SOX: 'Keep your eyes on the ball'

Drs. M.A. Francken RE RA CISA

Mede ingegeven door de US Sarbanes-Oxley Act van 2002 en vergelijkbare regelgeving over de gehele wereld, zien we een verhoogde aandacht voor IT governance. Beursbedrijven worden geconfronteerd met strenger toezicht en de ondernemingsleiding moet aantoonbaar maken dat ze de bedrijfsprocessen beheerst. De C-level-betrokkenheid is een duidelijk doelwit geworden van toezichthouders! In dit speelveld is het belangrijk om de kostbare tijd en energie aan de juiste zaken te besteden, wat in de praktijk niet altijd meevalt.

Inleiding

Zowel bij de White en Red Sox, en eigenlijk bij alle baseballspelers, draait alles om 'the ball'. 'Keep your eyes on the ball' is dan ook een veelgehoorde kreet tijdens het spel. Ook binnen de Sarbanes-Oxley (SOX-)wetgeving en implementatie draait alles om focus. SOX is een Amerikaanse wetgeving, van toepassing voor SEC-geregistreerde ondernemingen, voor zowel 'domestic' (2004) als 'foreign filers' (2006). In sectie 404 (hierna SOX) moet het management verklaren een goed werkende interne beheersing inzake de financiële verantwoording te hebben. De externe accountant zal het aanwezige bewijs hiervoor controleren en een separate verklaring afgeven. De alignment van de business met IT is mede hierdoor aan de orde van de dag. Hierbij moeten keuzen worden gemaakt welke IT controls (beheersingsmaatregelen) significant zijn en hoe met tekortkomingen wordt omgegaan.

Dit artikel begint met een korte toelichting op IT governance en de recente ontwikkelingen, waarna het speelveld wordt beschreven en beperkt tot de algemene IT controls. Hierbij wordt de relatie tussen de financiële verantwoording en IT uitgewerkt. In de praktijk is deze relatie niet altijd even helder.

IT governance

De verhoogde aandacht voor IT governance blijkt onder andere uit een recent onderzoek, uitgevoerd in opdracht van het IT Governance Institute ([ITGI04a]). Dit onderzoek wees uit dat 93% van het business management IT als belangrijke driver zag voor de strategie. Dit hoge percentage is onder andere het gevolg van de gewijzigde regelgeving en het strengere toezicht. Opvallend is dat meer dan tweederde van de CEO/general managers

Drs. M.A. Francken RE RA CISA is als senior manager werkzaam binnen diverse SOX-trajecten, vanuit audit en advisory. Hierbij ligt de nadruk op de algemene IT-controls in relatie tot de financiële verantwoording.

francken.marco@kpmg.nl

zich niet comfortabel of in de positie voelde om onderzoeksvragen betreffende IT governance te beantwoorden ([John05]).

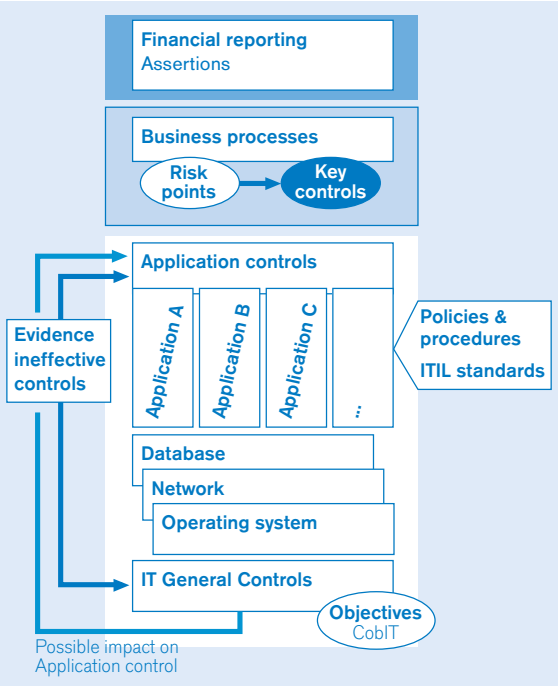
Maar wat is IT governance nu eigenlijk? NOREA ([NORE04]) hanteert hiervoor de definitie van het IT Governance Institute: 'IT-Governance is the responsibility of the board of directors and executive management. It's an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.' Hierbij geeft zij aan dat IT governance vooral van toepassing is waar '... op basis van bedrijfs- en internecontroledoelstellingen (setting objectives) de business in overleg met de IT-organisatie bepaalt welke IT-producten en -diensten door de IT-organisatie moeten worden geleverd en welke randvoorwaarden daarbij worden gehanteerd (strategic alignment ...' Hierbij worden de volgende drie aandachtsgebieden onderscheiden:

- de beheersing van de informatievoorziening binnen een organisatie;
- het afleggen van verantwoording over de beheersing van IT naar buiten toe;
- het uitoefenen van toezicht op de IT-beheersing (RvC, extern).

Bovengenoemde aandachtsgebieden komen terug in SOX. Volgens SOX zal het management expliciet *naar buiten* moeten verklaren dat haar *interne beheersing*, in relatie tot de financiële verantwoording, effectief is. De toezichthouders, waaronder het audit committee en de PCAOB[1], zullen hier *op toezien*.

2) Dit model zal in dit artikel niet verder worden uitgewerkt, maar wordt als bekend verondersteld.

1) Public Company Accounting Oversight Board.



Figuur 1. Overview IT controls.

Het speelveld

Binnen SOX staat de beheersing van de bedrijfsprocessen ten behoeve van de financiële verantwoording centraal. De IT ondersteunt deze processen en zal daarmee ook voldoende moeten worden beheerst. Voor de gehele beheersing van een organisatie wordt meestal het COSO-model[2] als beheersingsraamwerk gehanteerd. Binnen IT zijn de relevante IT controls in een organisatie in drie categorieën te onderscheiden:

1. organisatiebrede controls (COSO-component Control Environment);
2. applicatiecontroles (input – output controls, autorisaties, interfacecontrols, ...);
3. algemene IT controls (change management, security management, ...).

De laatste twee soorten controls hebben een (in)directe relatie met de bedrijfsprocessen en worden vanuit de geïdentificeerde risico's in de processen geselecteerd. Hierbij worden de applicatiecontroles direct in de processen geïdentificeerd en zijn de algemene IT controls gericht op de IT-componenten die deze applicatiecontroles ondersteunen. Dit artikel beperkt zich tot deze algemene IT controls (hierna IT controls). Bij de selectie van de relevante IT controls komen in de praktijk de volgende vragen naar voren:

- Welke processen, risico's en IT controls zijn relevant?
- Wat wordt onderzocht?
- Hoe worden tekortkomingen geëvalueerd?

Aan de hand van het gesimplificeerde overzicht in figuur 1 zullen deze vragen worden behandeld.

Vanuit de beweringen in de financiële verantwoording worden bedrijfsprocessen geïdentificeerd die een belangrijke (significante) bijdrage leveren aan de standen en stromen in deze verantwoording. Vervolgens zal het management de risicopunten in de bedrijfsprocessen bepalen, gebaseerd op mogelijke significante onjuistheden in de verantwoording. Deze risicopunten worden beheerst door middel van zogenaamde key controls, dit kunnen applicatiecontroles zijn. De goede werking van de applicatiecontroles moet door het management worden aangetoond. Indien een applicatiecontrole niet goed werkt, is het risicopunt niet voldoende beheerst en volgt een proces van het identificeren/testen van compenserende controls of het herstellen van controls en/of het bepalen van de mogelijke fout in de financiële verantwoording. In de praktijk wordt dit proces als vanzelfsprekend ervaren en wordt in organisaties hierop de nadruk gelegd.

Welke processen, risico's en IT controls zijn relevant?

In het kader van SOX zijn uitsluitend de processen en controls relevant die uiteindelijk de betrouwbaarheid van de financiële verantwoording ondersteunen. Voor IT controls is hierover veel gediscussieerd, omdat deze

relatie vaak niet 1-op-1 is te leggen. Het IT Governance Institute heeft, in samenwerking met ISACA, aan het leggen van bedoelde relatie ondersteuning gegeven door de controledoelstellingen (objectives) voor IT te publiceren ([ITGI04b]). Deze objectives zijn gebaseerd op de algemene risico's die voor alle IT controls binnen SOX van toepassing zijn. Hierbij is het van belang de juiste volgorde tussen processen, risico's en IT controls te hanteren om een heldere afbakening te krijgen. Niet de IT-processen, veelal op ITIL gebaseerd, zijn het vertrekpunt, maar de IT-componenten binnen de applicaties, databases, netwerk en operatingsystemen. Deze IT-componenten ondersteunen de goede werking van de applicatiecontroles, die vanuit de bedrijfsprocessen zijn geselecteerd. Vervolgens worden met behulp van de objectives de IT controls geïdentificeerd. De PCAOB Standard No. 2 onderscheid vier gebieden waarop IT controls minimaal aanwezig dienen te zijn, namelijk 'access to programs and data, program changes, program development and computer operations'.

In de praktijk zien we vaak dat organisaties starten met de implementatie van alle ITIL-processen, voorzover nog niet aanwezig. Deze aanpak heeft tot gevolg dat veel procedures en standaarden worden opgesteld. Hierbij bestaat het risico dat deze onvoldoende zijn uitgewerkt in IT controls, gericht op de betreffende IT-componenten. De geïmplementeerde set van procedures is weliswaar een belangrijke randvoorwaarde voor goede beheersing, maar is niet of moeilijk testbaar voor het management/externe auditors indien de directe relatie met de IT-componenten ontbreekt.

Wat wordt onderzocht?

Zoals bij ieder auditproces onderscheiden we het object van onderzoek, de kwaliteitsaspecten waarmee wordt getoetst en de normen waartegen wordt getoetst. In figuur 1 zijn de IT controls (gericht op de beheersing van de IT-componenten) het object van onderzoek, is de betrouwbaarheid het aspect (PCAOB Standard No. 2) en worden de normen verkregen uit de algemeen geaccepteerde standaarden (ITIL, BS7799). Via de IT-componenten die de geïdentificeerde applicatiecontroles uit de bedrijfsprocessen ondersteunen, wordt de link gelegd naar de uiteindelijke betrouwbaarheid van de financiële verantwoording.

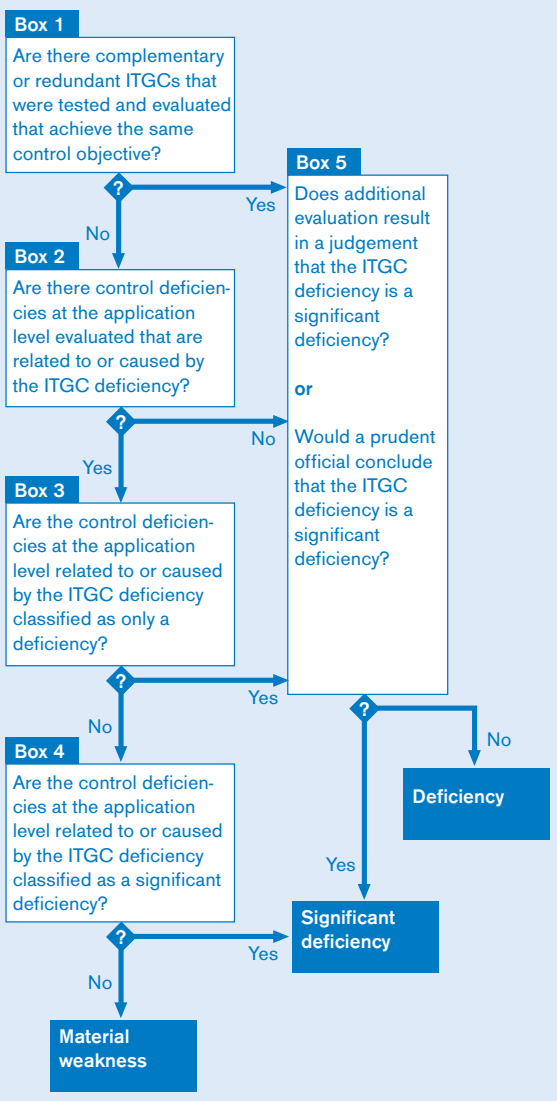
Het bewijsmateriaal voor de effectieve werking van de IT controls wordt voor een groot gedeelte verkregen uit het onderzoeken van de betreffende IT-componenten.

Hoe worden tekortkomingen geëvalueerd?

Indien specifieke IT controls niet werken, is het lastig om de impact hiervan te bepalen, indien er geen relatie is gelegd met de businessprocessen en de daarin opgenomen applicatiecontrols. Door de IT controls direct aan de relevante IT-componenten te relateren, kan een tekortkoming worden geëvalueerd door de impact hiervan op de goede werking van de betreffende applicatiecontroles te bepalen. In overleg met de SEC hebben negen grotere accountantskantoren in de Verenigde Staten een raamwerk opgesteld om onder andere tekortkomingen in de IT controls te kunnen evalueren (zie figuur 2, [Fram04]).

Niet de IT-processen zijn het vertrekpunt, maar de IT-componenten

Indien een IT control niet effectief is, wordt eerst beoordeeld of er compenserende controles aanwezig zijn die dezelfde controledoelstelling halen (Box 1). Ontbreken deze dan wordt vastgesteld of er ineffectieve applica-



Figuur 2. Deficiency evaluation IT controls.

tiecontroles zijn die een relatie hebben met of zijn veroorzaakt door een ineffectieve IT control (Box 2). Vervolgens is het de vraag of deze ineffectieve applicatiecontroles zelf meer zijn dan slechts een 'deficiency' (Box 3). Is dat het geval, dan zal de ineffectieve IT control een 'significant deficiency' of een 'material weakness' zijn (Box 4). In alle gevallen dat de ineffectieve IT control uiteindelijk een 'deficiency' is, moet dit weloverwogen zijn (Box 5). Hierbij wordt verwezen naar de 'prudent official' uit de PCAOB Standard No. 2.

Samengevat betekent dit dat indien een applicatiecontrole wordt aangemerkt als een 'significant deficiency', dit nooit kan leiden tot een 'material weakness' in de (algemene) IT control en daarmee tot een afkeurende 'SOX-verklaring'. Dit onderstreept het belang van het identificeren van de relatie tussen de IT controls ten opzichte van de applicatiecontrole, aan de hand van de IT-componenten! Zoals eerder aangegeven zijn deze IT-componenten onderdelen uit de database, het netwerk en het operatingsysteem die de goede werking van de applicatiecontrole ondersteunen. Binnen de aanwezige IT-infrastructuur zullen de relaties tussen deze IT-componenten moeten worden uitgewerkt, zodat hierop specifiek kan worden getest en tekortkomingen via bovenstaand model kunnen worden geëvalueerd. Met name in grotere IT-omgevingen zal dit een nadere inventarisatie van servers, tabellen, interfaces, etc. tot gevolg hebben. Door deze relaties vooraf gedetailleerd in kaart te brengen kan de totale SOX- (en test-) scope aanzienlijk worden beperkt. Daarnaast kan weloverwogen worden besloten enkele ineffectieve IT controls niet op te lossen, bijvoorbeeld indien de betreffende applicatiecontroles wel effectief zijn of slechts een 'deficiency'.

Bovenstaande betekent niet dat IT controls die geen directe invloed hebben op de goede werking van de applicatiecontroles, niet relevant zouden zijn, omdat zij niet direct kunnen leiden tot een 'material weakness'. Een veelheid van tekortkomingen duidt op een minder goed beheerste control environment, wat op zich een 'significant deficieny' of 'material weakness' kan zijn. Via de 'prudent official' lijkt 'professional judgment' ook hier onontbeerlijk.

Conclusie

'The ball' of 'waar het eigenlijk om draait' binnen SOX is het zichtbaar aantonen dat de relevante risico's voldoende effectief worden beheerst gericht op de betrouwbare financiële verantwoording. Dit betekent dat niet alle gesignaleerde tekortkomingen in de IT controls even relevant zijn en dat er zal moeten worden gezocht naar een directe relatie met de belangrijke applicatiecontroles (via de relevante IT-componenten). Dit zal geen makkelijke opgave zijn, maar zorgt wel voor de juiste focus in scope (breedte en diepgang).

Het spreekt voor zich dat IT governance, ook binnen SOX, in eerste instantie een verantwoordelijkheid is van het gehele management ('The eyes'), waarbij het ervoor moet zorgen dat de juiste focus wordt gelegd. Als uiteindelijk niet alle tekortkomingen in de IT controls even belangrijk zijn, kunnen prioriteiten worden gelegd bij de implementatie en het testen van de IT controls. Kortom: 'Keep your eyes on the ball'.

Literatuur

[Fram04] *A Framework for Evaluating Control Exceptions and Deficiencies, Version 3*, december 2004.

[ITGI04a] IT Governance Institute, *IT Governance Global Status Report*, 2004.

[ITGI04b] IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley*, april 2004.

[John05] Everett C. Johnson, CPA, *IT Governance: new players, challenges and opportunities*, Information Systems Control Journal, Volume 2, 2005.

[NORE04] NOREA, *IT-Governance, een verkenning*, juni 2004.