SAS met Abbas

Maarten Buijs en Ed Ridderbeekx

De redactie van de EDP Auditor sprak met Abbas Shahim, senior EDP Audit Manager bij KPMG IT Advisory, over SAS70: de Amerikaanse auditing standaard die definieert hoe een auditor de interne controle van een serviceorganisatie moet beoordelen ten behoeve van een uitbestedende organisatie. De belangstelling voor deze standaard en het gelieerde 'SAS70 rapport' is, zeker dankzij de toegenomen nadruk op goede en aantoonbare governance, groot. Een aantal praktijkervaringen...

Dit wordt een heel positief gesprek over SAS70, want jullie verdienen er vast veel geld mee.

'Dat klopt. Binnen KPMG valt de dienstverlening rondom SAS70 onder de service line IT attestation. Het is een term die we gebruiken voor het aanduiden van diensten op het gebied van assurance rondom IT governance. Het is een recent verbijzonderde service line, snel groeiend, en we verwachten er ook veel van in de toekomst. Dat heeft te maken met een toenemende behoefte aan zekerheid rondom IT governance, zekerheid rondom de kwaliteit van de dienstverlening van een service provider bij outsourcing en conformiteit met afspraken in het kader van service level agreements. Naast de traditionele worteling van SAS70 in de financial audit zien we tegenwoordig een breder gebruik. Natuurlijk is het zo, dat een externe accountant van een uitbestedende organisatie zich nog steeds prettig zal voelen als hij de beschikking heeft over een SAS70 rapport, maar de doelgroep voor zo'n verklaring is inmiddels veel breder. We praten daarom ook veel meer over een conformity report."

Wij kenden al Third Party Mededelingen (TPM's). Als je die afzet tegen SAS70, zijn we er dan op vooruit gegaan?

'In vergelijking met TPM's vind ik SAS70 in sommige opzichten wel een verbetering. Het geeft bijvoorbeeld de mogelijkheden van een wat strakkere uitvoering van je opdracht. Wel is het zo, dat het gemiddelde beeld op de markt is, dat SAS70 een uitermate formeel traject is, en veel minder detailinformatie geeft over beheersing dan een TPM. Dat kun je zien als je bijvoorbeeld naar een typisch Amerikaans SAS70 rapport kijkt. Het komt voor dat men daar, in sectie 3, waarin de resultaten van de uitgevoerde testwerkzaamheden staan, volstaat met de opmerking of er in een test afwijkingen of uitzonderingen geconstateerd zijn: exception noted, ja of nee. Een TPM geeft traditioneel veel meer detailinformatie over bevindingen. Binnen KPMG hebben we dat geconstateerd en omdat veel van onze klanten gewend waren aan de uitgebreide informatie in een TPM en ook veel waarde hechten aan die informatie, hebben we een onderscheid gemaakt in twee typen SAS70 rapporten, een "kale" variant, en een uitgebreidere variant, met veel meer detailinformatie, die meer aansluit op TPM's. Qua rapportage is er een verschil wat de inhoud van sectie 3 betreft. Dit onderdeel van het SAS70-rapport bevat uitgebreidere informatie en geeft onder andere de bevindingen weer. Het achterliggende werk is echter precies hetzelfde.'

Men zegt wel dat SAS70 in feite een 'lege doos' is, en dat je erin kunt verpakken wat je wilt.

'Tot op zekere hoogte klopt dat. Zoals ik al zei, de perceptie rondom SAS70 is dat het een heel formele en voorgeschreven standaard is. Maar dat is schijn. Zelfs al heb je gekozen om een SAS70 traject in te gaan, dan moet je nog steeds heel veel keuzes maken. Het is goed om te beseffen dat er drie belangrijke elementen spelen rondom SAS70: scoping, raamwerk, en rapportagestructuur. SAS70 op zichzelf geeft eigenlijk alleen ten aanzien van dat laatste veel handreikingen, alhoewel zelfs die structuur strikt genomen geen voorschrift is. Over scoping en raamwerk moet je hoe dan ook met de uitbestedende organisatie afstemmen. En ook voor de betrokken auditor geldt, dat in het team heel goede afspraken gemaakt moeten worden om uiteindelijk het auditor's report consistent te kunnen opstellen.'

Sectie 2 van een SAS70 rapport bevat de beschrijving van de beheerdoelstellingen en beheersmaatregelen die de serviceorganisatie heeft genomen. Welk raamwerk gebruik je om deze beschrijving te maken?

'Je moet vooropstellen dat de diepgang van die beschrijving afhankelijk is van de assurance-behoefte van de uitbestedende organisatie. De SAS70 guidance adviseert toepassing van COSO als model voor de beschrijving van beheersmaatregelen, maar verplicht is dat niet. In principe kun je je toevlucht nemen tot bijvoorbeeld COSO in combinatie met CobIT als achterliggend model. De keuze die je maakt moet geworteld zijn in de scoping van je opdracht. Om een voorbeeld te geven: als de scope van je SAS70 met name is gericht op de domeinen van IT governance zoals die door het IT Governance Institute beschreven zijn, dan is het niet zo'n gekke keuze om naast COSO ook CobIT te gebruiken als raamwerk voor het beschrijven van je controledoelstellingen en controlemaatregelen. In de praktijk van KPMG gebruiken we vaak de general IT controls als uitgangspunt, en breiden dat uit, al naar gelang de behoeften van de klant. Het is heel belangrijk je af te vragen wie de stakeholders bij de uitbestedende organisatie zijn; denk hierbij aan de externe accountant, een audit committee, een toezichthouder. Zij zullen immers allen, vanuit hun eigen perspectief, in het SAS70 rap-

In een artikel in de EDP Auditor 2006-4 discussieerden enkele materiedeskundigen over SAS70 en Third Party Mededelingen. Binnen het NiVRA/NOREA is een werkgroep actief met dezelfde materie. Eind oktober verschijnt een boek van de hand van Ronald Jonker, getiteld 'Third Party Mededelingen en SAS 70-onderzoeken', bij Sdu Uitgevers te Den Haag.

port terug willen zien dat aan hun assurance-behoefte is voldaan. Het raamwerk moet geworteld zijn in bestaande standaarden, maar voldoende flexibel zijn om alle stakeholders tevreden te kunnen stellen.'

Pratend over de scoping van een SAS70: als jullie als auditor optreden voor de serviceorganisatie, neem je dan die scoping als een gegeven, of ga je ook nog na of die scoping in overeenstemming is met de assurance-behoefte van de uitbestedende organisatie?

'Wij stellen dat wel altijd voor. In principe is het zo, dat de serviceorganisatie verantwoordelijk is voor secties 2 en 4 van het SAS70-rapport, en de auditor voor het auditor's report in sectie 1 en voor de presentatie van de testresultaten in sectie 3. Maar de praktijk leert dat er rondom SAS70 veel onduidelijkheid bestaat. Zeker bij klanten die voor het eerst met SAS70 in aanraking komen, pleiten we voor een zogenaamde diagnostic review, omdat men de neiging heeft het traject van SAS70 te onderschatten. In die diagnostic review bereiden we de organisatie voor en geven we duidelijkheid over wat er verwacht wordt. Het is, zou je kunnen zeggen, ook een traject van bewustwording voor de service provider; we maken duidelijk dat je een aantal zaken goed op orde moet hebben om aantoonbaar te kunnen maken dat je beheersmaatregelen voldoende zijn. Ook gaan we met de service provider in dialoog over de scoping van de SAS70, over het te hanteren raamwerk, en over de structuur en invulling van de secties in het rapport. Dat is er allemaal op gericht om niet halverwege het traject voor onaangename verrassingen komen te staan.'

En in hoeverre zou je als gebruiker van een SAS70-rapport, als uitbestedende organisatie dus, betrokken moeten zijn bij de scoping?

'Als je het mij vraagt: uitermate intensief. Als uitbestedende organisatie gebruik je het SAS70-rapport om een bepaalde mate van zekerheid te krijgen over de beheersing van processen die onder jouw verantwoordelijkheid vallen. Dat betekent niet alleen dat de scope van de SAS70 moet aansluiten met jouw assurance-behoefte, maar ook dat je eventuele tekortkomingen die gerapporteerd worden, kunt vertalen naar een impact op jouw bedrijfsvoering. In algemene zin kan de auditor in zijn verklaring wel iets zeggen over die impact, maar echt alleen in algemene zin. Vanuit het perspectief van de serviceorganisatie is het ook van belang een dialoog te hebben met je afnemers. Vaak zijn die serviceorganisaties een beetje "auditmoe" geworden, ze worden benaderd door verschillende klanten met vragen rondom de beheersing van uitbestede processen. Een SAS70-rapport kan dan uitkomst bieden, maar de assurance-behoefte van de klanten hoeft niet gelijk te zijn. Er zijn service providers die dan, in overleg met hun belangrijkste klanten, komen tot een soort "basis-scoping" die voor elke klant noodzakelijk is. Vervolgens kan met individuele klanten een afspraak worden gemaakt over specifieke uitbreidingen daarop binnen het kader van de SAS70-verklaring.' ■