

Top 10 lessons learned SOx

Over het boekjaar 2004 zijn in Amerika voor de eerste keer SOx-statements afgegeven. In deze statements geeft het management een verklaring dat de controlemaatregelen van voldoende niveau zijn en waar mogelijk 'defecten' zitten. Op basis van de ervaringen die organisaties hebben met SOx zijn een aantal lessen te leren uit de praktijk.

JEROEN VAN DEN OEVER EN BOUDEWIJN WILDEMAN

1 Institutionaliseer risicobewustzijn
De invoering van SOx-wetgeving leidt tot verandering in denken en doen voor medewerkers. De SOx-wetgeving richt zich op het testen en aantonen van de controlemaatregelen in de praktijk. Deze controles kunnen ervoor zorgen dat medewerkers het gevoel krijgen dat zij 'gecontroleerd' worden en worden afgerekend op eventuele defecten. Het management wil zelf een positieve en heldere sfeer creëren rondom de SOx-wetgeving. Daarom is tijdens de implementatie ruime aandacht voor interne communicatie en training noodzakelijk. Als gevolg van die openheid zien medewerkers een duidelijk verband tussen de te behalen organisatiedoelen en als afgeleide in het kader van SOx de hiermee gemoeide risico's, de controleactiviteiten en de verantwoording hierover. Deze openheid en dit inzicht leidt tot een groter risicobewustzijn van medewerkers. Dit geeft medewerkers een groter bewustzijn ten aanzien van hun eigen mogelijkheden en verantwoordelijkheden om risico's te beperken.

2 Stel een blauwdruk van de organisatie samen
Beursgenoteerde ondernemingen bestaan uit meerdere organisatieonderdelen met eigen processen. Deze processen zijn vaak in een keten met elkaar verbonden, waarbij partijen onderling werkzaamheden voor elkaar uitvoeren. Om het totale

interne control framework (ICFR) in zijn samenhang te kunnen beoordelen is het noodzakelijk de ketens met bijbehorende rollen en verantwoordelijkheden in kaart te brengen. Op basis van dit totaalbeeld, de blauwdruk, is het eenvoudig om de relatie met het grootboek te bepalen en de SOx-relevantie van de controls en processen in de keten te achterhalen. Hetzelfde is van toepassing op de IT-infrastructuur van de organisatie. Vooral bij de categorie IT general controls en de application controls is het bepalen en afdekken van de SOx-scope een lastige klus. Breng daarom het systemenlandschap en de achterliggende infrastructuur helder in kaart.

3 Interpreteer SOx breder
Een SOx-implementatie kent over het algemeen een negatieve start: het is een wettelijke verplichting waaraan moet worden voldaan, gaat ten koste van klantprojecten en drukt het resultaat van de onderneming. Het is aan te bevelen de wetgeving breder te interpreteren: de SOx-activiteiten dragen bij aan het inzicht op welke plekken in de organisatie efficiencyvoordelen behaald kunnen worden door het uniformeren van gelijksoortige processen. Dit inzicht ontstaat door het in kaart brengen van de gehele procesgang en intensief testen van de controls. Vanuit kwalitatief oogpunt kan in de keten dezelfde betrouwbaarheid van de financiële verslaggeving gewaarborgd worden met minder controls.

4 **Betrek controlerend accountant en interne accountantsdienst tijdig**

Het scheelt veel tijd en inspanning wanneer bij aanvang van de implementatie directe samenwerking wordt gezocht met de controlerend accountant en de interne accountantsdienst. Bespreek de bepaling van SOx-significante accounts en selectie van SOx-kritische processen. Creëer samen heldere richtlijnen en een normenkader voor de lokale internal control frameworks. Plan vroegtijdige reviews in om de kwaliteit van controls en processen te beoordelen en om eventueel herstelwerkzaamheden uit te voeren.

5 **Definieer key controls top-down**

Te veel controls als 'key' aanmerken leidt tot een tegengesteld effect. In plaats van betrouwbaarheid van financiële verslaglegging ontstaat een onbeheersbaar en niet transparant bouwwerk van controls. Voor een top-down benadering is inzicht in de totale procesgang noodzakelijk. Dit inzicht is niet eenvoudig te achterhalen en vaak tijdrovend. Echter, de éénmalige investering betaalt zich terug doordat met dit inzicht de key controls scherp gekozen kunnen worden. Additioneel profiteert de organisatie van de jaarlijkse besparing in de testwerkzaamheden.

6 **Neem de tijd voor testwerkzaamheden en bedenk eerst een testaanpak**

De organisatie leert het meeste over de kwaliteit van haar ICFR door het daadwerkelijk testen van key controls en het uitvoeren van lijncontroles op SOx-relevante processen. Houdt de periode van documenteren relatief kort en de testcycli waarin testen, defecten oplossen en hertesten plaatsvindt relatief lang om mogelijke bevindingen tijdig te kunnen opvangen. De testwerkzaamheden van de key controls kunnen in bepaalde gevallen aanzienlijk worden beperkt door controls te clusteren of door een lagere frequentie voor de key control te kiezen.

De Sarbanes-Oxley Act

Na een reeks van schandalen bij beursgenoteerde ondernemingen bestond internationaal de behoefte aan meer zekerheid binnen organisaties om toekomstige boekhoudschandalen te voorkomen. Voor Amerika was dit aanleiding tot het formuleren van wetgeving die het vertrouwen van beleggers moest herstellen. Deze Sarbanes-Oxley Act (SOx), voor het gemak genoemd naar de indieners ervan, is in de zomer van 2002 in de Verenigde Staten in werking getreden. De officiële benaming van de wet is de 'Public Company Accounting Reform and Investor Protection Act' en beslaat een groot aantal terreinen, onder andere risico-beheersing en interne controle. De wet richt zich op een van de meest cruciale vragen op financieel gebied binnen een onderneming: *Zijn de interne controle maatregelen in de organisatie qua opzet, bestaan en werking van een zodanig niveau, dat de getrouwheid van de financiële verantwoording is gewaarborgd?*

7 **Optimaliseer de betrokkenheid van de lijnorganisatie**

De kennis van de business over procesgang, uitvoering van key controls en werking van applicaties is onmisbaar. Laat SOx geen feestje van de financiële functie zijn, maar betrek het lijnmanagement en haar medewerkers in de implementatie. Immers, het management in kwestie zal na afronding een oordeel moeten vellen over de werking van het ICFR en de medewerkers zullen veel van de SOx-relevante key controls in de dagelijkse praktijk uitvoeren. Ook moet er specifieke aandacht zijn voor de functioneel ontwerpers/beheerders van SOx-relevante systemen. Zij hebben inzicht in de werking van de geprogrammeerde controles (application controls) en de grootboekrekeningen die de systemen vullen.

8 **Procesgerichte sign-off procedure**

De sign-off door het management is vaak complex omdat er zeer veel verschillende SOx-relevante processen zijn die over meerdere juridische eenheden en eventueel service organisaties verspreid zijn. Alleen al de realisatie van de sign-off kan aangemerkt worden als een separaat 'logistiek' project. De uitdaging is om de sign-off boom van verantwoordelijke managers die moeten tekenen zo compact mogelijk te houden. Uiteindelijk tekent de (bedrijfsketen)proceseigenaar af voor haar proces, op basis van de testresultaten en de interpretatie hiervan door de procesdeskundigen. De proceseigenaar rapporteert vervolgens rechtstreeks aan CEO en CFO. Uiteindelijk wordt formeel afgetekend door CEO en CFO.

9 **Benoem rollen en verantwoordelijkheden vroegtijdig**

In het structurele SOx-proces zijn verschillende rollen te onderkennen: de SOx-regisseur, lijnmanagement, change management, testcoördinator, medewerkers die controles uitvoeren en testers. Een vroegtijdige betrokkenheid van deze rollen faciliteert de borging van het structurele jaarlijkse SOx-proces. Eventuele kennisachterstand met betrekking tot het AO/IC-vakgebied of de SOx-wetgeving kan gedurende de implementatie via bijvoorbeeld training-on-the-job worden hersteld. Praktijk leert echter dat organisaties benoeming van vaste lijnfunctionarissen op bovenstaande rollen te lang uitstellen. Dit vertraagt het borgingsproces en leidt tot efficiencyverlies.

10 **Lever projectresultaten tijdig en volledig op**

Tijdens de invoering worden verplichte deliverables vaak periodiek opgeleverd, bijvoorbeeld control matrices, controlbeschrijvingen en testresultaten. Het juist en volledig invullen van deze documenten vergt tijd en overzicht. Het opleveren van de documenten is van belang, aangezien deze de basis zijn voor aftekening en de controlewerkzaamheden van de externe accountant. Ervaring leert echter dat onvoldoende time-management de grootste oorzaak is van onjuiste, onvolledige, en vertraagde oplevering van projectresultaten.