# SAS 70 in een ICT-fabriek

## Accessoire, fabrieksoptie of onderdeel van de standaard?

*Drs. ing. S.R.M. van den Biggelaar RE, drs. S. Janssen RE en drs. G.J.L. Lamberiks*

**De trend is gezet. Aantoonbaar in control zijn is en wordt steeds belangrijker in het hedendaagse bedrijfsleven. Ook een ICT service provider ondervindt inmiddels welke impact de Sarbanes-Oxley Act Sectie 404 heeft. Verantwoording afleggen vond in de afgelopen jaren grotendeels plaats door middel van service level rapportages en meetings. Dit is niet langer voldoende voor jaarrekening of SOX, een accountantsverklaring over de werking van de controls is vereist, ofwel een SAS 70 type II-verklaring. Dit artikel beschrijft de belangrijkste ontwikkelingen op dit gebied bij een ICT service provider.**

### Inleiding

Veel ICT service providers hebben klanten die actief zijn in diverse marktsegmenten. Zo hebben de meeste ICT service providers klanten uit de financiële sector maar ook de industriële productieondernemingen en in de telecom- en consumentenindustrie. Meer en meer zien wij in de praktijk dat deze klanten accountantsverklaringen vragen van hun ICT service provider, waarin 'assurance' wordt gegeven dat aan de voor hen relevante wet- en regelgeving wordt voldaan. Naast bijvoorbeeld ISO, BS7799, code-Tabaksblat of de Sarbanes-Oxley Act (SOXA) is hieronder een aantal voorbeelden genoemd:

- Ondernemingen actief in de financiële sector hebben al snel te maken met toezichthouder DNB en de richtlijnen van Basel II.
- Als ondernemingen in de farmaceutische of voedingsindustrie willen opereren in Amerika zijn de richtlijnen van Food and Drug Administration (FDA) aan de orde.
- Ondernemingen actief in de telecom hebben bijvoorbeeld ook te maken met de OPTA als toezichthouder.

De consequentie hiervan is dat ICT service providers compliance moeten kunnen aantonen met al deze vormen van wet- en regelgeving. Vanzelfsprekend betekent dit dat de auditkosten van ICT service providers de afgelopen tijd sterk zijn toegenomen.

In dit artikel staat het SAS 70-onderzoek in relatie tot ICT service providers centraal. Het SAS 70-onderzoek wordt in toenemende mate toegepast om klanten van de gevraagde 'assurance' te voorzien, vooral als gevolg van de SOXA. Dit artikel is het eerste uit een serie van twee. Het tweede artikel dat in de volgende Compact verschijnt, legt het accent op de 'gebruikers' van het SAS 70-rapport, de klant van de serviceorganisatie en diens accountant.

*Drs. ing. S.R.M. van den Biggelaar RE*
is partner bij KPMG Information Risk Management en docent aan het Tilburg Institute of Advanced Studies. Hij is verantwoordelijk voor diverse SAS 70-trajecten bij zowel ICT als andere service providers. Daarnaast heeft hij veel ervaring op het gebied van ERP-systemen en HR Shared Service Centers.

vandenbiggelaar.stephen@kpmg.nl

*Drs. S. Janssen RE*
is als senior manager werkzaam bij KPMG Information Risk Management en docent aan het Tilburg Institute of Advanced Studies. Hij heeft meerdere SAS 70-onderzoeken in complexe IT-omgevingen geleid. Tevens heeft hij adviesopdrachten geleid die gericht waren op het opzetten van internal control frameworks in relatie tot Sarbanes-Oxley.

janssen.stephan@kpmg.nl

*Drs. G.J.L. Lamberiks*
is adviseur bij KPMG Information Risk Management. Hij heeft ervaring opgedaan met een breed scala van advies- en auditopdrachten. Hij is betrokken geweest bij meerdere SAS 70-onderzoeken in zeer complexe IT-omgevingen. Voorts heeft hij zich gespecialiseerd in informatiebeveiliging en IT-audit tooling.

lamberiks.gideon@kpmg.nl

Dit artikel beschrijft allereerst het krachtenveld waarin ICT service providers zich bevinden, om vervolgens in te gaan op de betekenis van de SOXA voor de ICT service providers. Het geven van zekerheid over de kwaliteit van de dienstverlening aan belanghebbenden kan worden afgegeven in de vorm van een SAS 70-rapport. In dit artikel wordt stilgestaan bij de verschillende vormen van SAS 70-rapporten, generiek en specifiek. Verder zal een onderzoeksbenadering worden beschreven waarmee een specifieke SAS 70-rapportage efficiënt kan worden opgesteld en waarbij de operatie van de ICT service provider zo minimaal mogelijk wordt verstoord met diverse audits. Tot slot zal een aantal tips worden gegeven voor zowel de gebruikers van het SAS 70-rapport als de verstrekkers ervan.

### Krachtenveld ICT service providers

Bedrijven blijven er in toenemende mate voor kiezen hun IT-operatie of delen daarvan te outsourcen naar externe serviceorganisaties. Naast verwachte financiële voordelen zijn de meer kwalitatieve redenen die daarvoor worden aangevoerd ([Vank05]):

- versterken van aandacht op kernactiviteiten;
- verhogen van commerciële slagkracht;
- vrijmaken van middelen voor investeringen.

Zo stelt bijvoorbeeld Heijmans NV in haar persbericht van 9 februari 2006 waarin de outsourcing van ICT wordt aangekondigd, dat met de outsourcing flexibeler kan worden ingesprongen op de complexe ICT-behoefte van haar innovatieve producten.

**Het waarmaken van op zich realistische verwachtingen blijkt in de praktijk een lastige klus te zijn**

Ook ABN AMRO, dat in het kader van het Group Shared Serviceprogramma in 2005 aankondigde onder andere haar IT-infrastructuur te outsourcen, noemt hiervoor argumenten als ‘duurzame versterking van concurrentiekracht en verbetering van dienstverlening door toegang tot moderne technologie’.

Met andere woorden, er leeft een verwachting bij het management dat met het outsourcen van de IT-operatie kosten worden bespaard, de kwaliteit ervan toeneemt en de gewenste flexibiliteit voor het doorvoeren van veranderingen en innovaties hierdoor wordt ondersteund. Voorts verwacht de klant de individuele aandacht die hij altijd was gewend.

Hoewel de hier uitgesproken verwachtingen naar onze mening realistisch zijn, blijkt het realiseren ervan in de praktijk een lastige klus te zijn. Zeker bij grote ‘deals’, waarbij complete rekencentra, bestaande infrastructuren, mensen en werkwijzen worden overgenomen, is het bereiken van succes geen sinecure. Naast het feit dat tijdens een outsourcingsdeal integratie actief dient te worden gemanaged en geen genoegen mag worden genomen met het resultaat dat de services gewoon zijn blijven ‘doordraaien’, is er een aantal zeer belangrijke voorwaarden waaraan moet worden voldaan wil integratie voor zowel klant als provider succesvol zijn:

- Kennis, kunde en ervaring dienen te worden gecentraliseerd, benut en verbeterd.
- Processen dienen te worden gestandaardiseerd, gestroomlijnd en gespecialiseerd.
- Er dient sprake te zijn van een ‘sustainable’, transparante en zoveel mogelijk klantonafhankelijke organisatievorm, waarin toekomstige ‘deals’ kunnen worden geabsorbeerd.
- Een standaardraamwerk van controls, instructies en verantwoordingsinformatie dient te zijn ingericht.

De auteurs hebben in de praktijk integraties gezien die binnen een jaar nagenoeg waren afgerond, maar tevens voorbeelden van integraties die na twee jaar nog in de kinderschoenen stonden voornamelijk als gevolg van het niet voldoen aan één of meer van de bovengenoemde voorwaarden.

In dit artikel zal blijken dat de genoemde randvoorwaarden ook zeer belangrijk zijn om op een zo kosteneffectief mogelijke manier een op de klant en zijn accountant afgestemd SAS 70-rapport te leveren.

### SOXA (Sarbanes-Oxley Act) en ICT service providers

Met de komst van SOXA hebben ook de ICT service providers er een uitdaging bij gekregen. Vanuit alle uithoeken komen de verzoeken binnen om aan te tonen dat de general IT controls in en rondom de voor de klant relevante infrastructuren, systemen en processen op orde zijn. Hierop kan grofweg op twee verschillende manieren antwoord worden verkregen:

- via het door de klant uitoefenen van het ‘right of audit’ (indien dit is overeengekomen);
- via een Statement on Auditing Standards nr. 70 (SAS 70) (type II)-rapport.

Vanuit het perspectief van de ICT service provider is het effectueren van het ‘right of audit’ het laatste waarop hij zit te wachten. Praktisch betekent dit namelijk het volgende:

- Vanuit SOXA dient het management van degene die klant is bij de provider, zelfstandig vast te stellen dat key controls aanwezig en effectief zijn.
- De accountant van de klant dient in het kader van de jaarrekeningcontrole en ter toetsing van de juistheid

van de managementbewering zelfstandig testwerkzaamheden uit te voeren.

De serviceorganisatie wordt tweemaal belast met auditwerkzaamheden. Nu valt dit allemaal wel mee wanneer de ICT service provider slechts één klant heeft, het wordt pas echt lastig als iedere klant dit recht gaat uitoefenen. In het gunstigste geval zou dit betekenen dat er eerst tientallen managementteams of afvaardigingen daarvan, rondom een en dezelfde persoon staan om bijvoorbeeld via waarneming ter plaatse vast te stellen dat toch wel echt via een 'securID'-token wordt aangelogd op het servicenetwerk en een paar weken later de auditors van die klanten rond diezelfde persoon staan om vast te stellen dat de bewering van het management klopt. In een minder gunstig geval komen de verzoeken verspreid binnen en vindt gedurende enkele maanden meerdere keren per week een audit plaats op een en dezelfde control. Dit is slechts één voorbeeld om aan te tonen waarom een ICT-serviceorganisatie dit niet zou willen.

Een SAS 70-rapport zou uitkomst kunnen bieden voor dit probleem. Om dit goed te kunnen begrijpen moet het concept iets verder worden toegelicht.

In het SAS 70-concept worden vier partijen onderscheiden:
- de userorganisatie, dit is de organisatie die haar diensten heeft uitbesteed en de primaire vrager van het SAS 70-rapport;
- de user-auditor, dit is de accountant van de userorganisatie;
- de serviceorganisatie, dit is de externe (IT-)dienstverlener en de verstrekker van het SAS 70-rapport;
- tot slot de service-auditor, de onafhankelijke door de PCAOB erkende auditor die een oordeel afgeeft bij het SAS 70-rapport.

SAS 70 bestond al lang voordat in 2002 de SOXA zijn intrede heeft gemaakt. Van oudsher is een SAS 70 een instrument om zekerheid te bieden aan de externe accountant van een klant die processen of delen daarvan heeft uitbesteed aan een derde partij en waarbij deze processen van invloed waren op de jaarrekening van de klant. Dit is niet veranderd.

Echter, sinds de publicatie van standaard nr. 2 van de PCAOB ([PCAO04]) heeft SAS 70 een breder bereik gekregen. In artikel B18 van PCAOB-standaard 2 is vrij vertaald opgenomen dat hoewel SAS 70 in beginsel een auditor-to-auditor rapport is, dit ook door het management mag worden gebruikt voor zijn 'assessment of internal control over financial reporting'. Wel is hiervoor een SAS 70 type II-rapport vereist waarin naast opzet en bestaan ook zekerheid over de werking van controls wordt gegeven. Hiermee wordt het SAS 70-rapport enerzijds een verlengstuk van het internal control framework dat een organisatie in het kader van haar SOX-programma opzet, anderzijds behoudt het zijn initiële doelstelling om zekerheid te geven aan de user-auditor in het kader van zijn audit op de jaarrekening van de klant.

**Van oudsher is een SAS 70 een instrument om zekerheid te bieden aan de externe accountant van een klant**

In een SAS 70-rapport worden vier secties onderscheiden (voor meer details zie [Bigg05]). Hoewel de structuur niet strikt voorgeschreven is, bevat in de praktijk Sectie 1 het oordeel van de service-auditor. Sectie 2 is een beschrijving van dienstverlening, control objectives en controls binnen de serviceorganisatie. Sectie 3 geeft de testwerkzaamheden en resultaten van de service-auditor weer. Sectie 4 is gereserveerd voor aanvullende informatie die de serviceorganisatie noodzakelijk vindt te vermelden. Over de inhoud van deze sectie wordt door de service-auditor geen zekerheid gegeven (zie voor meer details tabel 1).

Sectie 2 omhelst bij een ICT service provider vaak het onderwerp general IT controls. PCAOB-standaard 2 spreekt in dit kader over vier relevante gebieden:
- Access to Programs and Data;
- Program Changes;
- Program Development;
- Computer Operations.

In de praktijk zien de auteurs dat userorganisaties die hun IT-operatie of delen ervan hebben geoutsourcet, in het kader van hun eigen SOX-programma voor deze vier gebieden zogeheten control objectives definiëren. Deze control objectives geven in wezen per gebied specifieker aan waarover door de userorganisatie aan de serviceorganisatie zekerheid wordt gevraagd (zie voorbeelden tabel 2). De serviceorganisatie beschrijft op haar beurt

*Tabel 1. Secties per type SAS 70-rapport.*

| SAS 70 report content | Type I | Type II | Responsibility |
|---|---|---|---|
| Section 1 – Independent service auditor's report (i.e. opinion). | included | included | service auditor |
| Section 2 – Service organization's description of controls. | included | included | service organization |
| Section 3 – Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests (Type II report only) and other information that the service auditor feels may be useful to a user organization and their auditors. | *optional (normally not included)* | included | service auditor |
| Section 4 – Other information provided by the service organization (e.g. service organization plan for enhancing its systems). | *optional* | *optional* | service organization |

| PCAOB Domain | Control Objective |
|---|---|
| Program Changes | Controls provide reasonable assurance that any changes to the systems/applications providing control over financial reporting have been properly authorized by an appropriate level of management. |
| Program Development | Controls provide reasonable assurance that there is adequate testing for the development or acquisition of systems / applications used during financial reporting processes and that testing is signed off by both the users at an appropriate level of IT and business management. |
| Accces to Programs and Data | Controls provide reasonable assurance that user accounts are added, modified and deleted in a timely manner to reduce the risk of unauthorized / inappropriate access to the organization's relevant financial reporting applications or data. |
| Computer Operations | Controls provide reasonable assurance that backup and recovery procedures can recover data, transactions and programs that are necessary for financial reporting. |

*Tabel 2. Voorbeelden van control objectives per PCAOB-domein.*

welke 'controls' zij in operatie heeft om aan de control objectives te kunnen voldoen.

Aangezien elke userorganisatie vaak eigen control objectives definieert, dient de serviceorganisatie in principe telkens opnieuw controls te definiëren die zij heeft geïmplementeerd om aan de control objective te kunnen voldoen. Omwille van efficiency, zo zien de auteurs in de praktijk, definieert een ICT-serviceorganisatie op basis van bestaande processen een eigen internal control framework waaruit zij kan putten voor het beschrijven van controls. Hierover meer in het vervolg van dit artikel.

**Een klant wil in een SAS 70-rapport vaak een afbeelding zien van zijn specifieke situatie**

### Generieke of specifieke SAS 70-rapporten? ... of ...?

Zeker voor wereldwijd opererende ICT service providers, die van diverse multinationals de IT-operaties hebben overgenomen, is er sprake van een grote diversiteit aan dienstverlening. Deze diversiteit wordt bepaald door technologische en organisatorische aspecten, waarbij onder meer bepaald moet worden of er sprake is van:
- diverse platformen die worden ondersteund (mainframes, Unix, Windows, etc.);
- databasemanagementservices en zo ja, welke (Oracle, SQL-server, Informix, etc.);
- technisch applicatiebeheer rondom bijvoorbeeld SAP en Oracle;
- systeemontwikkelingsactiviteiten en zo ja, op welke ontwikkelomgevingen;
- het aantal rekencentra;
- netwerkbeheeractiviteiten.

Tevens vindt voor multinationale klanten in veel gevallen de dienstverlening verspreid over de wereld vanuit verschillende organisatorische eenheden plaats.

Gegeven deze situatie duiken twee belangwekkende, met elkaar samenhangende vragen op:
- In hoeverre is het *mogelijk* om generieke SAS 70-verklaringen af te geven?
- Welke waarde heeft een generieke SAS 70-verklaring voor de gebruikers ervan?

Strikt genomen is het mogelijk een generiek, niet-klantspecifiek, SAS 70-rapport op te stellen voor een gestandaardiseerde dienst. Wel is het dan belangrijk dat ook de controls binnen deze dienst uniform zijn. Hierbij dient echter wel afgewogen te worden welke geografische/organisatorische reikwijdte de verklaring beoogt te hebben. Wanneer deze dienst bijvoorbeeld over de wereld door verschillende organisatorische entiteiten wordt verricht waarbij deze entiteiten tevens van elkaar verschillende klanten bedienen, dan lijkt een generiek rapport over deze verschillende entiteiten op voorhand niet zinvol te zijn. In dit geval is een generiek rapport per entiteit wellicht verstandiger.

Belangrijker is echter te onderkennen dat de totale dienst die door een klant wordt afgenomen een complexe en unieke samenstelling is van een veelheid aan diensten rondom verschillende technische platformen en verspreid kan zijn over meerdere geografische locaties en organisatorische eenheden. Een klant wil in een SAS 70-rapport vaak een afbeelding zien van zijn specifieke situatie. Hiermee valt te begrijpen dat de behoefte van de klant meer is dan een optelsom van generieke per dienst opgestelde SAS 70-rapporten.

De hierboven genoemde behoefte in ogenschouw genomen en de omstandigheid dat sprake is van klantspecifieke control objectives afkomstig uit het eigen interne SOX-programma, verklaren waarom in deze situatie generieke SAS 70-rapporten meestal niet volstaan en als 'te high level' worden ervaren. Daardoor is er al snel sprake van een kostbaar maatwerktraject. Dit zijn echter niet de enige determinanten voor maatwerk. De keuze daarvoor wordt mede bepaald door:
- *De aard en organisatie van de dienst*. Zo maakt het een verschil of de dienstverlening betrekking heeft op een inherent centraal georganiseerd platform zoals een mainframe of op een meer gedistribueerde omgeving en een inherent meer verspreide beheerorganisatie van bijvoorbeeld Unix- en Windows-systemen.
- *De volwassenheid van de insourcing* (voltooiing van de integratie). Wanneer de insourcing nog niet voltooid is en infrastructuren en systemen nog niet zijn opgezet conform de standaard (security) baselines en de diensten nog niet volledig via de standaardprocessen verlopen, is maatwerk haast onvermijdelijk.

• De mate waarin er überhaupt sprake is van de *randvoorwaardelijke standaardprocessen en beheersingsmaatregelen*.

Dit zijn in wezen alledrie interne factoren die door de ICT service provider zelf te beïnvloeden zijn. Stel dat de ICT service provider zich dusdanig heeft georganiseerd dat alle systemen conform gedefinieerde baselines zijn ingericht, of tenminste afwijkingen daarvan bekend en bewust overeengekomen zijn en dat IT-beheerprocessen en controls voor alle klanten hetzelfde zijn, zou dan een generiek SAS 70-rapport voor zowel klant als diens auditor voldoende zijn? Uit gesprekken die de auteurs met userorganisaties en hun auditors hebben gevoerd, valt af te leiden dat er een duidelijke behoefte bestaat dat de service-auditor de specifieke omgeving en situatie van de userorganisatie test bij het geven van 'assurance' op een afgenomen dienst. Met andere woorden, ook al blijkt bijvoorbeeld dat het change-managementproces van een Unix-service-unit, waardoor zowel servers voor klant A als voor klant B worden beheerd, op een uniforme manier wordt uitgevoerd, dan nog blijft de behoefte bestaan dat een selectie van klantspecifieke changes wordt getest. Terwijl in die situatie volstaan zou kunnen worden met een voor die service-unit relevante selectie.

Is daarmee voor de userorganisatie een kostbare en voor de serviceorganisatie een vaak terugkerende en operatieverstorende maatwerkaudit het enige alternatief? Of is er een vorm denkbaar waarin ingegaan wordt op de specifieke behoefte van de userorganisatie zonder dat dit leidt tot exponentieel hoge kosten en waarbij de serviceorganisatie minimaal wordt gestoord met operatieverstorende audits?

### Building block approach

Vanuit het perspectief van de ICT service provider zijn er, zoals hierboven beschreven, interne en externe factoren die een 'neiging' naar maatwerkaudits bepalen. De interne factoren zijn door de service provider zelf te beïnvloeden en kunnen aan de bron zelfstandig worden opgelost. De externe factoren (klantspecifieke control objectives en testvereisten) zijn deels een gegeven waarmee op een creatieve manier moet worden omgegaan. Wat de klantspecifieke control objectives met elkaar gemeen hebben, is het feit dat ze zijn afgeleid van één gemeenschappelijk referentiepunt namelijk de general IT control-aspecten die door de PCAOB in standaard 2 worden genoemd (zie hierboven). In de praktijk zien wij dat:
1. per klant het aantal control objectives per aspect sterk verschilt;
2. de ene klant zijn control objectives met betrekking tot bijvoorbeeld 'access to programs and data' bondiger en concreter formuleert dan de ander.

Beide punten leiden ertoe dat het aantal door de ICT service provider te benoemen en door de service-auditor te testen controls per klant varieert.

Het is voor de ICT service provider van belang de grootste gemene deler van key-controls te definiëren en implementeren die de afdekking van de door zijn klanten gevraagde control objectives waarborgt. In de praktijk zien de auteurs dat CObIT ([ITGI00]) hiervoor een bruikbaar handvat biedt. Op deze manier kan per klantsituatie een mapping worden gemaakt tussen de generieke key-controls en de klantspecifieke objectives, waardoor een klantspecifieke SAS 70-rapportage efficiënt kan worden gerealiseerd.

**De ICT service provider dient de grootste gemene deler van key-controls te definiëren en implementeren**

Hiermee is één van de externe factoren opgelost. Hoe echter om te gaan met de factor van het klantspecifieke testen van controls enerzijds en het minimaal verstoren van de IT-operatie anderzijds? Hierin spelen twee zaken een belangrijke rol:
1. Er dient in een zo vroeg mogelijk stadium bekend te zijn welke klanten van de ICT service provider over welke tijdsperiode een SAS 70 type II-verklaring wensen.
2. In het plannen van het testen van de controls dient niet de klant, maar het organisatieonderdeel als primair uitgangspunt te worden genomen.

Er is al aangegeven dat een type II-verklaring naast opzet en bestaan ook zekerheid geeft over de werking van controls. De beoordeelde werkingsperiode dient daarbij in beginsel minimaal zes maanden te omvatten (paragraaf 4.36 in [AICP06]). De auteurs zien in hun praktijk een ontwikkeling dat deze minimale periode in de meeste gevallen door de userorganisatie en haar auditor wordt gevraagd en wel over het tijdvak van april tot en met september van het onderhavige kalenderjaar (in het geval er geen sprake is van een gebroken boekjaar). Met die wetenschap is het voor de ICT service provider en de service-auditor mogelijk in een vroeg stadium te bepalen welke organisatieonderdelen voor welke klanten in één testblok kunnen worden afgehandeld, waarin rekening kan worden gehouden met het klantspecifiek testen van controls (bijvoorbeeld het testen van beveiligingsparameters op specifiek door de klant gevraagde Unix-machines).

Samengevat heeft deze building block-benadering de volgende voordelen:

- De klant (en diens externe auditor) ontvangt een specifiek op zijn SOX-programma aansluitend SAS 70-rapport tegen een aanvaardbare prijs.
- De operatie van de ICT service provider wordt minimaal gestoord door een veelheid aan audits.
- De werkzaamheden zijn zowel voor de service auditor als voor de ICT service provider veel beter te plannen.

Het klantorderontkoppelpunt ligt met andere woorden tussen het veldwerk, dat generiek en zoveel mogelijk anoniem wordt uitgevoerd, en de rapportage, die op basis van dit veldwerk specifiek op de klant tot stand wordt gebracht (zie tevens figuur 1).

Overigens sluit deze benadering ook volledig aan bij de manier waarop de ICT service providers hun dienstverlening aan hun klanten wensen te organiseren. Aan de voorkant een op de klant toegespitste Customer Care-organisatie, aan de achterkant anonieme gestandaardiseerde Service Delivery-processen.

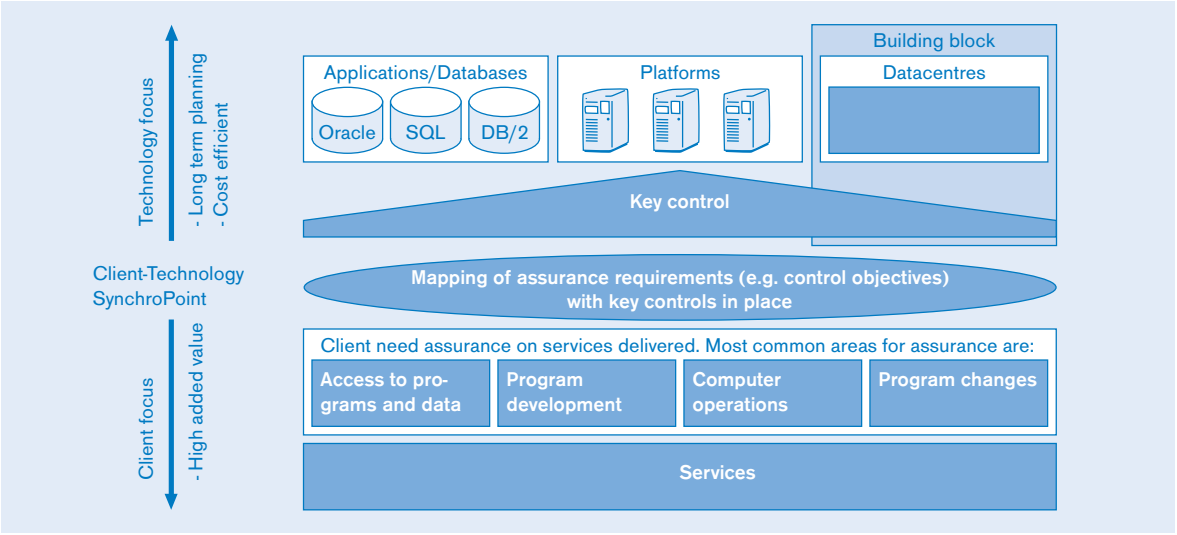
### Controls transformation, synergie onderkennen en benutten

Klanten van ICT service providers zijn op dit moment nog bereid om extra te betalen voor 'assurance'. Dit zal waarschijnlijk echter maar van tijdelijke duur zijn. Vergelijk het met alle nieuwe vaak technologische ontwikkelingen waarvoor de klant in het begin bereid is te betalen, maar die naarmate de tijd verstrijkt vanzelfsprekend worden. Meer voor minder zal ook het 'lot' van SAS 70 en meer algemeen van 'assurance' zijn. Deze wetmatigheid is slechts één van de redenen waarom ICT service providers op zoek zullen moeten gaan naar randvoorwaarden om de kosten voor het bieden van 'assurance' te verminderen. Naast de SOXA worden steeds meer compliance-achtige vereisten door de klant overgedragen aan de ICT service provider. Denk hierbij aan de ROB, Basel II, FDA, BS7799, OPTA, etc. Vreemd genoeg biedt juist deze toename van 'drivers' de mogelijkheid om tot een relatieve kostenverlaging voor 'assurance' te komen. Wanneer namelijk een analyse wordt gemaakt tussen de 'assurance'-vereisten van deze verschillende 'drivers', dan blijkt dat hierin een grote overlap bestaat. Met andere woorden, de eerder benoemde key-controls gedefinieerd en geïmplementeerd in de processen van de ICT service provider dienen verschillende doelen. Wanneer dit wordt onderkend en gestructureerd wordt vastgelegd in het samenspel van de key-controls (control framework), dan biedt deze vastlegging een belangrijk fundament om audits ten behoeve van deze verschillende 'drivers' op een efficiënte manier te plannen en uit te voeren.

Het probleem dat hierbij wel komt kijken, is dat geaccrediteerde certificerende instanties voor de verschillende audits kunnen verschillen of juist bewust verschillend door de ICT service provider zijn gekozen, waardoor de resultaten van de vastlegging in beginsel slechts beperkt kunnen worden benut. Tenzij de ICT service provider bij de uitvoering van zijn key-controls (handmatig en geautomatiseerd) een gestructureerde vastlegging van de resultaten maakt en die op een 'data-room-achtige' manier beschikbaar stelt aan de auditors. Er zijn inmiddels geautomatiseerde hulpmiddelen beschikbaar die deze werkwijze ondersteunen. Hiermee worden als het ware internal compliance statements geïntegreerd met de normale management-controlhandelingen. Internal compliance statements vormen een belangrijke input voor een externe certificering.

### Tips

Wij sluiten dit artikel af met een aantal tips voor zowel de verstrekker van het SAS 70-rapport (serviceorgani-




*Figuur 1. Building block-benadering.*

satie) als de gebruikers (userorganisatie en user-auditor) ervan.

In veel bestaande servicecontracten, die veelal een meerjarige looptijd hebben, zijn een SAS 70-rapport en de daarmee samenhangende kosten niet voorzien. Als gevolg daarvan zien wij een commerciële discussie ontstaan over wie nu moet opdraaien voor de kosten van een dergelijk rapport. Met de bestaande contractclausule rondom 'the right of audit' is hierover op voorhand geen uitsluitsel te geven, aangezien in dergelijke situaties de klant meestal opdraait voor de externe auditkosten en de ICT service provider voor de interne auditteekosten en organisatorische overhead. Voor organisaties die aan de vooravond staan een servicecontract te vernieuwen of aan te gaan, is aan te bevelen een SAS 70-rapport in de onderhandelingen mee te nemen.

Zoals al in een eerdere paragraaf beschreven wil een klant zijn specifieke situatie herkennen in een SAS 70-rapport. Deze specifieke situatie wordt bepaald door:
- IT-platformen en -omgevingen waarop diensten betrekking hebben;
- organisatorische onderdelen die de dienst verlenen;
- IT-beheerprocessen die de dienst omvatten;
- control objectives waarover 'assurance' wordt gevraagd.

Verwachtingsmanagement rondom een specifiek SAS 70-rapport begint dan ook bij het opstellen van een auditplan waarin onder meer bovengenoemde aspecten expliciet overeengekomen worden. Een vroegtijdige communicatie en afstemming tussen de vier 'partijen' in een SAS 70-onderzoek is dan ook een belangrijke succesfactor voor een herkenbaar en daardoor voor de ontvanger zinvol SAS 70-rapport.

Een hierop aansluitend onderwerp betreft een rechtvaardige scoping. De auteurs hebben in hun dagelijkse praktijk kunnen ondervinden, dat de user-auditor liever te veel 'assurance' vraagt dan te weinig. Zo zijn er meermaals discussies gevoerd of bijvoorbeeld 'interne firewalls' wel of niet in scope zouden moeten zijn van een onderzoek. Tevens blijkt dat de omvang van het aantal control objectives waarover 'assurance' wordt gevraagd niet altijd in een redelijke verhouding staat met het reële risico dat met de dienst(en) samenhangt. Ook hiervoor geldt dat een open vierpartijenoverleg de beste basis is om tot een zinvolle en rechtvaardige scoping te komen.

## Conclusie

Of een SAS 70-rapport in een ICT-fabriek een accessoire, een fabrieksoptie of een onderdeel van de standaard is, is niet eenduidig te beantwoorden. Veel wordt bepaald door de mate waarin het totale dienstenpakket aan een klant specifiek en uniek is. In situaties waarin dit niet het geval is kan een generiek statement voor de gebruikers ervan zinvol zijn en is een SAS 70-rapport als standaard ook vanuit kostenoogpunt te adviseren. In situaties waarin de inrichting van diensten en processen klantspecifiek is, is maatwerk welhaast onvermijdbaar en als accessoire te beschouwen. In overige situaties kan door gebruikmaking van een 'handige onderzoeksaanpak' het compromis worden gevonden in een fabrieksoptie, waarbij in relatieve zin de operatie van de ICT service provider zo min mogelijk wordt verstoord en een klantspecifiek SAS 70-rapport kan worden geleverd tegen aanvaardbare kosten.

## Literatuur

[AICP06] American Institute of Certified Public Accountants, *AICPA Audit and Accounting Guide: Service Organizations: Applying SAS 70, as Amended*, 2006.

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

[ITGI00] IT Governance Institute/ISACA, *CobiT, Governance, Control and Audit for Information and Related Technology, Management Guidelines*, 2000, third edition.

[PCAO04] Public Company Accounting Oversight Board, *Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*, 2004/3.

[Vank05] G. Vankan, Th. Huibers en J. Schut, *Opnieuw op zoek naar de kerncompetenties – de invloed van shared services, outsourcing en offshoring op de prestaties van uw onderneming, white paper naar aanleiding van het KPMG sourcing seminar*, 2005/11.