Han Boer (KPMG): 'Een SAS 70-rapport mag niet buiten de kring van gedefinieerde gebruikers worden gepubliceerd.'

SAS 70 kent geen normenkader, zelfs geen voorgeschreven methode van toetsing.

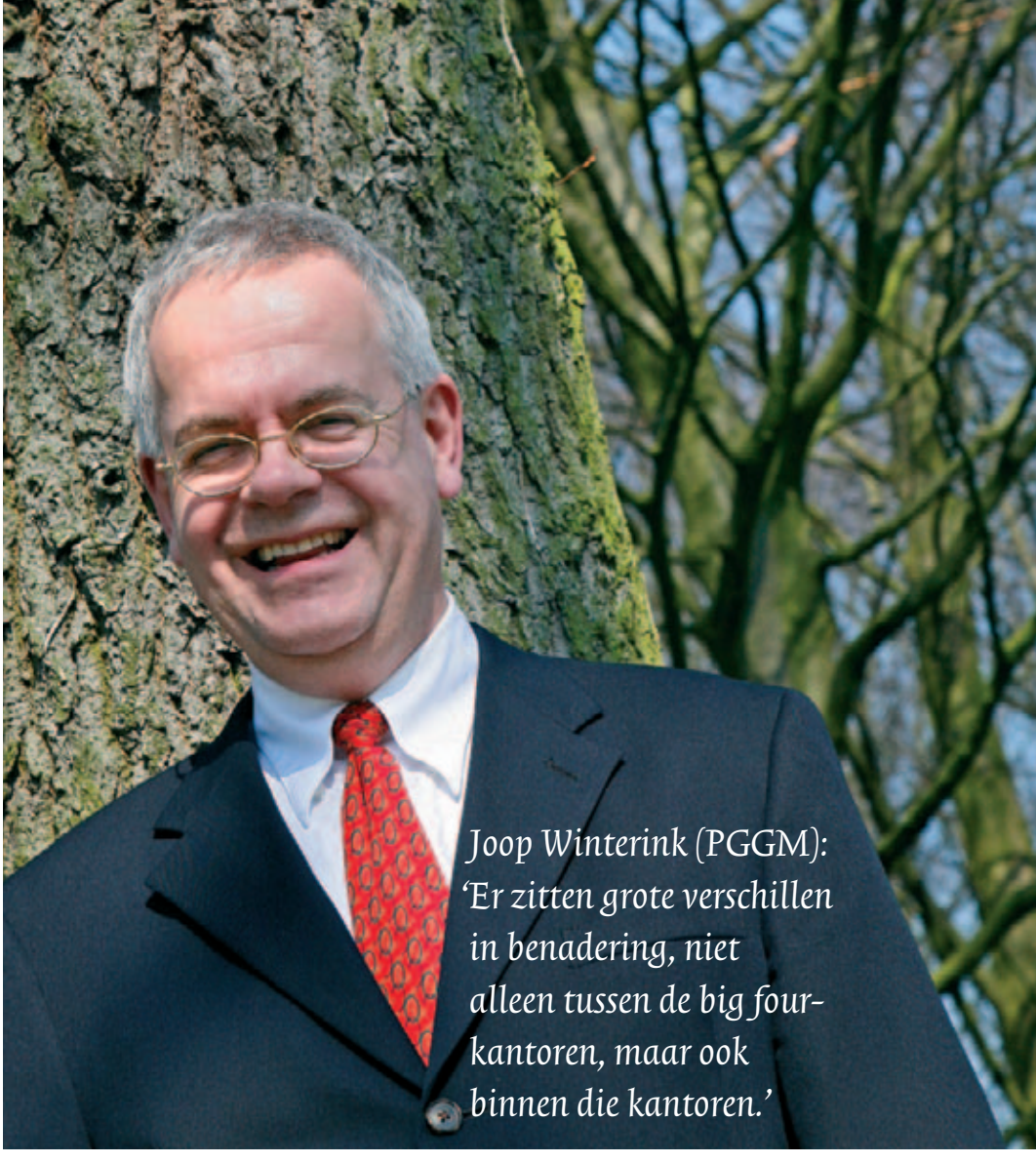
SAS 70: geen betonnen **reddingsvesten graag**

Met de trend naar meer uitbesteding groeit ook de behoefte aan zekerheid over de uitbestede processen. Bijvoorbeeld bij pensioenfondsen die hun vermogensbeheer overdragen aan een derde partij. De Amerikaanse controlestandaard SAS 70 mag zich dan ook verheugen in een groeiende belangstelling. Er zijn echter nogal wat misverstanden over.

NART WIELAARD

Op 6 maart 2007 komt op de redactie een persbericht binnen van pensioenuitvoerder en vermogensbeheerder Mn Services. 'Mn Services is geheel SAS 70 Type II gecertificeerd', zo luidt de eerste zin, die even verderop wordt vervolgd met de opmerking 'Mn Services voldoet volgens de verklaring aan de strengste *normen* die internationaal aan proces- en risicobeheersing worden gesteld' (cursivering NW). Dat gaat er bij de (potentiële) klanten van Mn Services natuurlijk in als koud bier op een heet strand. Een pensioenfonds of andere institutionele partij wil immers graag de

Het hebben van een SAS 70-rapport heeft wel degelijk uitstraling in de markt.



Joop Winterink (PGGM): 'Er zitten grote verschillen in benadering, niet alleen tussen de big four-kantoren, maar ook binnen die kantoren.'

zekerheid dat ze met een gerust hart processen kunnen uitbesteden. Er is echter een klein probleempje: het persbericht klopt niet. Sterker nog: eigenlijk hoort de accountant in te grijpen en aan te dringen op het intrekken van dit persbericht, omdat er een verkeerde schijn wordt gewekt bij de lezer.

Kant noch wal

Wat is het geval? Er leven nogal wat misverstanden rondom de toepassing van SAS 70. Een van de hardnekkigste is dat SAS 70 een certificaat is. Het geval van Mn Services staat bepaald niet op zichzelf: een zoekopdracht op Google leert dat tientallen organisaties er vol trots kond van doen in het bezit te zijn van een SAS 70-certificaat. De vergelijking met een certificaat - zoals ISO - raakt echter in feite kant noch wal, onder andere omdat een SAS 70-rapport voor een specifieke doelgroep - de klanten van de serviceorganisatie - wordt opgesteld, en niet voor algemeen gebruik. Han Boer, KPMG-partner en SAS 70-specialist, legt het uit: "Een SAS 70-rapport voorziet - als het goed is - in een behoefte aan zekerheid die bij een afnemer leeft. Het is dus geen algemeen geldende norm, maar een maatwerk antwoord op hun vragen. Daarom mag een SAS 70-rapport ook niet buiten de kring van gedefinieerde gebruikers worden gepubliceerd. We definiëren in onze rapportages zelfs altijd een expliciet verbod op verdere verspreiding." Boer wijst daarmee ook op het andere grote verschil met een certificaat: SAS 70 kent geen normenkader, en kent zelfs geen voorgeschreven methode van toetsing. Hoewel de standaard een aantal formaliteiten kent - zoals de voorgeschreven structuur van het rapport en de bewoordingen van het *auditor's report* - zijn de grenzen van het onderzoeksobject van een SAS 70-rapport (in jargon: de *scoping*) niet voorgeschreven.

Reddingsvest

Hoe gek het ook moge klinken: een organisatie die een SAS 70-rapport heeft, is zeker niet per definitie een organisatie die de processen goed beheerst. Het is immers mogelijk dat een organisatie een SAS 70-rapport opstelt met zeer lage ambities ten aanzien van de beheersingsdoelstellingen. De auditor heeft dan 'slechts' de taak om na te gaan of de beheersingsmaatregelen in lijn liggen met die doelstellingen.
Boer legt het uit aan de hand van een metafoor: het betonnen reddingsvest. "Een betonnen vest - het SAS 70-rapport met de lage ambities - kan volgens de hoogste eisen tot stand zijn gekomen zodat de accountant kan aftekenen, maar beschermt op geen enkele manier tegen verdrinking. Of in het geval van SAS 70: tegen onvoldoende grip op de uitbestede processen. Ook kan de scope te beperkt zijn, als het rapport bijvoorbeeld maar enkele processen van de uitbestede activiteiten beschrijft. Ook dit is te verduidelijken met de metafoor van het reddingsvest: op de verpakking staat dan 'reddingsvest', maar uit de specificaties blijkt dat het gaat ▶

Foto of film

Er zijn twee typen SAS 70-rapporten:

*Type I: momentopname (een **foto** van de beheersingsmaatregelen op een bepaald moment)*
Een type I-rapport beschrijft de getroffen beheersmaatregelen (*controls*) die op een bepaald moment zijn geïmplementeerd, zodanig dat de beheersdoelstellingen (*control objectives*) kunnen worden bereikt. De beschrijving wordt ondersteund met een auditor's report dat aangeeft dat de maatregelen toereikend zijn om de beheerdoelstellingen te realiseren en dat deze op de specifiek genoemde datum daadwerkelijk waren ingevoerd.

*Type II: uitspraak over een bepaalde periode (een **film** van de werking van de beheersmaatregelen over een bepaalde periode)*
Een type II-rapport heeft betrekking op een periode - normaal gesproken minimaal zes maanden - waarin de beschreven beheersmaatregelen aanwezig waren om de beheersdoelstellingen doorlopend te bereiken. Ook het auditor's report is uitgebreid met een oordeel over de werking van de maatregelen in deze periode.

Wanneer over SAS 70 wordt gesproken, wordt meestal gedoeld op rapporten van het type II.

om een vest dat alleen geschikt is voor kinderen tot twintig kilogram."

Grote verschillen

Kortom: de inhoudelijke eenduidigheid is ver te zoeken. Hier en daar klinkt dan ook de roep om via andere weg de gewenste zekerheid te verkrijgen, bijvoorbeeld door een third party-mededeling.
Dat is geen goed idee vindt Joop Winterink. Hij is hoofd Internal Audit van PGGM en zit daarmee in de rol van 'lezer' van SAS 70-rapporten: "Er zijn goede SAS 70-rapporten, en er zijn slechte. Het probleem is dat er op inhoudelijk niveau geen enkele afspraak is over diepgang en scope. Ik ben dan ook geen tegenstander van SAS 70, maar vind wel dat er wat moet veranderen. Mijn perceptie is dat partijen die al langer een SAS 70-rapport afgeven, meer diepgang hanteren en betere informatie opnemen over het proces en de resultaten van risicobeheersing. Hier in Nederland zitten er grote verschillen in benadering, niet alleen tussen de big four-kantoren, maar ook binnen die kantoren. Daar moeten accountants samen aan werken."

Hans van Hoogenhuijze: 'Je moet kritisch zijn op de vraag wanneer een SAS 70-rapport rationeel is, en wanneer er andere mogelijkheden zijn om de zekerheid te verkrijgen.'

Nuance

Boer: "De kwaliteitsborging ligt nu feitelijk bij de ontvangende organisatie. Het management van de uitbestedende organisatie moet zelf - desgewenst ondersteund door specialisten - door lezing van het SAS 70-rapport beoordelen of en in hoeverre de beheersing voldoet aan de eisen."
Winterink, die in het najaar van 2006 een zogenaamde GAIN Round Table-conferentie over dit thema organiseerde voor interne accountants: "Ik kan uit een SAS 70-rapport vaak onvoldoende lezen hoe een organisatie de risicobeheersing precies voor elkaar heeft, hoe dit door de accountant is getest, de normstelling die is gebruikt en welke bevindingen hieruit zijn voortgekomen."
Overigens past bij dit alles een nuance, om een al te pessimistisch beeld te voorkomen. In de praktijk zegt het hebben van een SAS 70-rapport namelijk wel degelijk wat over het niveau van de interne beheersing. Over het algemeen durven namelijk alleen organisaties met een solide systeem voor beheersing het aan om een SAS 70-traject te beginnen. Het hebben van een SAS 70-rapport heeft dan ook wel degelijk uitstraling in de markt.

Hoge kosten

De kosten van het verkrijgen van een SAS 70-rapport zijn vaak hoog, en ook dat leidt hier en daar nog wel eens tot gemor over het welbekende schieten met een kanon op een mug. Hans van Hoogenhuijze, registeraccountant, wijst erop dat een SAS 70-traject in elk geval geen vanzelfsprekendheid moet zijn: "Je moet kritisch zijn op de vraag wanneer een SAS 70-rapport rationeel is, en wanneer er andere mogelijkheden zijn om de zekerheid te verkrijgen. En als je dan toch besluit tot een SAS 70-traject, dan moet je ook weer goed oppassen wat je doet."
Boer sluit zich daarbij aan: "Ook een zogenaamd 'rapport met specifiek overeengekomen werkzaamheden' kan in een aantal gevallen volstaan. En soms is het mogelijk om bij de uitbestedende organisatie zelf voldoende zekerheid te krijgen door het uitvoeren van verbandscontroles. Dan hoef je dus helemaal niet langs bij de uitvoerende organisatie. Per situatie moet je de beste optie selecteren. Maar hoe dan ook, we kunnen er niet omheen dat SAS 70 veel uitstraling heeft in de markt."

SAS 70 in vogelvlucht

In een SAS 70-rapport beschrijft een **serviceorganisatie** hoe zij processen beheerst. Het rapport definieert beheersdoelstellingen en het geheel van (controle)maatregelen dat de organisatie neemt om die doelstellingen te realiseren.

Een **externe auditor** voegt een rapportage toe aan dit rapport, waarin hij ingaat op de realisatie van deze beheersdoelstellingen, beschrijft welke toetsingsmaatregelen hij heeft uitgevoerd en wat het resultaat van zijn werkzaamheden is.

De ontvanger van het rapport - de **uitbestedende organisatie** - beoordeelt de bevindingen in dit rapport en moet op basis daarvan zelf vaststellen of de beheersing van de uitbestede processen op een niveau ligt dat voldoet aan zijn normen.
Ook de accountant die verantwoordelijk is voor de jaarrekeningcontrole van de uitbestedende organisatie kan het rapport gebruiken om inzicht te krijgen in de administratieve organisatie en interne controle van de serviceorganisatie.

Aantoonbaarheid

Over die hoge kosten ten slotte: de oorzaak daarvan ligt vooral in het *prove me*-karakter van SAS 70. De beschrijving van de administratieve organisatie en interne controle moet meer zijn dan een 'papieren tijger', maar aantoonbaar functioneren. In de praktijk schort het vaak juist aan die aantoonbaarheid: de auditor kan dan niet vaststellen dat de maatregelen ook hebben gewerkt.
Boer: "Het aantoonbaar vastleggen van controles vergt vaak meer discipline van de organisatie, en is dan ook een van de belangrijkste - en kostbaarste - onderdelen van het project. Dit proces wordt in de praktijk - vooral door commerciële managers met weinig controlebewustzijn - nogal eens onderschat." ■