SOX ING: de aanpak van ING in het kader van de Sarbanes-Oxley Act

Drs. ing. D. Brouwer RE RA

Het is een goede zaak dat de Amerikaanse overheid paal en perk probeert te stellen aan boekhoudschandalen. Uit de opbouw en inhoud van de SOX-wetgeving blijkt duidelijk dat deze door de schandaalpraktijken is ingegeven. De pijnpunten bij deze schandalen zaten niet zozeer in IT-aspecten maar meer in de integriteit van de bestuurders en duistere boekhoudpraktijken. Toch heeft de SOX-wetgeving een grote invloed op de internal control van IT-omgevingen. In dit artikel wordt hierop ingegaan en worden tevens de ING-aanpak en de beperkingen van SOX behandeld. Tot slot worden enkele verwachte ontwikkelingen toegelicht.

Inleiding

Zelden zal een stukje wettekst van één alinea zoveel werk voor IT-beheerders en IT-auditors gegenereerd hebben als nu het geval is bij sectie 404 uit de Sarbanes-Oxley wet van 2002 (zie figuur 1).

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

Figuur 1. Tekst uit sectie 404 van de SOX-wet.

De SOX-wet heeft grote consequenties voor de aan de Amerikaanse beurs genoteerde ondernemingen omdat zij aan moeten tonen 'SOX-compliant' te zijn. Deze consequenties werken ook door op de IT-omgeving. Hierbij is in de praktijk gebleken dat een groot aantal zaken vaktechnisch gezien nog onderwerp van discussie is. De opbouw van dit artikel kent een indeling naar drie tijdperken:

- *Pre-SOX-tijdperk.* In dit deel van het artikel komen vragen aan de orde als:
  - Deden we het voor SOX niet goed?
  - Welke rol speelde IT eigenlijk in de recente beursschandalen zoals bij Worldcom en Enron?
- *SOX-tijdperk.* Hier wordt ingegaan op vragen als:

Drs. ing. D. Brouwer RE RA is zijn loopbaan bij ING begonnen bij de Interne Accountants Dienst van ING Groep. Vanaf 2000 heeft hij meerdere functies vervuld bij het centrale automatiserings-onderdeel, onder meer als hoofd van de afdeling Expertise Centrum Security en als Information Security Manager. Sinds 1 maart 2005 werkt hij voor het SOX-programma op ING Groep-niveau ter ondersteuning van de SOX-projecten van de bedrijfsonderdelen van ING.

dirk.brouwer@mail.ing.nl

Dit artikel is geschreven op persoonlijke titel. De auteur dankt de heer Jan van Thienen, programmamanager SOX ING Groep, voor zijn commentaar op de concept-versie van dit artikel.

– Wat zijn de consequenties voor de huidige internal control en IT-audit?
– Welke aanpak heeft ING gevolgd voor de implementatie van SOX?
– Wat zijn de beperkingen van SOX?
– Welke discussiepunten spelen momenteel?

• *Post-SOX-tijdperk.* In het slot van het artikel worden de volgende vragen behandeld:
– Wat is nu de blijvende waarde van SOX?
– Blijven we nu verder verschoond van beursschandalen?

Pre-SOX-tijdperk

Veelal werd de werking van de internal control van de IT bij financiële instellingen getoetst door een eigen internecontroleafdeling. Door deze werkzaamheden functioneel aan te sturen en ook periodiek te beoordelen kon de Interne Accountants Dienst en in het verlengde daarvan ook de externe accountant daar mede op steunen en zichzelf grotendeels beperken tot het periodiek beoordelen van opzet/bestaan. Daarbij werd door de Interne Accountants Dienst volgens een algemeen aanvaarde controleaanpak gecontroleerd in een driejaarlijkse cyclus waardoor ieder relevant IT-aspect minimaal één keer in de drie jaar het object van onderzoek was. Dat wilde niet zeggen dat alles in principe maar één keer per drie jaar aan bod kwam. Er werd een risk-based approach gevolgd waarbij het relatieve risico bepalend was voor de frequentie. Risicovolle objecten werden derhalve frequenter gecontroleerd.
Daarnaast werd tussentijds de voortgang van de acties op grond van eerder gerapporteerde auditbevindingen gevolgd. Vaak werd ook een interne verklaring afgegeven over de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. De externe accountant steunde voor een belangrijk deel op het werk van de interne accountant en verrichtte zelf ook controle op opzet en bestaan.
Inmiddels is bij meerdere financiële ondernemingen uit efficiencyoogpunt een beweging ingezet en vaak grotendeels al afgerond om de taken van afzonderlijke internecontroleafdelingen samen te voegen met de taken van afdelingen zoals Operational Risk Management en/of de Interne Accountants Dienst.

Rol van IT(-audit) in de beursschandalen

Een belangrijke vraag is of de hierboven algemeen toegepaste aanpak in de praktijk niet juist is gebleken. Of meer concreet: heeft dit bijgedragen aan het kunnen ontstaan van de financiële schandalen bij Enron, Ahold en recentelijk AIG?
Naar mening van de auteur moeten beide vragen ontkennend worden beantwoord. Er was niets mis met de in Nederland algemeen aanvaarde IT-auditaanpak. Boekhoudschandalen zijn helaas van alle tijden. Eén van de eerste boekhoudschandalen betrof de VOC (Verenigde Oostindische Compagnie). Je kunt zelfs zeggen dat Nederland hier een primeur had omdat de VOC als eerste multinationale onderneming wordt gezien. Dat IT geen rol gespeeld heeft bij dit schandaal hoeft verder geen betoog. Maar ook bij de andere genoemde schandalen zoals Ahold (malversaties met het boeken van nog te ontvangen inkoopkortingen en met het ten onrechte consolideren van deelnemingen), Enron (verhullen van schulden en verliezen door deze te parkeren op niet in de jaarrekening opgenomen BV's) en AIG (verhullen van schulden en risico's op een gelijksoortige wijze als door Enron) heeft IT niet een direct aanwijsbare rol gespeeld. Waarom de SOX-wetgeving dan toch doorwerkt op IT-aspecten wordt hieronder toegelicht.

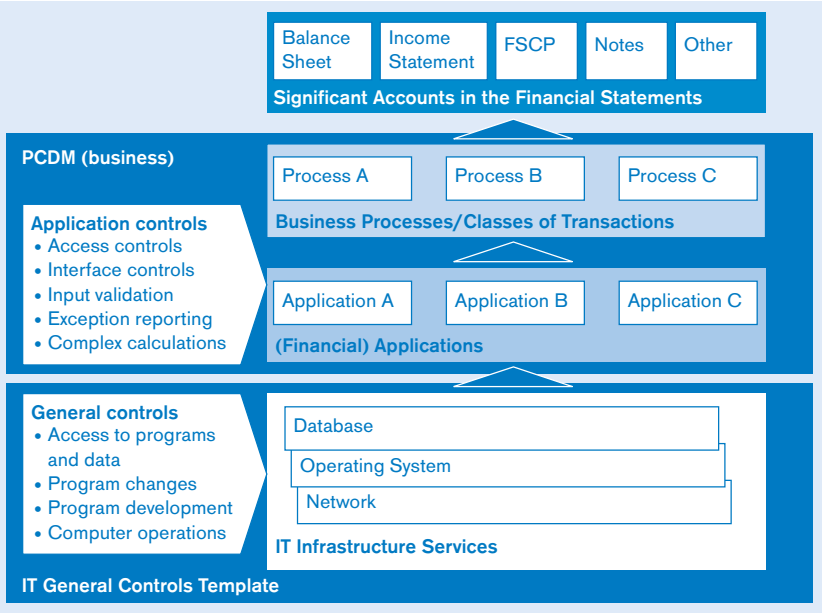
SOX-tijdperk

Consequenties voor internal control en IT-audit

De SOX-wetgeving brengt voor de internal control rond IT en IT-audit veel werk met zich mee. Niet omdat IT een prominente plaats heeft in SOX. Integendeel, wie in de SOX-wet gaat zoeken naar begrippen als application control, automated control of general control zal niets vinden.
Wel omdat IT prominent in beeld is gekomen door de PCAOB. De Public Company Accounting Oversight Board is in het leven geroepen in Titel I van de SOX-wet en heeft als doelstelling: 'to oversee the auditors of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports'. De PCAOB heeft inmiddels drie auditingstandaarden gepubliceerd. Auditing Standard 2 gaat over 'An audit over internal control' en onderkent dat IT (onder meer application controls en IT general controls) een belangrijke component van de interne controle is. Voor IT-auditors zal dit geen nieuwe constatering zijn omdat dit ook duidelijk is af te leiden uit het bekende schema waarin de samenhang tussen de application controls, general controls, businessprocessen en (financiële) gegevens is weergegeven (zie figuur 2).

Er was niets mis met de in Nederland algemeen aanvaarde IT-auditaanpak

Volgens SOX 302 moet de ondernemingsleiding periodiek rapporteren over de effectiviteit van de Design Effectiveness (grofweg aan te duiden als opzet en bestaan) en Operating Effectiveness (werking) van de internal control. De externe accountant heeft hierover een attest en rapportagefunctie volgens SOX 404. Daar-



Figuur 2. Samenhang tussen general controls, application controls, businessprocessen en (financiële) gegevens.

bij is in PCAOB Auditing Standard 2 voorgeschreven dat iedere jaarlijkse controle op zichzelf moet staan (PCAOB Auditing Standard 2, sectie E120 en verder). Ieder jaar moeten dus de controles worden getest, ook als er in dat jaar geen wijzigingen in de controles zijn doorgevoerd. Voorts is de documentatie zeer belangrijk. Inadequate documentatie over de Design Effectiveness en/of de Operating Effectiveness van de internal control wordt namelijk aangemerkt als een deficiency (PCAOB Auditing Standard 2, sectie 138).
De SOX-wetgeving brengt dus voor de meeste ondernemingen en ook voor de externe accountant meer werk met zich mee omdat de tests jaarlijks moeten worden uitgevoerd, dieper c.q. breder gaan dan voorheen en zowel de internalcontrolmaatregelen als de daarop uitgevoerde tests zeer nauwgezet moeten worden gedocumenteerd.
Het organiseren en de kwalitatieve uitvoering van de tests zijn in eerste instantie een verantwoordelijkheid van het betreffende management. De Interne Accountants Dienst wordt bij meerdere ondernemingen ingezet om de tests geheel of gedeeltelijk uit te voeren.

De ING SOX-aanpak

Recentelijk is gepubliceerd over de SOX 404-aanpak die de vier grote accountantskantoren voor hun cliëntèle hebben afgeleid van de PCAOB-richtlijn ([Herw05]). De aanpak van ING om de SOX-compliancy aan te tonen is totstandgekomen in afstemming met onder meer Ernst & Young en KPMG. Het zal geen verbazing wekken dat de ING-aanpak grote overeenkomsten vertoont met de door Herwaarden en Buurman gepubliceerde stappen van een SOX-project. Het is dan ook een in de praktijk bewezen aanpak. De ING-aanpak is schematisch weergegeven in figuur 3. De weergegeven stappen worden hieronder kort toegelicht.

Stap 1, 2 en 3
Op groepsniveau (stap 1) wordt vastgesteld wat de significante accounts (stap 2) en bedrijfsonderdelen (stap 3) zijn. Hierbij wordt een Tolerable Error gehanteerd voor de bijdrage aan de winst-en-verliesrekening en de balans op groepsniveau. Accounts met een bijdrage kleiner dan de Tolerable Error worden als niet-significant beschouwd tenzij er een verhoogd inherent risico is.

Stap 4
Per significant bedrijfsonderdeel worden de hoofdlijnen van de internecontrolecomponenten getest op Design en vindt tevens een assessment plaats op de Effectiveness. Deze tests vinden plaats aan de hand van een questionnaire die is geënt op het COSO-framework.

Stap 5
Voor de significante accounts en bedrijfsonderdelen wordt vastgesteld tot welke accountingprocessen die zijn te herleiden.

Stap 6 en 7
Per accountingproces wordt vastgesteld waar de belangrijkste risico's worden gelopen (stap 6) en met welke key controls deze risico's zijn afgedekt (stap 7). Key controls zijn beheersingsmaatregelen die noodzakelijk en voldoende zijn om het risico te ondervangen.

Stap 8
De key controls kunnen worden onderscheiden in handmatige en geautomatiseerde controles (stap 8.1). Van de geautomatiseerde key controls wordt vastgesteld in welke applicaties (software) deze zijn geïmplementeerd en op welke IT-infrastructuur (hardware) deze applicaties draaien. Dit wordt vastgelegd in een zogenaamde identificatiematrix (stap 8.2). Voor de betreffende hard- en softwareplatforms wordt een evaluatie gedaan van de general IT controls die voor die platforms van toepassing zijn (stap 8.3).
Ook de handmatige key controls worden geëvalueerd. De uitkomsten van de evaluatie van de handmatige en de geautomatiseerde key controls worden per bedrijfsproces vastgelegd in een Process Control Documentation Matrix (stap 8).

Stap 9 en 10
De uitkomsten van stap 8 zijn samen met de uitkomsten van stap 4 bepalend voor de totale evaluatie van de eventuele SOX-defecten en derhalve voor het SOX-compliant (stap 9) zijn. De rapportage over de geëvalueerde uitkomsten wordt afgetekend door de CFO en CEO (stap 10).

Stap 11
Ter ondersteuning van de door ING gekozen aanpak is

door ING zelf een applicatie ontwikkeld. Deze applicatie heeft de naam ICE-tool (Internal Control Evaluation) en wordt gestart vanaf een webbrowser. De bedrijfsonderdelen zijn zelf verantwoordelijk voor het ontwerpen, documenteren en testen van de internal control en het vastleggen van de uitkomsten daarvan in het ICE-tool. Op groepsniveau kan hierdoor de voortgang worden bewaakt en zo nodig worden bijgestuurd.

Beperkingen van SOX

De SOX-wet is er gekomen als een reactie op een aantal beursschandalen. Belangrijkste oorzaken waren niet-integere (of op zijn minst niet-capabele) managers en accountants die de daaruit voortvloeiende malversaties niet aan de orde stelden. De reacties op deze elementen zijn duidelijk terug te vinden in de SOX-wet:

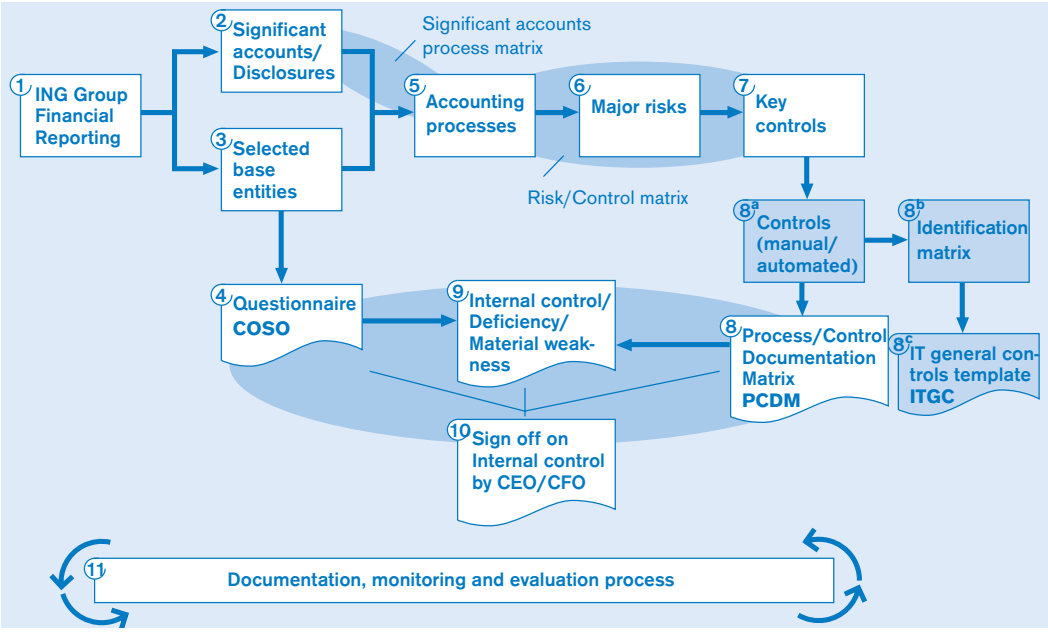
a. Als reactie op zelfverrijking door de bestuurders:
- De SOX-wet benadrukt de verantwoordelijkheid van de bestuurders voor de financiële verslaggeving, het stelsel van interne controle en het voorkómen van fraude door voor te schrijven dat daarover een verklaring moet worden afgelegd (zie titel III van de SOX-wet, met name sectie 302).
- De SOX-wet bevat bepalingen omtrent bonussen en leningen aan en aandelentransacties door bestuurders (zie titel IV).
- Op grond van de SOX-wet is het mogelijk een verbod op te leggen tot het verder uitoefenen van bestuursfuncties (zie sectie 1105).
- De SOX-wet bevat strafrechtelijke bepalingen voor zowel bestuurders als medewerkers met een maximumstraf van twintig jaar hechtenis en/of 5 miljoen dollar boete (zie titel VIII en IX).

b. Als reactie op een falend toezicht door de accountants:
- Door middel van de SOX-wet is de PCAOB (Public Company Accounting Oversight Board) ingesteld als toezichthoudend orgaan (zie titel I).
- De SOX-wet stelt eisen aan de onafhankelijkheid van en kwaliteitszorg door de externe accountant (zie titel II).
- Sectie 404 van de SOX-wet legt de verantwoordelijkheid vast van de externe accountant voor de attestfunctie op de door bestuurders afgegeven SOX-verklaring.
- Sectie 802 bevat strafrechtelijke bepalingen voor accountants met een maximumstraf van tien jaar hechtenis en/of een geldboete.

Uit een aantal elementen van de wet blijkt duidelijk dat de SOX-wet een reactie is op beursschandalen

c. Als reactie op fraude in het algemeen:
- SOX biedt bescherming van klokkenluiders (zie sectie 806) en informanten (zie sectie 1107).

Dit korte overzicht bevat enkele belangrijke bepalingen die in de SOX-wetgeving zijn opgenomen om herhaling van de eerder opgetreden schandalen te voorkomen. Toch is de scope van SOX beperkt in die zin dat deze is gericht op financial reporting, interne fraude en inte-



Figuur 3. De ING-aanpak.

griteit. Voor IT-auditors is het van belang dit te onderkennen. In het kader van SOX hoeft dus niet te worden gekeken naar processen die geen relatie hebben met financial reporting. Buiten de scope van SOX valt ook externe fraude (door bijvoorbeeld klanten of leveranciers). Binnen de scope valt alleen de interne fraude en dan nog alleen maar fraude die is gepleegd door management of door personen die een belangrijke rol hebben in het internecontrolesysteem. Tot slot wordt van de kwaliteitsaspecten CIA alleen het Integrity-aspect door de scope omvat en vallen bijgevolg de aspecten Confidentiality en Availability buiten de scope.

Discussiepunten

Als start eerst een waarschuwing. Door alle nadruk op SOX bestaat het gevaar dat er alleen nog maar gekeken wordt naar controlemaatregelen die van belang zijn om SOX-compliancy te kunnen aantonen. Door de hierboven genoemde scopebeperkingen van SOX is er evenwel een groot aantal beveiligingsmaatregelen (zoals disaster recovery en vertrouwelijkheidsmaatregelen) die weliswaar niet SOX-relevant zijn maar wel degelijk zeer belangrijk zijn voor de organisatie. Ook deze maatregelen dienen periodiek op effectiviteit te worden getest.

In Nederland werd voorheen over het algemeen principle-based gecontroleerd. Met de komst van SOX is een rule-based beweging ingezet. Met de huidige rules is de precieze scope van SOX nog niet uitgekristalliseerd. In de praktijk loop je tegen vragen aan als:

- Availability valt buiten SOX-scope, maar hoe zit het ten aanzien van back-up en recovery?

De algemene opinie is dat back-up en recovery van de financial reporting data en processen wel moet worden meegenomen.

- In hoeverre is het datacommunicatienetwerk in scope?

Is een firewall of een Intrusion Detection System voorgeschreven in het kader van SOX? Of is het voldoende als de financiële data adequaat zijn afgeschermd? Naar de mening van de auteur geldt het laatste.

- Is de controle op de identiteit van nieuwe klanten een SOX-relevante maatregel?

Vooralsnog lijkt het van niet, want stel dat hierbij fraude door de klant in het spel zou zijn, dan is dat geen fraude die onder SOX valt.

- Is de elfproef op bankrekeningnummers en de naam/nummer-controle een SOX-relevante maatregel?

Figuur 4. De definitie van de IT general controls volgens PCAOB Auditing Standard 2.

> 50. Some controls (such as company-level controls, described in paragraph 53) might have a pervasive effect on the achievement of many overall objectives of the control criteria. For example, information technology general controls over program development, program changes, computer operations, and access to programs and data help ensure that specific controls over the processing of transactions are operating effectively. In contrast, other controls are designed to achieve specific objectives of the control criteria. For example, management generally establishes specific controls, such as accounting for all shipping documents, to ensure that all valid sales are recorded.

Beide maatregelen zijn zeker belangrijke internalcontrolmaatregelen, maar zijn naar mening van de auteur niet per se vereist in het kader van SOX.

- Moet de betrouwbaarheid van een voor een key control gebruikte automatische verschillenlijst expliciet jaarlijks worden vastgesteld?

Dit is een lastig punt dat vooralsnog van geval tot geval bekeken wordt.

- Wat moet in het kader van SOX precies worden getest ten aanzien van de IT general controls?

Het eerste waar hierbij tegen aangelopen wordt, is dat er in de vakliteratuur geen consensus is over het begrip general controls. Dat begint al bij de naam. Begrippen als general controls, IT general controls, general IT controls, computer controls worden door elkaar gebruikt. De PCAOB had hier een standaard kunnen zetten, maar opvallend is dat de definitie van general IT controls volgens PCAOB Auditing Standard 2 (zie figuur 4) afwijkt van de definitie in het COSO-rapport. Hoewel Auditing Standard 2 aangeeft te zijn gebaseerd op COSO, wordt deze afwijking verder niet toegelicht of gemotiveerd. ING hanteert de definitie van de PCAOB.

- Hoe verhouden de begrippen opzet, bestaan en werking zich versus Design Effectiveness en Operating Effectiveness?

Over het algemeen wordt gehanteerd dat opzet en bestaan onder Design Effectiveness vallen en werking onder Operating Effectiveness, maar in de praktijk is er over deze tweedeling vaak discussie. Uit oogpunt van pragmatisme pleit de auteur ervoor de Nederlandse begrippen opzet, bestaan en werking te laten schieten en uitsluitend de termen Design Effectiveness en Operating Effectiveness te hanteren. Over deze twee moet namelijk een SOX-verklaring worden afgegeven.

- Welke steekproefgroottes moeten worden gehanteerd bij de tests op Operating Effectiveness?
- Moet een accountant specifiek gaan controleren op het bestaan van fraude?

Over het antwoord op de meeste vragen bestaat wel consensus tussen de binnen ING betrokken partijen, maar het is de indruk van de auteur dat accountants zich als gevolg van de met SOX ingezette ontwikkeling pas 'senang' voelen als een interpretatie ook echt formeel vastgelegd is door de PCAOB.

Post-SOX-tijdperk

Het post-SOX-tijdperk zal niet snel bereikt worden. Het is namelijk niet de verwachting van de auteur dat de SOX-wet binnen afzienbare tijd zal worden afgeschaft. Misschien kunnen we post-SOX beter lezen als: na de invoering van SOX volgend jaar (de verplichting tot SOX-compliancy voor buitenlandse ondernemingen die aan een Amerikaanse beurs zijn genoteerd, is in maart 2005 voor een jaar uitgesteld).

De auteur verwacht voor de nabije toekomst de volgende ontwikkelingen:

- De invloed van Amerikaanse auditbegrippen en -technieken zal toenemen.
- Er is een rule-based beweging ingezet en de regelgeving door de PCAOB zal in eerste instantie alleen nog maar verder toenemen omdat er nu nog veel discussiepunten bestaan over zaken die niet (precies) zijn vastgelegd.
- De jaarlijkse inspanningen die nodig zijn voor het uitvoeren van de controles en de vastlegging van de uitkomsten zullen aanzienlijk toenemen ten opzichte van het pre-SOX-tijdperk.
- Hierdoor zullen de externe accountants en de ondernemingen richting de PCAOB een lobby starten om te proberen of de extra werklast niet kan worden verminderd door de regels te versoepelen.
- Er blijft met name focus op de key controls die relevant zijn in het kader van SOX.
- Ondanks SOX zullen er nieuwe beursschandalen volgen. Wellicht zal het aantal minder zijn omdat men terugschrikt voor de strafrechtelijke consequenties. Toch zal een aantal figuren de verleiding niet kunnen weerstaan. En tegen frauduleus handelen door een bestuurder is weinig opgewassen, zeker niet als er samenspanning tussen meerdere bestuurders in het spel is.

Conclusie

IT was niet de oorzaak van de beursschandalen de afgelopen jaren, maar IT en IT-audit worden wel geraakt door de SOX-wetgeving als gevolg van de bepalingen in Auditing Standard 2 van de PCAOB. Hierdoor zal de invloed van de Amerikaanse controlebegrippen en methoden in het IT-auditwerkveld verder toenemen. Een eerste consequentie is al dat de kritische IT-componenten nu frequenter (namelijk jaarlijks) en dieper c.q. breder (namelijk ook op gebied van operationele effectiviteit) gecontroleerd moeten worden. Door de rule-based aanpak zijn er momenteel onduidelijkheden over zaken (zoals scope, testomvang) die nog niet expliciet zijn beschreven. Terwijl IT in het begin van SOX nauwelijks aan bod kwam, moet men er nu voor uitkijken dat de regelgeving door de PCAOB ten aanzien van IT-componenten en de interpretatie daarvan niet naar de andere kant doorslaat.

Gewaarschuwd moet ook worden voor het gevaar dat organisaties alleen nog maar aandacht hebben voor beveiligingsmaatregelen die SOX-relevant zijn omdat deze maatregelen al een groot capaciteitsbeslag leggen op de beschikbare resources, en er alleen (SOX-) regeltjes worden nageleefd zonder er verder over na te denken. Als deze waarschuwing ter harte wordt genomen, zal SOX zonder meer een positieve invloed hebben op de internecontrolecomponenten, maar er moet niet de illusie bestaan dat beursschandalen hiermee voorgoed tot het verleden behoren.

Naschrift

Inmiddels is de beweging op gang gekomen die de auteur had voorzien en zijn signalen afgegeven aan de PCAOB over de grote werklast en de hoge kosten die verbonden zijn aan SOX. De PCAOB is hier niet ongevoelig voor gebleken en heeft per 16 mei 2005 nadere guidance afgegeven om het proces effectiever en minder kostbaar te maken. Om twee specifieke voorbeelden te noemen:
- Het voorschrift dat iedere jaarlijkse controle op zichzelf moet staan (PCAOB Auditing Standard 2, sectie E120 en verder) is nader genuanceerd voor geautomatiseerde controles. Deze controles hoeven niet jaarlijks opnieuw te worden getest, mits de IT general controls op orde zijn en de applicatie niet is veranderd (PCAOB Question and Answer 45).
- Aan het ontbreken van voldoende documentatie over de Operating Effectiveness van een controlemaatregel (PCAOB Auditing Standard 2, sectie 138) wordt niet per definitie de conclusie verbonden dat de controlemaatregel niet effectief is. Het gaat erom of de auditor voldoende andere aanknopingspunten heeft dat de controlemaatregel daadwerkelijk effectief was (PCAOB Question and Answer 53).

Ondanks SOX zullen er nieuwe beursschandalen volgen

Literatuur

[Herw05] Herwaarden en Buurman, *Het Sarbanes Oxley 404 rapport,* tijdschrift MCA, april 2005.

COSO, *Enterprise Risk Management – Integrated Framework,* September 2004.
COSO, *Internal Control – Integrated Framework,* May 1994.
ITGI (IT Governance Institute), *IT Control Objectives for Sarbanes Oxley,* 2004.
PCAOB, *Auditing standard 1, References in Auditors' Reports to the Standards of the Public Company Accounting Oversight Board,* 14-5-2004.
PCAOB, *Auditing standard 2, An Audit of Financial Control Over Financial Reporting Conducted in Conjunction With an Audit of Financial Statements,* 17-6-2004.
PCAOB, *Auditing standard 3, Audit Documentation,* 25-8-2004.
Protivity, *Guide to the Sarbanes Oxley Act: IT Risks and controls,* December 2003.
Sarbanes Oxley Act of 2002, 23-1-2002.
Sarbanes Oxley: Implications for Information Security, Information Security Forum, February 2005.