

Werking en gevolgen van SOx

Na een reeks van boekhoudschandalen werd in 2002 in de Verenigde Staten de Sarbanes-Oxley Act (SOx) van kracht, wetgeving die het vertrouwen van beleggers moest herstellen. Dit overzichtsartikel behandelt eerst de SOx-wetgeving. We gaan daarna in op de term SOx-compliance: wat betekent het eigenlijk om SOx-compliant te zijn? Vervolgens wordt de SOx-jaarcyclus toegelicht. Als laatste wordt de impact van SOx op organisaties besproken.

MARTINE WESTSTEIJN EN SILVIA VAN DER WERVE RE

De *Public Company Accounting Reform and Investor Protection Act*, de officiële benaming van SOx, beslaat een groot aantal terreinen, onder andere risicobeheersing en interne controle. Zij stelt in essentie de vraag: zijn de interne controlemaatregelen in de organisatie qua opzet, bestaan en werking van een zodanig niveau, dat de getrouwheid van de financiële verantwoording is gewaarborgd?

Daartoe moeten:

- de CEO en CFO verklaren dat de interne controlemaatregelen met betrekking tot financiële rapportage effectief zijn (het SOx-statement, oftewel een in-control-verklaring);
- een externe accountant geeft een soortgelijke verklaring af over de getrouwheid van deze verklaring.

SOx in vogelvlucht

De SOx-wetgeving is van toepassing op alle aan de Amerikaanse beurs genoteerde bedrijven, inclusief de 'foreign registrants' en bedrijven die zo'n notering nastreven; de wet heeft dus ook extraterritoriale werking. De forse gevolgen komen vooral tot uitdrukking in de secties 302 en 404 van de wet.

De sectie 302, 'Corporate Responsibility for financial reports', stelt dat het management elk kwartaal moet verklaren dat de inhoud van de financiële en niet-financiële rapportages juist en volledig is, de verschillende rapportage-

systemen betrouwbaar zijn en dat tijdig is gerapporteerd. Via deze verplichting, waarover expliciet gerapporteerd moet worden, wordt transparantie ten aanzien van de cijfers afgedwongen.

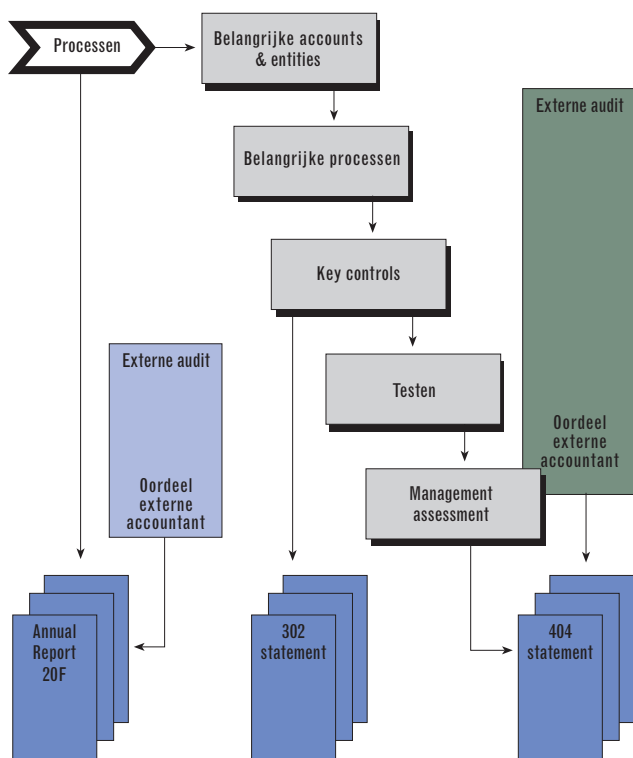
De sectie 404, 'Management Assessment of internal controls', bestaat voornamelijk uit een verklaring over de verantwoordelijkheid van het management voor het opzetten en handhaven van een adequaat internal control framework (ICF) en adequate procedures met betrekking tot de financiële verslaglegging.

De SOx-wetgeving maakt dat bestuurders hoofdelijk aansprakelijk kunnen worden gesteld als ze de wet overtreden (ze moeten tekenen voor het in control zijn). De straffen bij overtreding van de wet zijn geldboetes van miljoenen dollars en zelfs celstraffen tot 20 jaar.

Opdat CEO en CFO de garantie voor beheersing van risico's en correcte uitvoering van controls kunnen geven zijn ook andere afdelingen, vooral risk management en de interne accountantsdienst, actief bij het SOx-proces betrokken.

Wanneer is een onderneming SOx-compliant?

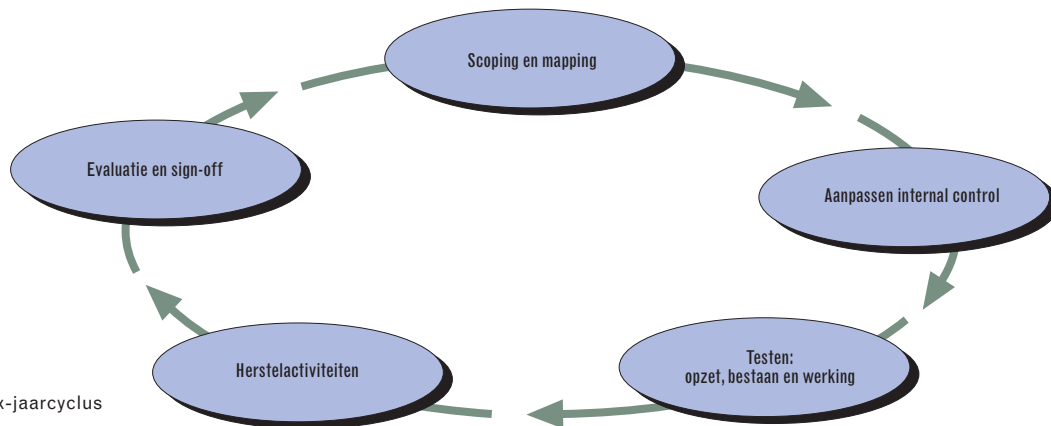
Als je als bedrijf kunt aantonen dat de cijfers in de jaarrekening een getrouw beeld geven van de werkelijkheid, ben je SOx-compliant. Dat lijkt weinig verschil met vroeger, want



Figuur 1. Overzicht SOx-werkzaamheden

sinds er jaarrekeningen worden opgesteld, moeten deze een getrouw beeld van de werkelijkheid geven. Het grote verschil zit in het woord aantonen. De SOx-wet geeft aan dat je moet aantonen dat je in control bent, dat je voldoet aan de wet. Dit aantonen, ofwel: ‘show me the evidence, prove me the effectiveness’, zorgt voor meer werk dan vroeger. Vóór het SOx-tijdperk was ‘tell me, trust me’ het adagium. De organisatie zal een aantal stappen moeten doorlopen om de 302- en 404-verklaringen (statements) te kunnen afgeven.

De organisatie zal inzicht moeten hebben in de belangrijke posten op de jaarrekening. Niet alleen van de jaarrekening-posten, maar ook van de onderliggende grootboekrekeningen wordt bepaald of zij belangrijk zijn voor de jaarrekening. De geselecteerde posten komen tot stand door processen. Deze processen worden aangemerkt als significante processen (ofwel de belangrijke processen). Hierbij is het goed om te realiseren dat dit niet alle processen in de organisatie zijn, alleen die processen die verantwoordelijk zijn voor de totstandkoming van de jaarrekeningposten. Binnen de processen loopt men risico's. Deze risico's wil de organisatie al dan niet afdekken door maatregelen (controls). Binnen de significante processen zijn niet alle maatregelen belangrijk. Voor de SOx-verklaringen zijn alleen die controls belangrijk die noodzakelijk zijn om een juiste afspiegeling van de financiële gang van zaken te garanderen



Figuur 2. De SOx-jaarcyclus

(key controls). Daarnaast is het belangrijk dat de organisatie laat zien dat zij de organisatie zo heeft ingericht dat:

- het management een goede beheersomgeving heeft gecreëerd, waarin de medewerkers gemotiveerd zijn om te voldoen aan de wet- en regelgeving in plaats van deze te negeren of te omzeilen;
- het management een goede monitoring en corrigerende maatregelen heeft ingevoerd indien de medewerkers niet voldoen aan de wet- en regelgeving.

Om dit te kunnen aantonen vult de organisatie de COSO-questionnaire in. Deze questionnaire bestaat uit een aantal vragen, die antwoord geven op de bovenstaande punten. Het management geeft in de 302-verklaring aan dat de organisatie voldoet aan de bovenstaande punten.

Het totaal aan processen, risico's en belangrijke maatregelen zijn of zullen in een internal control framework moeten worden vastgelegd. Veelal wordt dit per proces vormgegeven in een key control matrix, waarin de belangrijkste risico's zijn opgenomen en de belangrijke beheersmaatregelen, de key controls.

Uit hoofde van de 404-sectie zal het management moeten aantonen dat de key controls in opzet aanwezig zijn, bestaan en werken. Nadat het management de bewijzen van opzet, bestaan en werking heeft geëvalueerd en beoordeeld, kan uiteindelijk de 404-verklaring getekend worden. Bij deze sign-off zijn in de grotere organisaties verschillende managementlagen betrokken die al eerdere deelverklaringen hebben

getekend. Wat de aansprakelijkheid betreft, hebben hiermee niet alleen de CEO en de CFO een verantwoordelijkheid, maar ook de andere managementlagen die hebben meegetekend. Het neemt niet weg, dat de CEO en de CFO uiteindelijk natuurlijk altijd eindverantwoordelijk blijven. Omdat de 404-verklaring een interne verklaring is, vereist de SOx-wet dat de externe accountant een oordeel geeft over deze verklaring. Geeft de 404-verklaring een getrouw beeld van de werkelijkheid? Dit is een soortgelijke verklaring als de accountant altijd al gaf bij de jaarrekening.

De SOx-jaarcyclus

SOx is geen eenmalige activiteit; elk jaar weer moeten de CEO en de CFO tekenen voor het in control zijn van de organisatie. Dus ieder jaar zal de organisatie een aantal stappen moeten doorlopen:

1. scoping en mapping
2. aanpassen internal control framework
3. testen opzet, bestaan en werking
4. herstelactiviteiten
5. evaluatie en sign-off

Deze stappen vormen de SOx-jaarcyclus (figuur 2).

Hierbij is een duidelijke rolverdeling een belangrijke succesfactor, met name rond change management, testen van het interne controle-framework en expert-ondersteuning; maar ook tussen de CEO, de CFO, de SOx-proceseigenaren, de SOx-regisseur, de SOx-testcoördinator en de testers. De CEO en de CFO zijn eindverantwoordelijk en aansprakelijk voor alle SOx-activiteiten binnen hun organisatie zoals beschreven in de SOx-verklaring die ze jaarlijks moeten ondertekenen. De SOx-regisseur, rechtstreeks ressorterend onder CEO of CFO, vult hun directe verantwoordelijkheden in door de aansturing en begeleiding van activiteiten in de lijnorganisatie. De IAD reviewt de eindproducten van de SOx-cyclus. De (de)centrale risk management-afdeling wordt geconsulteerd voor assessments en het definiëren van controls. Daarnaast is zij verantwoordelijk voor de controle op het realiseren van de SOx-compliance door de lijnorganisatie en de borging daarvan in bestaande of nieuwe procedures en werkwijzen.

Scope en mapping

De eerste fase van de SOx-jaarcyclus wordt ingegaan op de bepaling van de scope en mapping. De bepaling van de SOx-scope binnen de organisatie geschiedt doordat men op cen-

Wat heeft SOx gekost?

De bedragen die aan SOx worden uitgegeven, verschillen per organisatie, omdat niet elk ICF een gelijkwaardig kwaliteitsniveau heeft. Nederlands onderzoek (Limbus Consulting, 2004) wijst uit dat er in 2004 gemiddeld 2000 interne mandagen aan de invoering van SOx werden besteed, in geld uitgedrukt minimaal 1 miljoen euro. De additionele it-investeringen varieerden van 0,3 miljoen tot 3 miljoen euro. In de VS zijn die bedragen fors hoger. Bijna 50 procent van de financiële managers in Nederland ziet invoering van de wet niet als een verbetering in de externe verslaggeving en slechts in beperkte mate een verbetering in de interne beheersing. In dit kader kan het bericht dat de SEC haar regels voor 'foreign registrants' heeft versoepeld, niet onverwacht zijn.

traal niveau naar aanleiding van eventuele wijzigingen in de verlies & winst-rekening en de balans ten opzichte van voorgaand rapportagejaar de materiële posten in de jaarrekening (belangrijke accounts) bepaalt. Tevens wordt bepaald welke materialiteitsgrenzen gelden voor de belangrijke accounts, alsmede de onderliggende en belangrijke grootboekrekeningen. Ten slotte worden de grootboekrekeningen gekoppeld aan de hoofdprocessen die verantwoordelijk zijn voor de standen en mutaties van deze rekeningen. Naast de bepaling van SOx-relevante jaarrekeningen en grootboekrekeningen op basis van de belangrijke accounts dient men bij de scope-bepaling ook te kijken naar producten of processen die als zeer risicovol worden gepositioneerd en om die reden kunnen leiden tot mogelijke misstanden in de jaarrekening. Vaak vindt mapping hiervan bottom-up plaats doordat men vanuit processen en producten met een groot inherent risico bepaalt op welke grootboekrekeningen zij terecht komen. De SOx-scope is bepalend voor al het werk dat hierna moet gebeuren. Hoe groter de scope, hoe meer werk er gedaan moet worden voor de SOx-verklaring.

Aanpassen internal control framework

Het belangrijkste en meest tijdrovende onderdeel van de doorvoering van sectie 404 van de SOx-wet is het opzetten en handhaven van een adequaat internal control framework (ICF) en adequate procedures met betrekking tot de financiële verslaglegging. Het ICF is opgedeeld in de processen in de keten en uitgewerkt per proces. De risicoanalyse in deze fase is een uitvloeisel van de vorige en wordt gebruikt om de relevante risico's inzichtelijk te maken. Men identificeert de belangrijkste financiële en operationele risicogebieden. Dan maakt men een onderverdeling van belangrijke posten in verschillende risicoprofielen en associeert getrouwheidsaspecten van de jaarrekening (financial statement assertions) met elke significante post. De belangrijkste soorten transacties en aanverwante processen worden geïdentificeerd. Het verband tussen de processen/transactiestromen en de belangrijke posten worden bepaald.

De scope beperkt zich bewust slechts tot de financiële stromen, in het kader van SOx zijn key controls op het operationele proces niet relevant. Een key control is cruciaal, omdat die mogelijke risico's in het proces afdekt en waarborgt dat de uitgevoerde processen leiden tot juiste, volledige en tijdige vastleggingen in de financiële administratie. Risico's en key controls worden vastgelegd in een key control matrix, die de koppeling tussen de grootboekrekening en de processtappen aangeeft, de risico's en maatregelen en tevens de verwachte documentatie.

SOx-compliant zijn betekent dan, dat de key controls géén materiële leemten of significante tekortkomingen bevatten die afbreuk doen aan de representatie van de cijfers. Er zijn drie soorten controlemaatregelen: manual controls, application controls en it general controls, die zowel preventief als detectief van aard kunnen zijn. Manual en application controls kunnen per transactie plaatsvinden (transactional) of een algemene werking hebben (managerial). De it general controls (ITGC) lijken veel op beheersingskaders die worden gebruikt voor operationele processen, maar omvatten specifieke aspecten als betrouwbaarheid, integriteit en beschikbaarheid van data.

Testen

Voordat ze tot het ondertekenen van dergelijke rapportages kunnen overgaan, hebben de CEO en de CFO behoefte aan bewijsmateriaal (evidence) dat de controlemaatregelen voldoende gewerkt hebben en de geïdentificeerde risico's zijn afgedekt. Het verzamelen van de evidence gebeurt door het uitvoeren van testen op opzet, bestaan (ToD) en de juiste werking van controls (ToE).

Herstellen

Wanneer blijkt dat de testen geen volledig bevredigend resultaat hebben opgeleverd, moeten herstelactiviteiten plaatsvinden. De herstelactiviteiten kunnen betrekking hebben op opzet, bestaan en/of werking. Uiteraard afhankelijk van waar zich een defect heeft voorgedaan. Het kan voorkomen dat er meerdere defecten worden gemeld. Om te zorgen dat de organisatie de capaciteiten voor het herstel en de her-testen zo goed mogelijk inzet, is het van belang dat men voldoende tijd besteedt aan het inschatten van het defect. Dat wil zeggen dat belangrijkere defecten (die een grotere impact op misstanden in de financiële verslaglegging hebben) eerder moeten worden opgelost dan minder belangrijke.

Evaluatie en sign-off

De SOx-rapportage geeft ten slotte een samenvatting van alle voorgaande stappen in het proces: scoping, doorvoeren van wijzigingen in de onderneming, testen en testbevindingen. Tevens worden de testrapporten uit alle juridische entiteiten geaggregeerd en worden globale conclusies voor opzet, bestaan en werking en het totale interne-controle-framework getrokken. Als sluitstuk van de structurele cyclus bespreken de CEO en de CFO de SOx-rapportage met de groepsverantwoordelijke voor SOx. De SOx-rapportage dient hiertoe als uitgangsdokument, inclusief de eventuele deelverklaringen van de verschillende onderdelen. Nadat CEO en CFO hun goedkeuring hebben verleend aan de SOx-rapportage, kan de formele SOx-verklaring worden opgesteld en worden ondertekend door CEO en CFO (sign-off), met inachtneming van de verplichte disclosures. Ten slotte wordt de verklaring gedeponereerd bij de SEC.

Wat doet SOx met een organisatie?

Invoering van SOx in een organisatie veroorzaakt een grote verandering in het gedrag van de medewerkers, het management, zijn toezichthouders en accountants. De impact is groot en wordt direct gevoeld. Zo heeft SOx naast bedoelde ook onbedoelde effecten.

De impact van de SOx-wetgeving op de organisatie wordt bepaald door de volgende factoren:

- de kwaliteit van het bestaande internal control framework;
- imago'schade;
- terughoudendheid onder accountants;
- comfortgevoel bij het management.

Hoeveel vertrouwen de CEO en de CFO in het ICF (kunnen) hebben is de belangrijkste factor van de SOx-impact voor een onderneming. Wanneer tijdens een SOx-implementatie aan méér dan alleen de minimale vereisten van compliancy aandacht wordt besteed, leidt invoering van de wet tot een grotere flexibiliteit van en transparantie in de bedrijfsprocessen en duidelijke communicatielijnen.

De SOx-wet verordonneerde ook de oprichting van een toezichthoudend orgaan op de accountantsbureaus. Deze Public Company Accounting Oversight Board (PCAOB) heeft verregaande bevoegdheden, waaronder een mogelijkheid tot onbeperkte sanctiëring. Praktijkervaring leert dat de accountant als reactie hierop uiterst voorzichtig is met het vellen van een oordeel. Op haar beurt zoekt het management zekerheid vóórdat zij de compliancy statement ondertekent, bijvoorbeeld in het hanteren van een brede scope. Méér werkzaamheden, meer controlewerk en een grotere impact dan noodzakelijk zijn hiervan het gevolg. Naar onze mening gaan de meeste accountants in hun terughoudende opstelling voorbij aan de taak van de natuurlijke adviesfunctie en blokkeren ze hiermee één van de essentiële succesfactoren van een goede SOx-implementatie: vroegtijdige en proactieve betrokkenheid van de accountant.

Het effect van een implementatie van interne beheersing op een organisatiecultuur verschilt per bedrijf. Het opstellen van een internal control framework leidt niet in alle gevallen tot een goede uitkomst en een SOx-statement. Dit is met name het geval wanneer een ICF mechanisch wordt toegepast zonder voeling te houden met de organisatie. Wanneer de medewerkers vrezen persoonlijk slachtoffer te worden van slecht nieuws en hierdoor fouten gaan verstoppen, ontkennen of niet rapporteren, ontstaat een angstcultuur. In een bureaucratische cultuur raakt men snel verstrikt in het controleren en beoordelen van elkaar en is er een hoge behoefte

om verantwoording af te leggen. Hierdoor wordt het behalen van de doelstellingen van de AO/IC een doel, in plaats van een middel.

Als laatste dan nog even dit: laat SOx geen feestje van de financiële functie zijn, maar betrek het lijnmanagement en de medewerkers bij de implementatie. Immers, het management in kwestie zal na afronding een oordeel moeten vellen over de werking van het ICF en de medewerkers zullen veel van de SOx-relevante controls in de dagelijkse praktijk uitvoeren. **-C**

Dit artikel is een bewerking van het boek *Handen & Voeten aan Sarbanes Oxley, denken durven voelen*, door drs. Jeroen van den Oever RA mnc, drs. Boudewijn Wildeman, drs. Evienne Peeters RO en drs. Martine Weststeijn.

Haal hier PE-punten mee

Bij dit artikel hoort een online cursus waarmee u punten kunt halen in het kader van uw permanente educatie (PE). Kijk voor meer informatie en een overzicht van alle cursussen op www.finance-en-control.nl/pe. Ter kennismaking kunt u de cursus *Control self assessment* gratis volgen en uw eerste studiepunten binnenhalen.

advertentie