# Verbetermogelijkheden bij de totstandkoming van een SAS 70-rapport


**Drs. A.R.J. Basten RE**
is senior manager bij KPMG IT Advisory. Zijn ervaring ligt voornamelijk op het gebied van het adviseren over en beoordelen van applicatieve beheersingsmaatregelen en de algemene computercontroles (IT General Controls). Deze ervaring is voornamelijk opgedaan bij het uitvoeren van of adviseren over jaarrekeningcontrole-, SOx- en SAS 70-opdrachten.
basten.fons@kpmg.nl

**C.F. J. Hoffman RE RA**
is senior manager bij KPMG IT Advisory en is gespecialiseerd in risk- en compliancevraagstukken en betrokken bij diverse SAS 70-opdrachten als adviseur en auditor.
hoffman.chris@kpmg.nl


**Drs. Fons Basten RE en Chris Hoffman RE RA**

Bij uitbesteding van processen wordt in veel gevallen een SAS 70-rapport vereist van de serviceorganisatie. Het opstellen van het SAS 70-rapport door het management en de certificering door een auditor vergt veelal een forse investering. In dit artikel geven de auteurs op basis van hun praktijkervaring inzicht in de mogelijkheden om deze investering te beperken en de toegevoegde waarde van het SAS 70-rapport te vergroten.

## Introductie

Organisaties vragen tegenwoordig bij uitbesteding van hun processen steeds vaker een SAS 70-rapport aan hun serviceorganisatie(s). Het SAS 70-rapport biedt op een gestructureerde wijze inzicht in de mate waarin het uitbestede proces wordt beheerst. De vraag naar SAS 70-rapporten is sterk toegenomen doordat Sarbanes Oxley (SOx)-plichtige organisaties voor al hun materiële uitbestede processen dienen te beschikken over een SAS 70-rapport. Wij zien ook in de praktijk dat organisaties van hun serviceorganisaties een SAS 70-rapport krijgen opgestuurd, zonder dat ze daarom hebben gevraagd. De serviceorganisatie wil naar haar huidige en potentiële klanten, maar vooral naar de markt toe haar professionaliteit uitstralen. En dat terwijl SAS 70 ooit bedoeld was als een 'in control statement' voor de auditor.

Inmiddels zijn vele organisaties gewend geraakt aan SAS 70. Voor bijvoorbeeld de pensioenbranche geldt dat in enkele jaren tijd SAS 70 is uitgegroeid van een 'nice to have'- tot een 'must have'-instrument. Verwonderlijk is dat niet, aangezien de belangen bij uitbesteding groot zijn en in deze branche de verantwoordelijkheid richting pensioengerechtigden zwaar weegt. Deze ontwikkeling geldt voor meer sectoren en zal in de toekomst steeds breder gaan gelden.

Het uitbrengen van een SAS 70-rapport vergt echter veelal een forse investering. Voor het proces om te komen tot een SAS 70-rapport kan een aantal mogelijkheden worden geïdentificeerd voor het verlagen van deze investering. Dit proces kan worden aangeduid met het rationaliseren van het SAS 70-rapport. Van Dale omschrijft rationalisatie als: '(econ.) een zo gunstig mogelijke organisatie van de productie met het doel de prestatie te verhogen en kracht, tijd en geld te besparen'. Met andere woorden: kan er een effec-

tievere set van controls worden vastgesteld, zijn er manieren om beter met resources om te springen, het SAS 70-rapport leesbaarder te maken en de kosten van 'assurance' te verlagen?

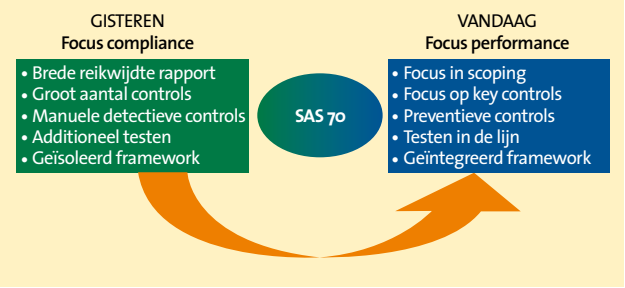
## Ontstaan en achtergrond van SAS 70

Het SAS 70-rapport is ontstaan om een rapportagevorm aan te reiken die organisaties kunnen hanteren om de kwaliteit van de beheersing van hun processen aantoonbaar te maken voor de gebruikersorganisaties. De kracht van het SAS 70-rapport is dat deze wordt getoetst door een auditor en de resultaten daarvan worden opgenomen in het rapport. Hierdoor krijgt het rapport een hoog betrouwbaarheidshalte. Een groot voordeel van een serviceorganisatie om over te gaan tot een SAS 70-rapport is dat zij op die manier de (vele) audits van de auditors van de gebruikersorganisaties kan voorkomen. Weliswaar vergt het verkrijgen van een SAS 70-rapport een veel grotere inspanning dan een audit door een auditor van de gebruikersorganisatie, maar wanneer een dergelijke audit meerdere keren wordt uitgevoerd op initiatief van verschillende gebruikersorganisaties, is het redelijk eenvoudig om het voordeel van een SAS 70-rapport aan te tonen.

In de meeste gevallen komt vaak nog een behoorlijk aantal verbeterpunten aan het licht. Om te voorkomen dat deze verbeterpunten aan de gebruikersorganisatie worden gecommuniceerd en om de kosten van de SAS 70 te beperken voert de serviceorganisatie veelal eerst een kwaliteitsverhogend traject uit. Daarmee is SAS 70 ook een middel geworden om de AO/IC te verbeteren.

Nadat de eerste SAS 70-rapporten het daglicht hadden gezien, ontstonden ook nieuwe vragen bij de uitbestedingstrajecten. Kan een SAS 70-rapport door de serviceorganisatie worden overgelegd en zo nee, per wanneer zou dat wel kunnen? Als een SAS 70-rapport kan worden overgelegd, wat zijn dan de negatieve bevindingen van de auditor? Daarmee kreeg het SAS 70-rapport niet alleen toegevoegde waarde voor de huidige gebruikersorganisaties, maar werd het ook een steeds belangrijker vereiste in uitbestedingstrajecten.
Zoals eerder gesteld vergt een SAS 70-rapport veelal een forse investering. In de navolgende paragraaf zijn verbetermogelijkheden opgenomen om deze investering te verlagen.

**SAS 70 is in diverse branches uitgegroeid van een 'nice to have'- tot een 'must have'-instrument**




Figuur 1. **Vijf gebieden met verbetermogelijkheden.**

## Vijftal verbetermogelijkheden

In deze paragraaf komen vijf aspecten aan de orde waarop verbetermogelijkheden zijn te realiseren binnen het SAS 70-proces (zie figuur 1).

Voor deze gebieden bestaat een volgordelijkheid. Allereerst het samenstellen van het SAS 70-rapport. Welke processen worden opgenomen (eerste aspect) en welke beheersingsmaatregelen worden geïdentificeerd vanuit deze processen (tweede en derde aspect)? Daarna verschuift de aandacht naar het optimaliseren van het proces door het verbeteren van de wijze waarop het management de beheersingsmaatregelen documenteert en test, en het integreren van het SAS 70-framework met de overige control frameworks (vierde en vijfde aspect).

### Betere scoping, beter rapport

Een belangrijke 'quick win' is te behalen bij het vaststellen van de reikwijdte (scoping) van het SAS 70-rapport. Deze dient optimaal aan te sluiten op de behoefte van de gebruikersorganisatie(s). Onze ervaring is dat onvoldoende overleg plaatsvindt met de ontvangers van het SAS 70-rapport, waardoor de scope van de SAS 70 doorgaans vrij breed wordt en ook (deel) processen worden meegenomen die minder relevant zijn voor de gebruikersorganisatie. Is de scope te breed, dan ontstaan er hogere interne en externe controlekosten of kan de organisatie worden verweten niet de essentie van haar eigen dienstverlening te onderkennen. Wanneer men besluit om bepaalde processen niet mee te nemen in het SAS 70-onderzoek scheelt dat al veel werk. Een duidelijker afbakening van het SAS 70-onderzoek bevordert ook de leesbaarheid van het SAS 70-rapport. Een deel van het bos is immers weggekapt en de belangrijkste bomen staan nog overeind. Ook dat is winst. Meer overleg met de gebruikersorganisatie over de scoping kan dus een grote kostenbesparing opleveren. Te allen tijde moet natuurlijk worden voorkomen dat essentiële onderdelen van de dienstverlening niet worden afgedekt, want dan bereikt het rapport zijn doel niet. Indien de SAS 70 wordt gevraagd als gevolg van SOx-vereisten dient de scoping direct te worden overgenomen en is er geen ruimte voor onderhandeling. Is dit niet het geval, dan

moeten beide partijen om de tafel om de scoping te bespreken.

Uit de 'SAS 70 Rondetafel voor de financiële sector', die KPMG heeft georganiseerd in juni 2007, bleek dat de communicatie tussen de serviceorganisaties en de gebruikersorganisaties beperkt is. Dit wordt onderstreept door de uitkomsten van een NIPO-onderzoek in het kader van het *KPMG Pensioenenboekje 2007*, waaruit bleek dat twintig procent van de ondervraagde pensioenfondsen niet eens weet of de serviceorganisatie beschikt over een SAS 70-rapport. Uit het voornoemde rondetafelgesprek bleek ook dat de gebruikersorganisaties best wat mondiger zouden mogen zijn. Een betere communicatie tussen de gebruikersorganisatie en de serviceorganisatie zal leiden tot verbetermogelijkheden en wederzijds tot een beter begrip van elkaars situatie. Ook zal een gezamenlijk framework de communicatie tussen beide partijen verbeteren en de ontvangende partij meer toegevoegde waarde geven.

### Zijn de 'key controls' voldoende 'key'?

De huidige SAS 70-rapporten worden gekenmerkt door een omvangrijke set met controls (beheersingsmaatregelen) per proces. Bij twijfel wordt liever een control extra meegenomen. De SAS 70-praktijk, maar tevens ook de laatste SOx-ontwikkelingen laten zien dat er mogelijkheden zijn om de SAS 70-werkzaamheden efficiënter aan te pakken met dien verstande dat de behaalde assurance uit het 'control framework' intact blijft en soms zelfs verbetert. Daartoe is het nodig om de controls te heroverwegen: zijn de gekozen 'key controls' wel noodzakelijk voor het verkrijgen van zekerheid omtrent de beheersingsdoelstelling?

Het voordeel van een meer uitgebreide verzameling van controls is de compenserende werking hiervan. Wanneer een control niet effectief blijkt te zijn, kan de controledoelstelling toch worden gehaald omdat de compenserende zekerheid beschikbaar is in de vorm van een aantal ogenschijnlijk 'overtollige' controls. De meeste serviceorganisaties die gebruikmaken van een SAS 70-rapport doen dit nu al voor enkele jaren. De in die jaren opgebouwde ervaring biedt dan afdoende zekerheid om afscheid te nemen van de compenserende, overtollige controls die bij de introductie van de SAS 70 wellicht goed van pas zijn gekomen.

Uiteindelijk zullen door het verlagen van het aantal controls de test- en reviewwerkzaamheden afnemen waardoor de investering zal dalen. Kostenreductie wordt dus mogelijk door het doelgerichter opstellen en onderhouden van het control framework. Het verlagen van het aantal controls kan worden bereikt door een gerichte selectie van de controls, maar ook door het verleggen van de aandacht van signaleren (detectieve controls) naar voorkomen (preventieve controls).

### Van detectief manueel naar preventief geautomatiseerd

In de meeste SAS 70-frameworks zijn voornamelijk nog zogenaamde detectieve manuele controls benoemd. Onder detectief wordt verstaan dat de fout pas na optreden wordt gedetecteerd, waarna de fout wordt gecorrigeerd. Met manueel wordt bedoeld dat de control een menselijke controlehandeling is. Een voorbeeld hiervan is de controle op het vierogenprincipe aan de hand van de parafen. Beter zou het zijn om 'preventieve geautomatiseerde' controls te selecteren. Met preventief wordt bedoeld dat de fout wordt voorkomen. Geautomatiseerd is, voornamelijk bij routinematige processen, beter omdat de controlehandeling altijd, en ook altijd goed (volgens de specificaties) wordt uitgevoerd. Daarbij zijn, op de investering in het ontwikkelen van de geautomatiseerde controls na, geen arbeidskosten meer noodzakelijk. Hierbij kan worden gedacht aan een geprogrammeerd vierogenprincipe waarbij de betrokkenheid van een andere gebruiker (conform de competentietabel) wordt afgedwongen.

**Door het overgaan van detectieve manuele naar preventieve geautomatiseerde controls neemt de foutgevoeligheid van het proces af**

Een positief gevolg is dat door het overgaan van detectieve manuele naar preventieve geautomatiseerde controls de foutgevoeligheid van het proces afneemt. In plaats van achteraf vaststellen dat de uitkering geautoriseerd is door de juiste persoon met de juiste paraaf, kan dit proces zodanig worden geautomatiseerd dat alleen de juiste persoon de uitkering kan goedkeuren. Voorkomen is nu eenmaal beter dan genezen. Kortom, hier liggen belangrijke rationalisatiekansen: lagere foutkans en risico en er zijn dus minder controls en testwerkzaamheden nodig. Daarbij hoeft het vaststellen van het bestaan en de werking van geautomatiseerde controls binnen het SAS 70-onderzoek door de auditor maar eenmalig te geschieden. Een belangrijke randvoorwaarde hiervan is wel dat de IT General Controls de continue en betrouwbare werking van de geautomatiseerde controls kunnen waarborgen. Het SAS 70-rapport dient deze General IT Controls ook te beschrijven. Van deze controls dient onverkort het bestaan te worden vastgesteld en de werking te worden getest net als van de andere controls.

Uit het NIPO-onderzoek dat is uitgevoerd in het kader van het *KPMG Pensioenenboekje 2007* blijkt dat 47 procent van de ondervraagde serviceorganisaties het SAS 70-traject als een (zeer) belangrijk middel ziet om haar interne beheersing te ver-

beteren. Hoe lopen de processen exact en wat vindt de auditor er eigenlijk van die over de processen moet oordelen? SAS 70 'nieuwe stijl' maakt zaken expliciet en geeft helder aan waar het proces voor verbetering vatbaar is en kan zelfs leiden tot een mentaliteitsverandering wat betreft de wijze waarop men intern omgaat met risico's. Dit verbeteringstraject wordt door veel organisaties gezien als een belangrijk bijproduct naast het bieden van zekerheid aan gebruikersorganisaties over de door hen uitbestede processen.

Een andere verbeterslag is het meer gebruikmaken van entity level controls. Binnen een proces zijn vaak talrijke operationele controls en maar enkele of geen entity level controls dan wel procesoverstijgende controls geïdentificeerd. Afhankelijk van de controledoelstelling kunnen enkele procesoverstijgende controls een deel van de zekerheid aanreiken voor het realiseren van een controledoelstelling. Het testen van enkele procesoverstijgende controls is beduidend minder werk dan meerdere operationele controls. Hierbij kan worden gedacht aan een gedetailleerde cijferanalyse naar de resultaten van verschillende bedrijfsonderdelen, producten of processen, waaraan veel zekerheid kan worden ontleend. Natuurlijk gaat dit niet altijd op. Wanneer bijvoorbeeld de operationele controls bestaan uit preventieve geautomatiseerde controls, zou het efficiënter kunnen zijn om deze te testen in plaats van de procesoverstijgende handmatige controls. Kortom, je moet blijven nadenken om deze voordelen te behalen.

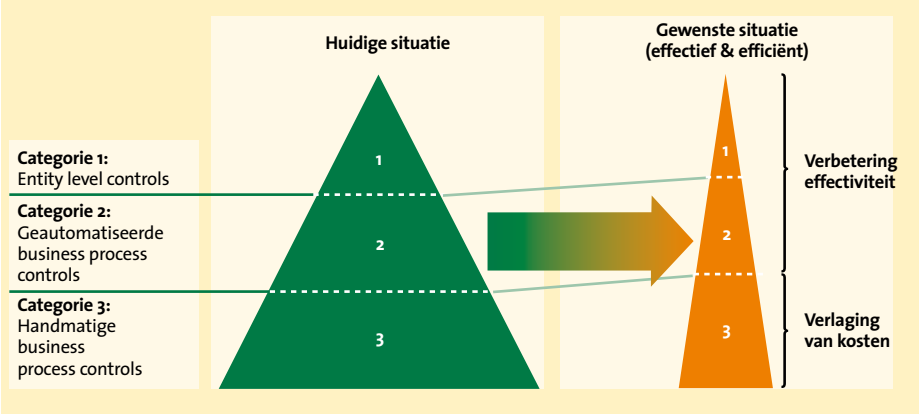
Samengevat zijn de voordelen dat het aantal controls wordt verminderd en dat er meer gebruik zal worden gemaakt van geautomatiseerde en procesoverstijgende controls. Figuur 2 illustreert deze verandering van het control framework. Het resultaat is een verbetering van de effectiviteit van de controls als gevolg van het identificeren van de key controls en een sterke verlaging van de kosten als gevolg van het reduceren van de handmatige controls.

## Embedded testing

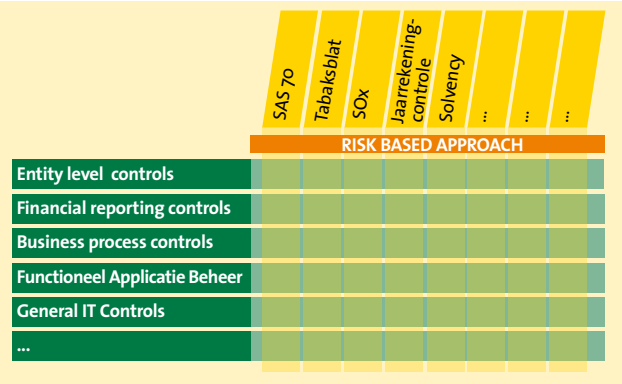
Momenteel verricht de auditor veelal de testwerkzaamheden om vast te stellen dat de beschreven controls bestaan en werken. Sommige van deze testwerkzaamheden omvatten hoogstwaarschijnlijk dezelfde procedures die al in de lijn door het management worden uitgevoerd. Wanneer deze managementwerkzaamheden goed worden uitgevoerd en gedocumenteerd, kan de auditor hier goed gebruik van maken. Door gebruik te maken van management testing kunnen bijvoorbeeld wekelijkse monitoring controls van het management worden getest in plaats van dagelijkse operationele controls. Het testen van een wekelijkse control vergt minder inspanning dan een dagelijkse control, waardoor een directe besparing wordt gerealiseerd.

Het testen door het lijnmanagement heeft meer voordelen. De controles worden uitgevoerd door mensen met vakinhoudelijke kennis. Tevens verbetert de betrokkenheid van de lijn en voorkomt men daarmee in een vroeg stadium mogelijke (dure) 'deficiencies' (tekortkomingen). 'Deficiencies' vergen veel tijd van de organisatie en de auditor, wanneer deze pas tijdens de controle worden geconstateerd.

Het kan ook nog beter, en wel door de controle door het lijnmanagement niet als een control te identificeren en te testen, maar als testwerk van de control waarop door de auditor kan worden gesteund. Als de auditor wil steunen op de werkzaamheden uitgevoerd door anderen moeten er twee vragen worden beantwoord: is de uitvoerende voldoende deskundig en is hij onafhankelijk. Deskundigheid bestaat enerzijds uit vakinhoudelijke auditkennis en anderzijds uit kennis van de regelgeving (bijvoorbeeld de noodzakelijke wijze van testen en documenteren). De onafhankelijkheid van het testwerk lijkt niet te zijn gewaarborgd wanneer dat is uitgevoerd door het directe lijnmanagement. Zij kan worden verhoogd door het introduceren van een onafhankelijke quality-assurancerol van de Interne Accountants Dienst of de afdeling Kwaliteitscontrole. Als de




Figuur 2. **Verandering van het control framework van huidige naar gewenste situatie.**




Figuur 3. **Grid ter bepaling van de overlap tussen de diverse control frameworks.**

deskundigheid en onafhankelijkheid zijn gewaarborgd, kan de auditor maximaal gebruikmaken van de uitgevoerde testwerkzaamheden.

### SAS 70 als onderdeel van een integraal framework

Een SAS 70-traject moet niet als een op zichzelf staand project worden beschouwd binnen een organisatie. Het is van groot belang dat andere control frameworks worden verenigd met het SAS 70-framework. Indien dit niet gebeurt, zullen dezelfde controls meermalen worden getoetst, omdat ze deel uitmaken van meerdere control frameworks. Door het integreren van frameworks worden de te testen beheersingsmaatregelen als het ware ontdubbeld. Andere control frameworks zijn bijvoorbeeld die voor SOx, Tabaksblat of de verzameling controls van belang voor de jaarrekeningcontrole. Het verenigen van de frameworks is zeker geen gemakkelijke opgave, doordat deze control frameworks niet een-op-een aan elkaar te relateren zijn door een verschil van reikwijdte en diepgang. Figuur 3 geeft op hoofdlijnen aan hoe de overlap tussen de diverse control frameworks inzichtelijk kan worden gemaakt en moet vervolgens nader worden uitgewerkt. Deze uitwerking is naar onze ervaring veelal een tijdsintensieve actie, maar wel noodzakelijk om ten volle de voordelen van het rationaliseren van het control framework te benutten.

## Conclusie

Er zijn goede besparingsmogelijkheden binnen het relatief dure project voor het opstellen en het realiseren van een SAS 70-rapport. Het beperken van het aantal controls, door een betere scoping van de processen en de selectie van de juiste controls binnen de processen, reduceert de kosten voor het opstellen, maar vooral de kosten voor de interne en externe toetsing. Focus op key controls, ofwel: méér controls wil niet zeggen meer 'in control'. Verder kan door de verschuiving van de inspanning van de auditor naar het management of een onafhankelijke quality-assurancerol een grote besparing worden gerealiseerd (door het vervangen van de dure externe door goedkopere interne uren), en dat geldt ook voor het ontdubbelen van dezelfde controls binnen de verschillende control frameworks. Buiten het doel van het verlagen van de kosten van het SAS 70-rapport kan deze aanpak ten slotte ook worden gebruikt als middel om de gehele beheersing van de organisatie te verbeteren.

**Méér controls wil niet zeggen meer 'in control'**

Vragen die een serviceorganisatie zich moet stellen zijn: is de scope van het rapport in lijn met de wensen van de klant? Steunt de organisatie intern wel op de juiste controls en kan dit niet beter of efficiënter door focus op key controls? Kan er niet meer gebruik worden gemaakt van preventieve geautomatiseerde controles en testwerkzaamheden van het management zelf? In deze aspecten ligt de uitdaging voor organisaties. Een duidelijke visie op scope, controls en testen van controls kan de procesinrichting verbeteren, het aantal te testen controls verminderen en tegelijkertijd de kwaliteit van het SAS 70-rapport verhogen.

## Literatuur

J.C. Boer RE RA en drs. H.P. van der Horst, *De Praktijkgids SAS 70*, KPMG Uitgave, 2007.

Drs. S.R. van Bellen RA, drs. J.P. Hoogstra RE en drs. M.A. Francken RE RA CISA, *Nut en noodzaak van SAS 70*, Compact 2007/3.

Drs. J.H.L. Groosman RE, *Verschillen en overeenkomsten tussen SOx en SAS 70*, Compact 2007/3.