De nieuwe AS5: Back to Basic

Drs. M.A. Francken RE RA CISA

Mede door de SOx 404-wetgeving en de door de PCAOB uitgebrachte Auditing Standard 2 is IT de afgelopen jaren nadrukkelijk op de agenda van het management geplaatst. Het belang van IT voor een betrouwbare verslaglegging en de noodzaak om hierover zichtbaar 'in control' te zijn, heeft tot vele hoofdbrekens geleid. Uiteraard steunen veel organisaties op IT, maar welke IT en hoe groot zijn de risico's precies. Naar de mening van de PCAOB hebben de organisaties en accountants te veel risico's geïdentificeerd, waardoor te veel beheersingsmaatregelen object van onderzoek werden. Op 24 mei van dit jaar heeft zij een nieuwe auditingstandaard uitgebracht, waarin zij een meer risicogebaseerde aanpak voorschrijft. In dit artikel wordt kort stilgestaan bij de impact die dit op de IT-aspecten kan hebben.

Inleiding

Op 24 mei van dit jaar is de nieuwe standaard (AS5) voor audits van SOx 404-plichtige ondernemingen door de PCAOB uitgebracht ([PCAO07b]). Na goedkeuring door de SEC zal de Auditing Standard 5 van kracht zijn voor de betreffende ondernemingen die een boekjaar hebben dat na 15 november 2007 eindigt. In dit artikel wordt kort stilgestaan bij de huidige ervaringen met betrekking tot IT binnen deze audits en wat de mogelijke invloed van AS5 zal zijn. Hierbij zullen niet alle mogelijke consequenties kunnen worden besproken, maar zal de auteur de (in zijn ogen) belangrijkste aspecten behandelen.

Drs. M.A. Francken RE RA CISA is als senior manager bij KPMG IT Advisory werkzaam binnen diverse SOx-trajecten, vanuit audit en advisory. Hierbij lag de nadruk op de IT-controles in relatie tot de financiële verantwoording. Daarnaast is hij actief betrokken bij IT Attestation (SAS 70) en External Audit support services binnen KPMG IT Advisory Nederland.

francken.marco@kpmg.nl

AS5 als vervanger van AS2

IT-ervaringen binnen Auditing Standard 2

In Auditing Standard 2 (AS2) ([PCAO04]) was IT nadrukkelijk opgenomen en werd het belang voor de betrouwbare informatieverstrekking benadrukt. In dit verband zijn specifiek de IT-gebieden 'program changes, program development, computer operations and access to programs and data' opgenomen. Veel organisaties hebben de relevante controles binnen deze gebieden voor IT general controls uitgewerkt en kwamen vaak tot veertig à vijftig verschillende controles per platform of omgeving ([Fran07]). Daarnaast was er ook aandacht voor applicatiecontroles, maar hiervoor was minder guidance en dit bleek in de praktijk lastiger. De algemene indruk is dat applicatiecontroles relatief weinig aandacht hebben gekregen, zoals ook bena-

drukt door de PCAOB in haar (onlangs) gepubliceerde bevindingen over de 2005-reviews ([PCAO07a]). De audits zouden veel efficiënter kunnen plaatsvinden indien meer gebruik zou worden gemaakt van de geautomatiseerde controles.

IT-voorschriften binnen Auditing Standard 5

Op 19 december jl. heeft de PCAOB een voorstel gepubliceerd om AS2 te vervangen door AS5 ([PCAO06]). De SEC heeft op dezelfde datum een 'guidance paper' voor het management gepubliceerd ([SEC06]). De conceptstandaard is op onderdelen aangepast en op 24 mei uitgebracht. Ten opzichte van AS2 heeft IT, met uitzondering van de benchmarkingaanpak van volledig geautomatiseerde controles, minder aandacht gekregen. In paragraaf 36 wordt verwezen naar de algemene uitgangspunten van AU sec. 319, 'Consideration of Internal Control in a Financial Statement Audit', welke effectief is vanaf 1990. Met andere woorden, de auditor dient IT in zijn werkzaamheden te betrekken, zoals hij dat al langere tijd diende te doen, vóórdat AS2 was uitgebracht. Dit staat uiteraard los van de vraag of IT inderdaad in voldoende mate was meegenomen bij de effectieve en efficiënte uitvoering van de controle.

De algemene indruk is dat applicatiecontroles relatief weinig aandacht hebben gekregen

Betekent dit dat IT minder nadruk zou moeten krijgen, nadat AS2 hier juist verhoogde aandacht aan had gegeven? Nee, AS5 benadrukt het belang van een top-down- en risicogebaseerde aanpak, waarbij IT zeker van belang is. Maar de mate waarin is sterk afhankelijk, meer dan voorheen, van de specifieke feitelijke omstandigheden. We zagen de afgelopen jaren dat ITGC bij veel organisaties (min of meer) dezelfde controles bevatten, waarbij een zogenaamde 'checkbox exercise' werd uitgevoerd. Hier zal nu meer een selectie van relevante ITGC plaatsvinden, gebaseerd op relevantie, risico en complexiteit. De relevantie is in dit verband afhankelijk van het belang van de betreffende applicatie(controles) in relatie tot de betreffende controledoelstellingen, gerelateerd aan de meest risicovolle beweringen in de jaarrekening.

Daarnaast hebben veel van de wijzigingen in AS5 ook een directe invloed op de IT-auditplanning en -uitvoering. Hier wordt in de volgende paragrafen kort op ingegaan.

AS5 en IT-auditplanning en -uitvoering

Verwijderen onnodige procedures

Naast de eerdergenoemde top-down- en risicogebaseerde aanpak streven de opstellers van AS5 ook naar het zoveel mogelijk verwijderen van onnodige procedures. In dit verband dient de auditor geen evaluatie van het 'management assessment'-proces uit te voeren en hierbij geen verklaring meer af te geven. Dit betekent dat de IT-auditor de uitgevoerde IT-testwerkzaamheden door het management met veel minder detail zal bekijken, indien hij geen gebruikmaakt van deze testwerkzaamheden. Het is de verwachting dat dit tot minder discussies zal leiden. Daarnaast wordt er minder vertraging in de uitvoering van de auditwerkzaamheden verwacht, omdat er niet hoeft te worden gewacht totdat het management zijn testwerk heeft uitgevoerd. Er wordt geen verklaring over afgegeven, de nadruk ligt op de werking van de relevante controles, die zouden moeten werken onafhankelijk van de uitgevoerde managementtesting. Hoeft het management dan helemaal niet meer te testen? Jawel, maar dit kan het op een andere wijze doen dan de auditor zou doen, waarbij de testing meer 'embedded' kan zijn.

Verder zijn de 'multi-location'-voorschriften aangepast en is het 'coverage'-principe verwijderd. Dit betekent dat de auditor meer vanuit de risico's beredeneerd zal selecteren welke processen en locaties in scope zijn voor de audit. Er zijn geen minimale percentages voor 'coverage', zoals de accountantskantoren intern voorschreven. Minder processen en locaties betekent ook minder IT in bereik.

Steunen op werk uit voorgaande jaren

Op aanraden van vele organisaties heeft de PCAOB aangegeven dat de auditor op voorgaande jaren kan steunen bij de uitvoering van zijn werkzaamheden. Maar ieder jaar staat nog wel op zichzelf en belangrijke controles dienen jaarlijks te worden getest. Op basis van de ervaring uit het verleden kan wel besloten worden minder te testen, bijvoorbeeld door het uitvoeren van andere testtechnieken en het selecteren van minder deelwaarnemingen. Voor geautomatiseerde controles kan men nog steeds gebruikmaken van de, in 2005, geïntroduceerde 'benchmarking'-aanpak, waarbij deze controles niet jaarlijks hoeven te worden beoordeeld, indien de ITGC effectief zijn en de betreffende controle aantoonbaar niet is gewijzigd.

Steunen op werk van anderen

Binnen AS2 werd uitgebreid ingegaan op de mogelijkheid voor de auditor om op het werk van 'anderen' te steunen. Deze anderen kunnen interne auditors zijn, maar ook andere partijen, vallend onder aansturing en

verantwoordelijkheid van het management. Hierbij is het begrip 'principal evidence' geïntroduceerd, wat in de praktijk heeft geleid tot aanzienlijke beperkingen bij het gebruikmaken van dit werk van 'anderen'. Vooral bij de ITGC zijn beperkingen aangebracht door de accountantskantoren en moest het merendeel van de controles vaak door de externe auditor worden uitgevoerd. AS5 is ook hier aangepast en men verwijst naar bestaande algemene auditingstandaarden (AU-322, [PCAO07b]) voor het gebruikmaken van andere partijen in het uitvoeren van de auditwerkzaamheden. Er is uiteindelijk geen aparte standaard gekomen voor het steunen op het werk van 'anderen'. Verder is in AS5 het begrip 'principal evidence' vervangen door 'sufficient competent evidence' om te benadrukken dat de eerdere voorschriften niet meer van toepassing zijn. Daarnaast is specifiek aangegeven dat we in dit verband mogen steunen op interne accountants, maar ook op andere medewerkers binnen de organisatie en ingehuurd personeel, zolang ze werken onder aansturing en verantwoordelijkheid van het management. Het is de verwachting dat er meer gesteund zal worden op 'anderen' bij het uitvoeren van de IT-auditwerkzaamheden.

Steunen op Company Level Controls

Mede doordat relatief veel organisatieonderdelen in de scope zaten voor de AS2-audit, zijn veel organisaties destijds gestart hun procescontroles in kaart te brengen en te testen. Hierbij werd een bottom-upaanpak toegepast in plaats van een top-downaanpak. De nadruk kwam hierbij te liggen op de procescontroles en in mindere mate op de aanwezige monitoring- en omspannende controles. Deze controles, zoals gedetailleerde marge- en cijferanalyses en verbandscontroles, kunnen voldoende bewijs leveren dat de betreffende controledoelstellingen zijn afgedekt, waardoor procescontroles minder (of niet) hoeven te worden getest. De PCAOB heeft in dit verband drie soorten Company Level Controls gedefinieerd:

- indirecte – indirecte impact op andere controles;
- controles die de effectiviteit van andere controles toetsen;
- directe – werken met dezelfde precisie als de betreffende procescontroles.

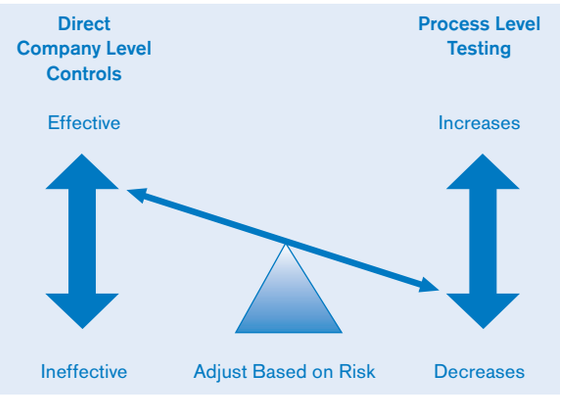
De monitoring (tweede categorie) en de directe Company Level Controls zouden tot een efficiëntere beheersing kunnen leiden en tot besparing in de auditwerkzaamheden. Figuur 1 geeft dit grafisch weer.

Dit principe is uiteraard ook van toepassing op de IT-controles, waarbij de auditors actief op zoek dienen te gaan naar de controles die impliciet andere controles testen, zoals de monitoring controles. Een review op de uitkomsten van geïmplementeerde geautomatiseerde security scripts op servers vervangt het beoordelen van de geïnstalleerde instellingen per server. En monitoring op het wijzigingsbeheerproces zou de noodzaak kunnen verkleinen om de individuele controles in het proces te testen. Uiteraard is dit soort voorbeelden afhankelijk van randvoorwaarden en feitelijke omstandigheden, maar AS5 stimuleert het creatief zoeken naar efficiency in de auditaanpak.

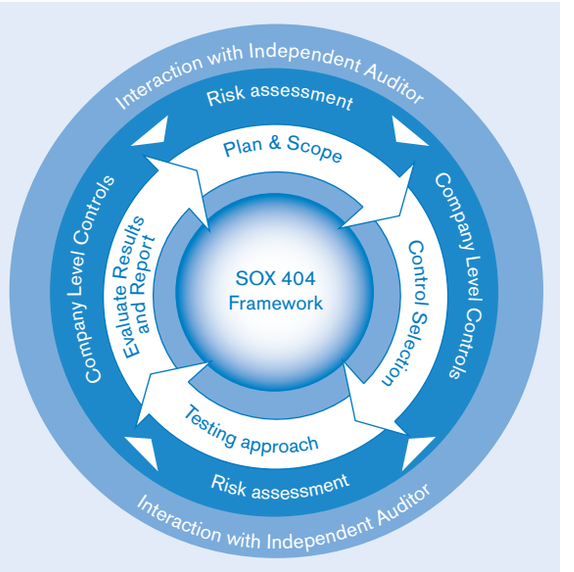
Ook onder AS5 dienen belangrijke controles jaarlijks te worden getest

Steunen op professional judgement

Als we terugkijken op bovenstaande wijzigingen, waarbij de nadruk ligt op een top-down- en risicogebaseerde benadering en waarbij we meer steunen op ervaring uit het verleden, het werk van 'anderen' en de Company Level Controls, dan steunen we feitelijk meer op professional judgement. Dit betekent uiteindelijk minder, maar effectiever en efficiënter auditwerk, waarbij de inzet van meer ervaren medewerkers in de plannings-



Figuur 1. Direct CLC versus PLC.



Figuur 2. Top-down, risk-based approach SOx 404.

fase toeneemt. In deze fase is een nauwe aansluiting tussen de scope en planning van het management en die van de externe auditor van groot belang. (Zie figuur 2 voor de SOx 404-aanpak.) Bedoelde interactie zal dan moeten leiden tot het realiseren van de kostenbesparingen, die mede ten grondslag lagen aan de gewijzigde AS5.

Conclusie

Bij het uitbrengen van AS2 is IT nadrukkelijk op de agenda gezet van het management en de auditors bij de SOx 404-plichtige ondernemingen. Dit heeft in de praktijk geleid tot een te grote nadruk op de IT general controls in relatie tot de applicatiecontroles, waardoor de compliancekosten zijn toegenomen. De PCAOB heeft benadrukt dat de efficiency in de geautomatiseerde controles dient te worden gezocht en in AS5 een meer top-down- en risicogebaseerde audit voorgesteld. Hierbij wordt in meerdere gevallen, zoals bij IT en het steunen op werk van anderen, verwezen naar bestaande standaarden. Ofwel, de auditors dienen hun werk meer op basis van professional judgement uit te voeren. Back to basic!

Literatuur

[Fran07] Drs. M.A. Francken RE RA CISA en drs. M.A.P. op het Veld RE, *SOx IT eerste praktijkervaringen en toekomstige ontwikkelingen*, Compact 2007/1.

[ITCO06] *IT Control Objectives for Sarbanes-Oxley*, second edition, ITGI, September 2006.

[PCAO04] *An Audit Of Internal Control Over Financial Reporting Performed In Conjunction With An Audit Of Financial Statements*, PCAOB Release No. 2004-001, March 9, 2004.

[PCAO06] *An Audit Of Internal Control Over Financial Reporting Performed In Conjunction With An Audit Of Financial Statements*, PCAOB Release No. 2007-001, December 19, 2006.

[PCAO07a] *Report on the second-year implementation of auditing standard no. 2, an audit of internal control over financial reporting performed in conjunction with an audit of financial statements*, PCAOB Release No. 2007-004, April 18, 2007.

[PCAO07b] *An Audit Of Internal Control Over Financial Reporting That Is Integrated With An Audit Of Financial Statements*, PCAOB Release No. 2007-005, May 24, 2007.

[SEC06] Securities and Exchange Commission, Release nos. 33-8762; 34-54976, *Management's Report on Internal Control over Financial Reporting*, December 20, 2006.