

SAS 70 en daarna: controls reporting in een breder kader

Stefan Verweij en Suzanne Keijl, Systems & Process Assurance

Ondernemingen besteden in toenemende mate processen uit, ook processen die in het verleden als kernproces werden beschouwd. Met de toenemende relevantie van uitbesteding wordt dienstverleners vaker gevraagd of ze een SAS 70-rapport hebben waarin zij verantwoording afleggen over hun interne beheersing. Het moet een rapport zijn dat de betrouwbaarheid weergeeft van financiële rapportage van de uitbestedende partij. Cliënten hebben echter eveneens belang bij de naleving van wet- en regelgeving en het behalen van overeengekomen serviceniveaus. Daarnaast vraagt het maatschappelijk verkeer in toenemende mate om inzicht in interne beheersing, al dan niet in samenhang met specifieke regelgeving. Dit vraagt om een verbreding van de reikwijdte van SAS 70-rapporten.

1. Achtergrond

De SAS 70-standaard is een Amerikaanse controlestandaard die zich richt op de interne beheersing bij serviceorganisaties voor de jaarrekeningcontrole van een gebruikersorganisatie. Sinds enkele jaren is een SAS 70-rapportage gemeengoed voor serviceorganisaties om verantwoording af te leggen over de interne beheersing. In Nederland is het eerste SAS 70-rapport uitgebracht in 2000. Daarna heeft dit instrument een grote vlucht genomen doordat er steeds meer bedrijfsprocessen uitbesteed werden en doordat er steeds strengere eisen gesteld werden aan de verantwoording van goed ondernemingsbestuur. Dit alles heeft geleid tot aanvullende regelgeving, zoals de uitbestedingsrichtlijnen voor verzekeraars en pensioenfondsen van De Nederlandse Bank en sectie 404 uit de Amerikaanse Sarbanes-Oxleywetgeving.

2. Het SAS 70-rapport

Volgens de principes van goed ondernemingsbestuur blijft een organisatie die haar bedrijfsprocessen (deels) uitbesteedt, onverkort verantwoordelijk voor de wijze waarop deze processen worden beheerd. Om invulling te geven aan deze verantwoordelijkheid kan een gebruikersorganisatie kiezen voor direct toezicht op de serviceorganisatie. Meestal maken gebruikersorganisaties echter gebruik van een SAS 70-rapport: de managementrapportages die afkomstig zijn van de serviceorganisatie. Om de betrouwbaarheid van deze verantwoordingsinformatie te vergroten, kan de gebruikersorganisatie een onafhankelijke partij vragen om de informatie te toetsen en de bevindingen te rapporteren in een 'Third Party Assurance'-rapport. De SAS 70-standaard geeft specifieke voorschriften voor de inhoud en de controle van dergelijke rapportages.

Samenvatting

In dit artikel wordt uitgebreid stilgestaan bij het SAS 70-rapport: de opbouw, de wijze van rapportage van maatregelen en werkzaamheden, de voordelen, maar ook de beperkingen. Verder wordt gekeken naar de mogelijkheden tot uitbreiding van de reikwijdte naar andere aspecten van interne beheersing en wordt de nieuwe internationale standaard ISAE 3402 besproken. Ten slotte wordt ingegaan op de verantwoording in de normenkaders, die nodig is voor de verbreding van de reikwijdte.

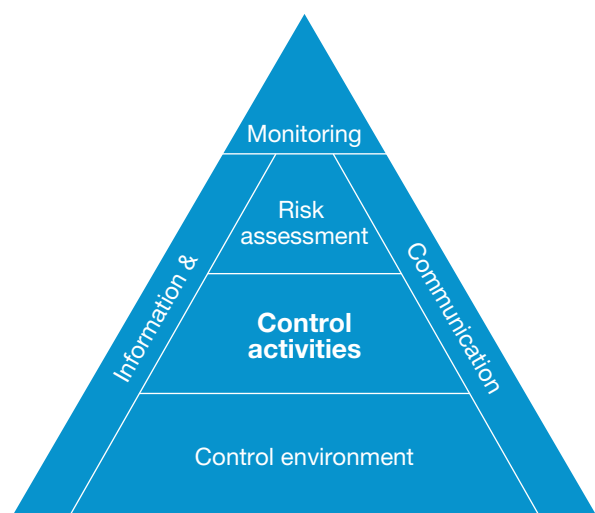
Opbouw SAS 70-rapport

Een SAS 70-rapport is opgebouwd uit een assurance-rapport van een externe accountant, een algemene beschrijving van de organisatie (dienstverlening, structuur, relaties met de omgeving), een beschrijving van de COSO-categorieën van interne beheersing op organisatieniveau (control environment, risk assessment, monitoring en information & communication) en een sectie met gedetailleerde beschrijvingen van de controlemaatregelen, gekoppeld aan internecontroledoelstellingen per proces of subproces. Zie figuur 1.

Wijze waarop maatregelen en werkzaamheden worden gerapporteerd

In een SAS 70 type 1-rapport beperkt de externe accountant zich tot de opzet en het bestaan van beheersmaatregelen. Een type 2-rapport gaat ook in op de werking van de maatregelen gedurende een bepaalde periode. Ook worden in een type 2-rapport de testwerkzaamheden van de externe accountant beschreven en de resultaten daarvan. De gebruiker van het rapport hecht doorgaans de meeste waarde aan de gedetailleerde beschrijvingen, die dan ook de

Figuur 1 - Beschrijving COSO-categorieën interne beheersing organisatieniveau



hoofdmoot vormen van het rapport. Tabel 1 geeft een voorbeeld van de wijze waarop beheersmaatregelen en testwerkzaamheden worden gerapporteerd.

Tabel 1 - Voorbeeld van wijze waarop beheersmaatregelen en testwerkzaamheden worden gerapporteerd

Proces	
Controledoelstelling De beheersmaatregelen geven een redelijke mate van zekerheid dat... enzovoort.	
Algemene toelichting Vaak is het nuttig een korte toelichting te geven op het proces zodat beheersmaatregelen in de juiste context zijn te plaatsen.	
Beheersmaatregelen	Testwerkzaamheden externe accountant
<i>Beheersmaatregel 1</i>	Voor een selectie van transacties is vastgesteld dat... etc. → Geen relevante afwijkingen waargenomen.
<i>Beheersmaatregel 2</i>	Voor een selectie van transacties is vastgesteld dat... etc. → Geen relevante afwijkingen waargenomen.
<i>Beheersmaatregel 3</i>	Voor een selectie van transacties is vastgesteld dat... etc. → Geen relevante afwijkingen waargenomen.

3. Voordelen van een SAS 70-rapport

De populariteit van SAS 70-rapportages wordt veroorzaakt door een aantal duidelijke voordelen:

- *Transparantie*
De beheersmaatregelen en de testwerkzaamheden moeten zodanig zijn beschreven dat de gebruikers (opdrachtgever van de uitbesteding en zijn externe accountant) zich zelf een oordeel kunnen vormen over de sterkte van de interne beheersing. Met andere woorden: de beschrijving moet zodanig zijn, dat ze niet alleen hoeven af te gaan op het oordeel van de SAS 70-auditor.
- *Publiceerbaar kwaliteitskeurmerk*
In tegenstelling tot andere vormen van Third Party Assurance over interne beheersing zoals Systrust en Webtrust, keurmerken voor de betrouwbaarheid van IT-dienstverlening en websites is het gehele SAS 70-rapport (dus inclusief de beschrijving van de interne beheersing) bedoeld voor publicatie aan belanghebbenden. Dit geeft de serviceorganisatie inzicht te bieden in de kwaliteit van de bedrijfsvoering, voorzien van een certificering door een externe accountant.
- *Verbetering van procesbeheersing*
Om tot een SAS 70-rapport te komen zien cliënten zich vaak genoodzaakt de interne beheersing op diverse punten aan te scherpen, wat resulteert in lagere operationele risico's. Het gedetailleerde inzicht is een uitstekend vertrekpunt tot procesverbetering. De jaarlijks terugkerende controle vraagt om discipline in de naleving van procedures. Dit zorgt ervoor dat organisaties hier sterker op kunnen steunen zodat additionele, vaak overbodige controles bij zowel de service- als de gebruikersorganisaties kunnen worden teruggebracht.

4. Beperkingen van de huidige vorm

In de introductie was al aangehaald dat SAS 70 een Amerikaanse controlestandaard is die zich richt op de interne controle van een serviceorganisatie voor zover van belang voor de jaarrekeningcontrole van een gebruikersorganisatie. Dit leidt tot een aantal inherente nadelen die door gebruikers van SAS 70-rapportages toenemend als beperkend worden ervaren.

- *Amerikaanse controlestandaard*
SAS 70 is internationaal uitgegroeid tot dé rapportagestandaard voor Third Party Assurance in afwezigheid van goede alternatieven. Dit heeft echter tot gevolg dat de accountant en de serviceorganisatie gehouden zijn aan het gehele Amerikaanse controleframework en goed op de hoogte moeten zijn van de wijzigingen in SAS 70 en in alle andere controlestandaarden die indirect van toepassing zijn. Eventuele non-compliance leidt tot een verhoogd aansprakelijkheidsrisico, zeker gezien de

Amerikaanse achtergrond van de standaard. Daarnaast wijkt de Amerikaanse regelgeving op een aantal punten af van de lokale regelgeving, wat de accountant voor een probleem stelt voor zover deze niet op elkaar aansluiten. Zo is het onder SAS 70 niet toegestaan internecontroledoelstellingen met betrekking tot continuïteit op te nemen, terwijl dit voor toezichthouders een belangrijk aspect is.

- *Risicobenadering ontbreekt*
SAS 70 gaat uit van de volledige set van internecontroledoelstellingen en beheersmaatregelen zonder afwegingen te maken ten aanzien van risico's of materialiteit van de financiële informatie. Als gevolg hiervan zijn de SAS 70-beschrijvingen zeer compleet; dit geeft veel inzicht in de processen en de interne beheersing. Toch sluit de SAS 70-standaard minder goed aan bij een moderne controlebenadering.
- *Beperkt tot betrouwbaarheid van financiële verslaggeving*
De COSO-doelstellingen 'Compliance met wet- en regelgeving' en 'Effectiviteit en efficiëntie van bedrijfsvoering' maken geen deel uit van de reikwijdte, terwijl ook deze aspecten van groot belang zijn. Het niet-voldoen aan wet- en regelgeving kan leiden tot aanzienlijke reputatieschade voor de gebruikersorganisatie wat voor met name toezichthouders in de financiële sector reden is om aanvullende eisen hieromtrent te stellen. Voor de bedrijfsvoering is het van groot belang dat de serviceorganisatie voldoet aan de overeengekomen serviceniveaus, zeker als deze relevant zijn voor de vergoeding.
- *Gericht op serviceorganisaties*
Reguliere ondernemingen (corporates) of shared service centers die willen rapporteren over hun interne beheersing aan belanghebbenden, kunnen de SAS 70-standaard wel gebruiken, maar deze is hier niet voor bedoeld. De vereiste mate van detail en transparantie kan concurrenten namelijk te veel inzicht in de bedrijfsvoering geven. Daarnaast zijn de controlekosten relatief hoog.

5. Mogelijkheden tot uitbreiding van de reikwijdte

Uitbreiding van de reikwijdte is mogelijk naar de andere COSO-aspecten van interne beheersing en andere organisaties. In figuur 2 zijn per COSO-aspect en type cliënt mogelijke onderwerpen voor rapportages weergegeven. De kleurtinten geven de mate weer van aantrekkelijkheid per propositie. De mate is ingeschat op basis van de ontwikkelingsinspanning en de marktvrage.

In andere bijdragen van deze Spotlight-uitgave wordt nader ingegaan op in-controlverklaringen, REACH en Corporate Responsibility-reporting.

Figuur 2 - Mogelijke onderwerpen voor rapportage

COSO \ Cliënten	Betrouwbaarheid van financiële rapportages	Naleving van wet- en regelgeving	Effectiviteit/ Efficiëntie
Service-organisaties	SAS 70	Continuïteit compliance	Service-level-management
Reguliere ondernemingen	In-control verklaring	Compliance (FS) REACH (CIPS) Sociaal jaarverslag	-

Serviceorganisaties

De uitbreiding van een SAS 70-rapportage richting wet- en regelgeving is al in gang gezet. Daarbij verdienen twee aspecten bijzondere aandacht.

- *Geen uitspraak over haalbaarheid controledoelstellingen continuïteit bedrijfsvoering*
De AICPA (American Institute of Certified Public Accountants) heeft naar aanleiding van de aanslagen op de Twin Towers in New York op 11 september 2001 bepaald dat de accountant in een SAS 70-rapport geen uitspraak mag doen over de haalbaarheid van de controledoelstellingen gericht op de continuïteit van de bedrijfsvoering. Dit brengt gebruikersorganisaties echter in de positie dat zij geen enkele onafhankelijk getoetste informatie ontvangen met betrekking tot 'business continuity planning', terwijl dit wel een belangrijk, zo niet cruciaal aspect is. Daarom is het te prefereren hier wel over te rapporteren, uiteraard met inachtneming van voldoende voorbehouden omtrent de voorspellende waarde van de beheersmaatregelen, mocht zich inderdaad een calamiteit voordoen.
- *Verantwoording over maatregelen voldoen wet- en regelgeving*
Iedere organisatie dient zich aan de geldende wet- en regelgeving te houden, die vooral in gereguleerde sectoren bijzonder complex kan zijn. Daarom is het van belang dat de serviceorganisatie verantwoording aflegt over maatregelen die erop gericht zijn de gebruikersorganisatie te laten voldoen aan de wet- en regelgeving, voor zover van toepassing op de uitbestede processen. Dit belang wordt veelal onderstreept door toezichthouders die vanuit hun verantwoordelijkheid eveneens inzicht wensen in de bedrijfsvoering bij een serviceorganisatie.

Daarnaast hebben gebruikersorganisaties behoefte aan informatie over het behalen van afgesproken

serviceniveaus. Dat kan onder meer gaan om zaken als beantwoording van vragen, behandeling van klachten, beschikbaarheid van een systeem of het maximaal aantal fouten, die geen directe relatie hebben met de financiële informatie. In veel uitbestedingcontracten is de beloning van de serviceorganisatie afhankelijk van de mate waarin serviceniveaus worden behaald, waardoor het belang de serviceniveaurapportages verder toeneemt. Voor zover processen direct zichtbaar zijn voor de gebruikersorganisatie kan men zich hier baseren op eigen waarnemingen, maar in veel gevallen is dit niet mogelijk. Het is dan ook van groot belang inzicht te hebben in de wijze waarop deze serviceniveaurapportages totstandkomen en de beheersmaatregelen die het management heeft getroffen ter waarborging van de betrouwbaarheid.

Reguliere ondernemingen

Ondernemingen met een notering aan de Amerikaanse beurs zijn uit hoofde van de Sarbanes-Oxleywetgeving al verplicht verantwoording af te leggen over de wijze waarop de betrouwbaarheid van financiële rapportages is gewaarborgd. Deze zogenaamde 404-rapportages dienen door de externe accountant te worden gecertificeerd. In Nederland hebben de commissies Tabaksblat en Frijs wel aanbevelingen gedaan ten aanzien van goed ondernemingsbestuur, maar zijn formele rapportages over de interne beheersing niet verplicht. Afhankelijk van het verloop van deze maatschappelijke discussie waarin de veranderende rol van de raad van commissarissen een belangrijke factor kan zijn, is het mogelijk dat ook in Nederland specifieke rapportages worden vereist.

Uitbreiding van de reikwijdte van 'Third Party Assurance'-rapportages over naleving van wet- en regelgeving naar serviceorganisaties en reguliere grote ondernemingen is een logische volgende stap in gereguleerde sectoren. Toezichhouders hebben in deze sectoren een aantal rollen. Zo verlenen zij partijen vergunningen om te opereren op markten waar zij verantwoordelijk voor zijn. Zij werken wetgeving uit in concrete regelgeving en zien toe op naleving. Toezichhouders doen in het kader van die laatste functie zelfstandig onderzoek, maar kunnen ook gebruik maken van werkzaamheden van bijvoorbeeld de externe accountant die de jaarrekening controleert. Ofschoon de externe accountant in het kader van een jaarrekeningcontrole een meldingsplicht heeft ten aanzien van het onvoldoende naleven van wet- en regelgeving, is dit niet het primaire object van zijn werkzaamheden, wat de volledigheid van zijn rapportage inherent beperkt. Tegen de achtergrond van de gelimiteerde onderzoekscapaciteit van veel toezichhouders, zou een 'Third Party Assurance'-rapport over compliance met wet- en regelgeving grote toegevoegde waarde kunnen hebben. Toezichhouders zouden hierin kunnen sturen door ondernemingen met een goed 'Third Party Assurance'-rapport te belonen met een lagere toezichthouderbijdrage, wat economisch verdedigbaar is door de gereduceerde

zelfstandige onderzoeksinspanning. Net zoals de uitbestedingstrend van invloed is geweest op de groei van SAS 70, is het voorstelbaar dat de juridisering van de samenleving de vraag naar compliancerapportages doet toenemen. In het oog springende voorbeelden zijn de financiële sector, maar ook de productiesector die onder invloed van REACH verantwoording af moet leggen over de productie en toepassing van chemische producten.

6. Nieuwe internationale controlestandaard voor serviceorganisaties

De IAASB (International Auditing and Assurance Standard Board) heeft na ISAE 3000 voor Non-financial Assurance Engagements, ISAE 3402 ontwikkeld met de titel 'Assurance Reports on Controls at a Third Party Service Organisation'. Deze standaard is ter consultatie gepubliceerd in december 2007 en zal naar verwachting eind 2008 worden geïmplementeerd. Net zoals ISAE 3000 is opgenomen in COS 3000 zal ook ISAE 3402 worden opgenomen in de Nederlandse beroepsstandaarden. Daarmee ontstaat een volwaardig alternatief voor SAS 70.

Naast het feit dat ISAE 3402 een internationale standaard is waardoor de accountant onder de reguliere lokale controlestandaarden kan werken, is de standaard op een aantal punten beter toegesneden op de huidige praktijk dan SAS 70. Zo wordt ISAE 3402 eveneens van toepassing op shared service centers, moeten risico's en materialiteit expliciet worden geadresseerd en – de belangrijkste uitbreiding – is het toegestaan controledoelstellingen op te nemen die betrekking hebben op compliance met wet- en regelgeving en effectiviteit en efficiëntie van de bedrijfsvoering. Dit stelt serviceorganisaties niet alleen in staat vollediger te zijn in hun rapportages, maar creëert ook mogelijkheden voor serviceorganisaties waarvoor SAS 70 tot op heden minder aantrekkelijk was.

Ook in de Verenigde Staten gaat de ontwikkeling verder. De AICPA heeft zich ten doel gesteld SAS 70 op korte termijn te herzien. Daarbij is het de bedoeling ISAE 3402 en SAS 70 zoveel mogelijk op elkaar te laten aansluiten zodat vooral internationaal georiënteerde cliënten slechts één serviceraapport hoeven uit te brengen om gebruikers in verschillende jurisdicties te bedienen. Het is van belang dat lokale accountantsorganisaties de hiermee samenhangende transitie goed begeleiden.

In Engeland is recent een vergelijkbare standaard van kracht geworden (AAF0106). Daar werkt de accountant volgens controlestandaard AAF0106 en wordt vermeld dat het rapport eveneens voldoet aan SAS 70. Nederland en de andere Europese landen die dienen te voldoen aan de ISA's, zouden eenzelfde benadering kunnen kiezen.

7. Verbreding reikwijdte vraagt om aanvullende normenkaders

Met het realiseren van een adequate controlestandaard zijn de beperkingen in de reikwijdte van de huidige SAS 70-rapportages slechts ten dele opgelost. Om een controle uit te voeren heeft de auditor namelijk ook een normenkader nodig. Ook indien wordt gekozen voor eenzelfde benadering als SAS 70 waarbij de gedetailleerde controledoelstellingen en beheersmaatregelen in detail zijn beschreven, is het van belang dat deze zijn gebaseerd op een algemeen aanvaard normenkader.

SAS 70 kent geen vastomlijnd normenkader, maar verwijst naar de audit 'assertions' (auditdoelstellingen) van de jaarrekeningcontrole voor de invulling van de controledoelstellingen. Dit geeft enig houvast op metaniveau; de wijze waarop een jaarrekening dient te worden gecontroleerd is immers vastgelegd in concrete controlestandaarden en over de interpretatie van die richtlijnen bestaat vrij brede consensus. Een dergelijk normenkader ontbreekt echter in veel gevallen voor nieuwe onderzoeksobjecten, wat wel een vereiste is om tot een objectief oordeel te kunnen komen. Voor een aantal sectoren zoals ICT-uitbesteding en 'business continuity planning' bestaan goede normenkaders die breed in de markt zijn geaccepteerd. Voor nieuwe objecten zoals REACH, CSR en Regulatory Compliance, zijn normenkaders (voor zover die aanwezig zijn) minder ver uitgekristalliseerd.

8. Tot slot

Vanuit de rol van externe accountant van een groot aantal service- en gebruikersorganisaties geeft PricewaterhouseCoopers mede vorm aan de inrichting van bredere 'Third Party Assurance'-rapporten en het opstellen van normenkaders. Naast cliënten wordt met toezichthouders gesproken over hun behoefte aan onafhankelijke toetsing en worden rondetafel-bijeenkomsten georganiseerd voor betrokkenen uit de sector. Samen kan ervoor gezorgd worden dat het concept van Third Party Assurance relevanter kan worden gemaakt voor ondernemers, toezichthouders en andere belanghebbenden.