *Praktijkgids 4, Service Organisatie Control-rapport, ISAE 3402*, 2012.

Over de auteurs

A.L. Perk MSc is adviseur bij KPMG Advisory. Hij houdt zich voornamelijk bezig met advies en assurance bij serviceorganisaties. Hierbij ligt de nadruk op het opstellen en toetsen van beheersingsmaatregelen voor Service Organisatie Control-rapportages.

A.M. Warner CISA is senior manager bij KPMG Advisory. Zij heeft ervaring met diverse wereldwijde SOC-rapportageportfolio's voor vastgoedbeheer en co-locatie datacenters. Zij is betrokken geweest bij de uitgave van het eerste KPMG SSAE 16-rapport in de Verenigde Staten en het eerste KPMG SOC 2-rapport in Nederland.

Drs. M.T. Fikke RE RA CISA is manager bij KPMG Advisory. Zijn werkzaamheden zijn gericht op audit- en adviesdiensten op het gebied van controls en assurance, waaronder SOC-rapportages. Hij is tevens als docent verbonden aan de IT Audit-opleiding aan de Universiteit van Amsterdam.

De regelgevende instanties hebben de kaders geschapen voor transparante verantwoording over de uitbestede dienstverlening