

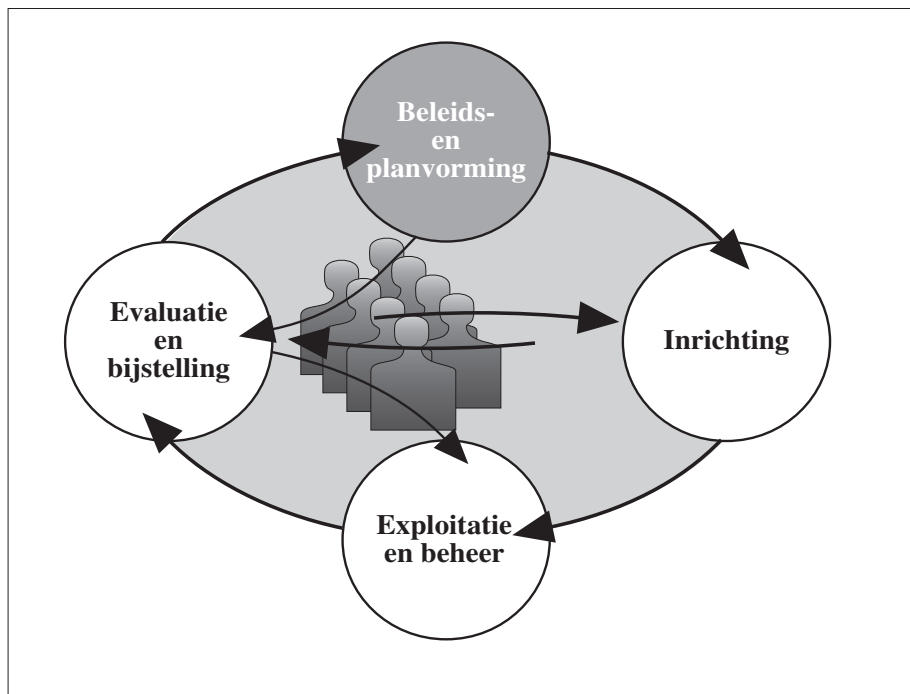
2.1.1.K Randvoorwaarden voor succesvolle implementatie van een AO/IC-bouwwerk voor Sarbanes Oxley 302/404

Toelichting van de redactie

Het opzetten van een Sox 302/404-project vereist een zorgvuldige aanpak. De auteur geeft aandachtspunten en randvoorwaarden voor de opzet van een dergelijk project.

Trefwoorden

Sarbanes Oxley, OA/IC, fraude



2.1.1.K Randvoorwaarden voor succesvolle implementatie van een AO/IC-bouwwerk voor Sarbanes Oxley 302/404

Drs. E.P. Johannsmann

Samenvatting

Na een korte inleiding over de achtergrond en tekortkomingen van de Sarbanes Oxley Act en de relatie met AO/IC beschrijft dit artikel de randvoorwaarden voor succes bij de opstartfase van een SOx-302/404-project. Uiteraard gelden alle algemene randvoorwaarden voor succes die voor ieder project gelden. Zo is een heldere scopeafbakening cruciaal voor elk project, maar in het geval van een SOx-project is deze gecompliceerder dan doorgaans het geval is. Een tweede randvoorwaarde zijn concernbrede architectuurstandaarden. Deze mogen geen vrijblijvend hulpmiddel zijn, maar zijn een verplichte 'kapstok'. Een derde randvoorwaarde is dat er bij de start van het project een goed inzicht bestaat in de bestaande architectuur. Onvoldoende inzicht door bijvoorbeeld onvolledige, onjuiste en ontbrekende procesbeschrijvingen en handleidingen van informatiesystemen leiden onherroepelijk tot hogere kosten, doorlooptijd of afbreuk aan kwaliteit.

I Inleiding

Dit artikel gaat over de opzet en uitvoering een Sarbanes Oxley 302/404-project. De Sarbanes Oxley Act is relatief nieuwe Amerikaanse antifraudewetgeving uit het jaar 2002. Doel van de Sarbanes Oxley Act (in het Nederlands afgekort als SOx¹) is het streven om boekhoudkundige schandalen te voorkomen. Aanleiding zijn de grote schandalen in de Verenigde Staten die de laatste tijd aan de orde van de dag zijn geweest. Hierbij valt onder andere te denken aan Enron, Worldcom en Global Crossings. Ook Europa is niet verschoond gebleven; vers in het geheugen liggen de affaires rond Nederlands-Amerikaanse KPN Qwest, het Nederlandse Ahold, het Italiaanse Parmalat en kort voor het ter perse gaan van dit artikel kwam daarbovenop het Nederlands-Britse Shell dat haar oliereserves te hoog heeft gewaardeerd. Verwacht wordt dat ook Europa op korte termijn gelijksoortige wetgeving zal invoeren.

De SOx Act bestaat uit 11 hoofdstukken met vele ge- en verboden waar ondernemingen aan moeten voldoen. De meest omvangrijke en complexe daarvan zijn de verplichtingen zoals genoemd in de SOx-paragrafen 302 en 404.

Dit artikel beschrijft de randvoorwaarden voor succes bij de opstartfase van een SOx-302/404-project. In figuur 1 wordt de focus van dit artikel grafisch weergegeven. Als er verderop in dit artikel over een 'SOx-project' wordt gesproken, wordt er een project bedoeld dat zich richt op de paragrafen 302 en 404.

In dit artikel zal niet worden ingegaan op het nut, dan wel de juridische aspecten van de SOx Act. Ook wordt er niet ingegaan op regelgeving voor externe verslaggeving, de rol van de (forensisch) accountant en inhoudelijke aspecten, zoals identificatie van SOx-risico's en het ontwerp van een adequate Administratieve Organisatie/Interne Controle (AO/IC) en EDP auditing. Voor deze onderwerpen wordt verwezen naar de veelheid aan bestaande literatuur.

In paragraaf 2 worden de achtergrond en tekortkomingen van de Sarbanes Oxley Act en de relatie tussen SOx en AO/IC kort behandeld. In paragraaf 3 worden de randvoorwaarden voor een Sox-project beschreven. De lezer wordt geacht bekend te zijn met de materie van AO/IC. In dit artikel zal dan ook niet nader worden ingegaan op de inhoud van SOx-risico's en de te nemen AO/IC-maatregelen. Er wordt uitsluitend ingegaan op de wijze waarop SOx-risico's kunnen worden geïdentificeerd.

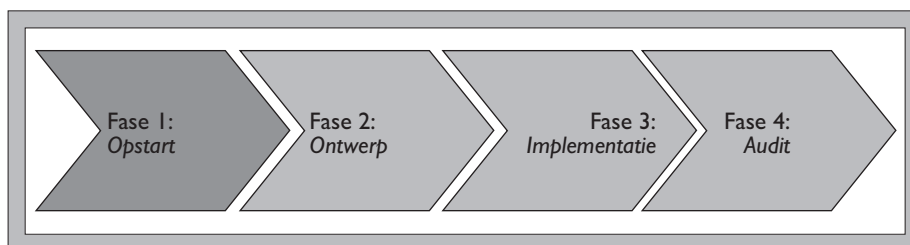
2 Achtergrond Sarbanes Oxley Act en relatie met AO/IC

Nederlandse ondernemingen met een notering aan de Amerikaanse beurs, evenals in Nederland gevestigde dochters van Amerikaanse ondernemingen dienen aan de SOx Act te voldoen. In 2003 ging het om 44 Nederlandse ondernemingen en een veelvoud aan dochters van Amerikaanse ondernemingen. Belangrijk element van SOx is dat bestuurders van vennootschappen hoofdelijk aansprakelijk kunnen worden gesteld als ze de SOx Act overtreden. In de Verenigde Staten hangen bestuurders boetes van miljoenen dollars en celstraffen tot 20 jaar boven het hoofd als ze veroordeeld worden.

2.1 Inhoud van de Sarbanes Oxley Act 2002

De hoofdstukindeling van de Sarbanes Oxley Act 2002 ziet er als volgt uit:

- I Public Company Accounting Oversight Board
- II Auditor Independence
- III Corporate Responsibility
- IV Enhanced Financial Disclosures
- V Analyst Conflicts of Interest
- VI Commission Resources and Authority
- VII Studies and Reports



Figuur 1 Focus van dit artikel betreft de opstartfase

- VIII Corporate and Criminal Fraud Accountability Act of 2002
- IX White-Collar Crime Penalty Enhancements
- X Corporate Tax Returns
- XI Corporate Fraud and Accountability

In de context van dit artikel, waar het gaat om het realiseren van een adequaat stelsel van interne controlemaatregelen, zijn uitsluitend de hoofdstukken III en IV relevant. Binnen de hoofdstukken III en IV zijn respectievelijk de paragrafen 302 en 404 van belang.

2.2 SOx lacune: niet alle risico's worden door SOx afgedekt

Naast het risico op foutieve externe rapportages en het risico op fraude gaat de SOx Act voorbij aan veel andere ondernemersrisico's. Met andere woorden: als een onderneming SOx-compliant wordt verklaard kunnen externe belanghebbenden er met relatief grote mate van zekerheid vanuit gaan dat de informatie in de verslaggeving correct is en er maatregelen zijn genomen tegen fraude, maar dat wil niet zeggen dat de onderneming geen andere risico's loopt die in de toekomst het aandeel kunnen doen kelderen. Lacunes in SOx:

- SOx richt zich niet op overige ondernemersrisico's (zoals bedrijfseconomische risico's);
- SOx is gericht op de kwaliteit van de verantwoording over het verleden en niet op de kwaliteit van toekomstprognoses;
- SOx is gericht op de vraag of we de dingen goed doen en vraagt zich niet af of we de goede dingen doen. SOx stelt bijvoorbeeld niet de eis dat een bedrijf bepaalde functies uitvoert (zoals marktonderzoek of forecasting); als een organisatie niet aan marktonderzoek of forecasting doet, is dit

conform SOx niet ernstig. Pas als het bedrijf deze processen wel uitvoert, maar ze niet naar behoren uitvoert, spreekt SOx van een risico.

Dit zijn in de optiek van de auteur serieuze tekortkomingen van de SOx Act; deze verschafft hierdoor slechts schijnzekerheid aan externe belanghebbenden.

In paragraaf 3.1.1. zal nader worden ingegaan op de verschillende soorten risico's die binnen, dan wel buiten de scope van SOx vallen.

2.3 Inhoud van de SOx-paragrafen 302 en 404

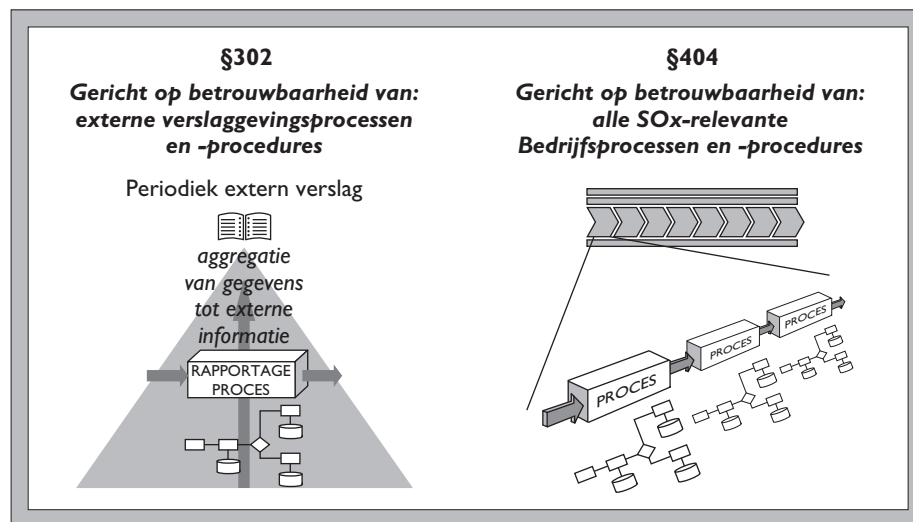
Als we de oorspronkelijke tekst² van de paragrafen 302 en 404 van de SOx Act lezen, kunnen we concluderen dat deze paragrafen zich slechts op één risicocategorie richten en dat is het risico dat er onjuistheden in de verslaggeving aan externe belanghebbenden voorkomen. Tevens stelt de SOx Act dat er twee manieren zijn om dit risico te minimaliseren:

- via goed werkende rapportagecontrols en -procedures (§302) en
- via een goed werkend stelsel van interne controlemaatregelen (§404)

SOx §302 lid 5 sub B stelt bovendien dat over alle geconstateerde fraude – materieel en immaterieel –, moet worden gerapporteerd. Er wordt echter geen definitie van het begrip 'fraude' gegeven. Derhalve wordt in paragraaf 2.3.1 nader op dit begrip ingegaan.

2.3.1 Fraude

In §302 wordt niet expliciet aangegeven dat fraude moet worden voorkomen. Het enige



Figuur 2 SOx §302 versus §404

dat wordt gesteld is dat alle ontdekte fraude moet worden gemeld. Als de SOx tekst letterlijk wordt geïnterpreteerd zou dit betekenen dat men niet verplicht is op actieve wijze fraude te voorkomen en op te sporen (anders dan met behulp van de normale AO/IC-maatregelen), maar dat men uitsluitend verplicht is fraude te melden als men deze toevallig op het spoor komt.

In dit artikel wordt ervan uitgegaan dat alle materiële fraude actief moet worden voorkomen, opgespoord, bestreden en gemeld, maar dat immateriële fraude slechts moet worden gemeld als deze (toevallig) wordt geconstateerd. Wat dit punt betreft wordt geadviseerd tijdens de projectplanning de actuele aanvullende regelgeving op de SOx Act te raadplegen.

Voor een definitie van fraude wordt teruggegrepen op Merriam-Webster's Dictionary of Law:

'Any act, expression, omission, or conceal-

ment calculated to deceive another to his or her disadvantage, specifically, a misrepresentation or concealment with reference to some fact material to a transaction that is made with knowledge of its falsity or in reckless disregard of its truth or falsity and with the intent to deceive another and that is reasonably relied on by other who is injured thereby' (1996, in Viton, 2002).

Vrij vertaald is er fraude in het spel als er kan worden gesproken van: bewuste misleiding, gekoppeld aan schade aan de andere partij die in redelijkheid had kunnen vertrouwen op de juistheid van de gepresenteerde informatie.

Er zijn drie hoofdvormen van fraude: managementfraude, transactiefraude en corruptie (Viton, 2002). Deze drie hoofdvormen kennen diverse subcategorieën. Er wordt in Bijlage 1 een overzicht van deze fraudeclassificatie gegeven, omdat: a) blijkt dat fraude een complex samengesteld begrip is, b) omdat een heldere afbakening van het begrip

van belang is voor de scope-afbakening van het project, c) omdat het een belangrijk aandachtspunt vormt bij het ontwerp van IC-maatregelen en d) omdat de SOx Act zich niet helder uitspreekt over de definitie van 'fraude'.

2.3.2 Toevoegingen aan de oorspronkelijke SOx Act 2002

In een toelichting op §302³ van de SOx Act heeft de Amerikaans beurswaakhond SEC aangegeven dat het in tegenstelling tot wat de letterlijke tekst stelt, het a) ook om niet-financiële materiële externe informatieverstrekking gaat en b) dat het naast de jaarlijkse en kwartaalrapportages ook om overige tussentijdse rapportages gaat (Renes, 2003). Dit vormt dus een uitbreiding ten opzichte van de scope zoals deze is omschreven in de oorspronkelijke tekst van §302.

2.4 AO/IC dekt slechts risico's betreffende §302 en §404 af

In dit artikel wordt er conform de assumpties in de SOx Act van uitgegaan dat een goed AO/IC-bouwwerk maximale garanties geeft op een juiste weergave van bedrijfsinformatie, zoals wordt nagestreefd door §302 en §404. Een goed AO/IC bouwwerk bestaat naast een goede *opzet* (ontwerp) uit een goede *werking* (functioneren in de praktijk ná implementatie). De SOx-auditor zal aan het eind van het project beoordelen of het AO/IC-bouwwerk goed genoeg werkt om de SOx-risico's zoals genoemd in de paragrafen 302 en 404 af te dekken en daarmee de onderneming op dit gebied al dan niet als SOx-compliant te kwalificeren.

AO/IC is procedureel van aard; het is 'slechts' gericht op de goede werking van

procedures. Naast AO/IC-maatregelen zijn er aanvullende, andersoortige maatregelen noodzakelijk om de risico's zoals weergegeven in de overige hoofdstukken en paragrafen van de SOx Act af te dekken. Deze risico's en maatregelen vallen echter buiten de scope van dit artikel. Hierbij valt onder andere te denken aan de volgende soorten maatregelen, waarvoor separate projecten zullen moeten worden opgezet:

- een moreel-ethisch normen- en waardenkader door onder andere het instellen van een gedragscode;
- beschermingsprogramma voor klokkenluiders;
- beloningsbeleid/meldpunt voor mensen die zwakke plekken in de organisatie/AO/IC rapporteren of verbeteringsvoorstellen doen;
- verhoging van de opsporingskans van fouten en fraude door actieve review/auditteams;
- screening van sollicitanten;
- een (anonieme) meldingsprocedure/-loket voor fraude;
- een helder sanctioneringsbeleid ten aanzien van criminaliteit van binnenuit.

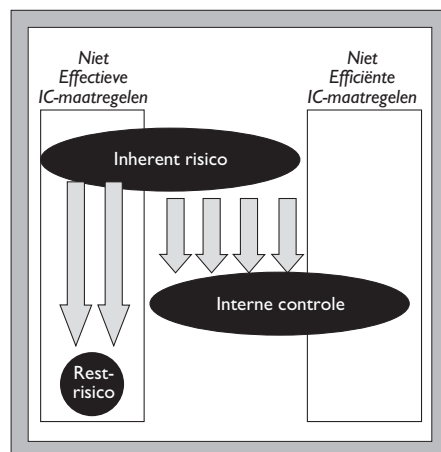
2.5 Aandachtspunt topmanagement

Specifiek aan de top van de onderneming is het SOx-risico en de schade in geval van fraude of onjuiste weergave van de cijfers erg groot. In nagenoeg alle gevallen van misleiding van externe belanghebbenden lag de oorzaak bij de top van de organisatie. Bij ieder soort maatregelen zal er dan ook extra aandacht aan de maatregelen rond de top van de organisatie moeten worden besteed. De praktijk leert dat het hier juist vaak aan schort. De onderkant van de organisatie

wordt afgedicht met IC-maatregelen, terwijl de top nagenoeg ongecontroleerd haar gang kan gaan.

2.6 Additionele maatregelen ter afdekking van restrisico

In de theorie van de AO/IC spreekt men van inherente risico's³, als men het heeft over risico's die van nature verbonden zijn aan een bepaalde bedrijfsactiviteit. Om deze risico's zoveel mogelijk te neutraliseren neemt men interne controlemaatregelen.



Figuur 3 Efficiëntie en effectiviteit van IC-maatregelen
(Bron: Atos KPMG Consulting/VU)

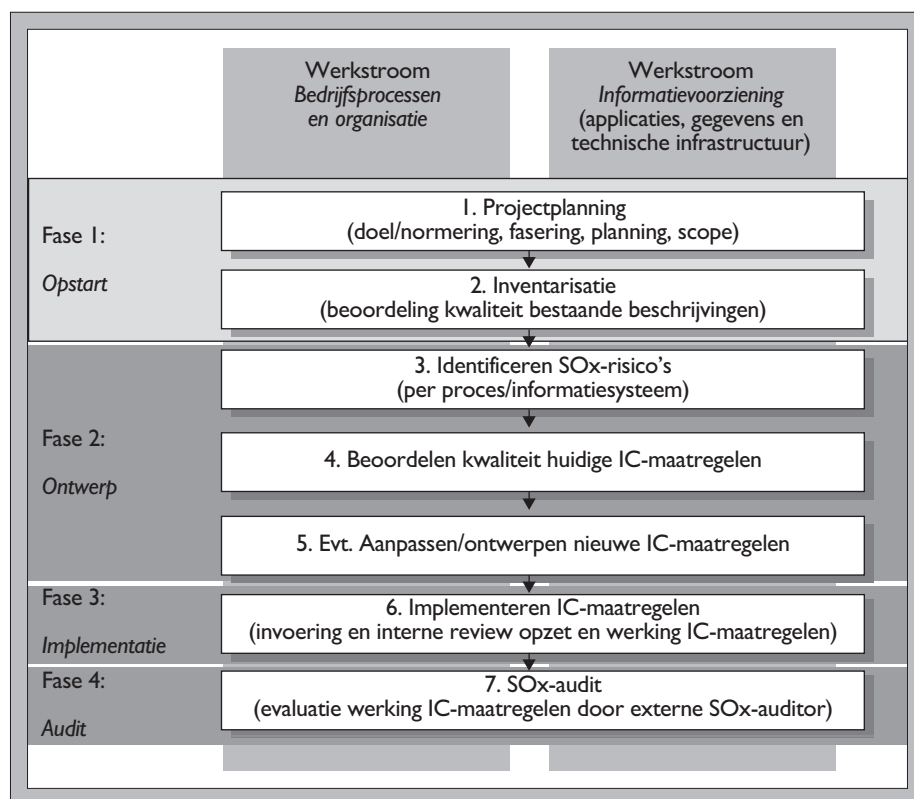
De risico's die overblijven na het instellen van de interne controlemaatregelen, noemt men 'restrisico'. Restrisico's zijn niet of niet tegen aanvaardbare kosten en inspanning af te dekken met IC-maatregelen, maar kunnen wel op andere wijze, bijvoorbeeld door middel van risico-overdracht (verzekering), worden geneutraliseerd. Hierbij valt bijvoorbeeld te denken aan een aansprakelijkheidsverzekering of fraudeverzekering. Vervolgens blijven er waarschijnlijk nog enkele risico's over

die men niet verder wil of kan afdekken; deze draagt men zelf.

3 Randvoorwaarden voor succes

Een SOx-project kan globaal in zeven stappen worden opgedeeld, zoals in figuur 4 weergegeven. In de figuur zijn daarnaast de twee duidelijk gescheiden werkstromen weergegeven: de eerste heeft betrekking op het SOx-compliant maken van de bedrijfsprocessen en niet-geautomatiseerde procedures, de tweede heeft betrekking op de geautomatiseerde gegevensverwerking. Het valt niet binnen de context van dit artikel om alle stappen en projectactiviteiten uitgebreid te beschrijven. De stappen 3 t/m 7 vallen binnen de vakgebieden AO/IC en EDP-auditing waarvoor wordt verwezen naar de bestaande literatuur op dit gebied. In dit artikel gaat het zoals gezegd om de opstartfase van het project; alleen de stappen 1 Projectplanning en 2 Inventarisatie zijn hier van belang. Dit zijn de stappen die garant moeten staan voor een succesvolle projectopzet en daarmee de basis vormen voor een succesvolle uitvoering van het project. Stap 1 Projectplanning richt zich op een goed projectplan, terwijl stap 2 Inventarisatie zich richt op de beoordeling van de kwaliteit van de bestaande beschrijvingen van bedrijfsprocessen, organisatie, gegevens, informatiesystemen en technische infrastructuur.

Voor een SOx-project gelden uiteraard alle algemene randvoorwaarden voor succes die voor ieder project gelden, zoals: helder afgebakende projectopdracht, een goed projectplan, een gedegen projectorganisatie, projectmanagers met een duidelijk mandaat, beschikbaarheid van documentatie en



Figuur 4 Globale projectstappen in een SOx-project

materiedeskundigen, resources die vrij zijn gemaakt voor het project, goed werkende projectprocedures en goede projectcommunicatie. Daarnaast kent een SOx-project een aantal specifieke randvoorwaarden die in dit hoofdstuk worden behandeld.

3.1 Randvoorwaarde nr. 1: heldere scope-afbakening

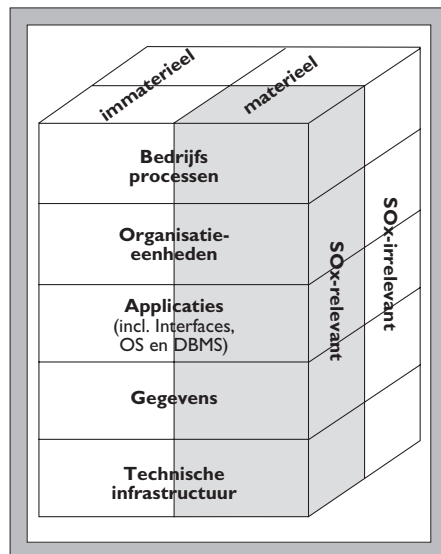
Een heldere scope-afbakening is cruciaal voor ieder project, maar in het geval van een SOx-project is deze gecompliceerder dan doorgaans het geval is. De scope van het project en van de verschillende aspecten/deelprojecten dient scherp afgebakend te zijn. Alle architectuurlagen (bedrijfsprocessen⁴,

organisatie-eenheden, applicaties⁵, gegevens en technische ICT-componenten) vallen voorzover ze 'SOx-relevant' en 'materieel' zijn, binnen de scope van een dergelijk project. Voor fraude geldt dat deze per definitie binnen de scope valt; ongeacht of deze materieel of immaterieel is.

De SOx Act doet op hoofdlijnen een uitspraak over wat SOx-relevant is, maar legt geen criteria aan voor materialiteit. In de volgende paragrafen zal nader worden ingegaan op de betekenis van deze beide begrippen.

3.1.1 Wat zijn SOx-relevante risico's?

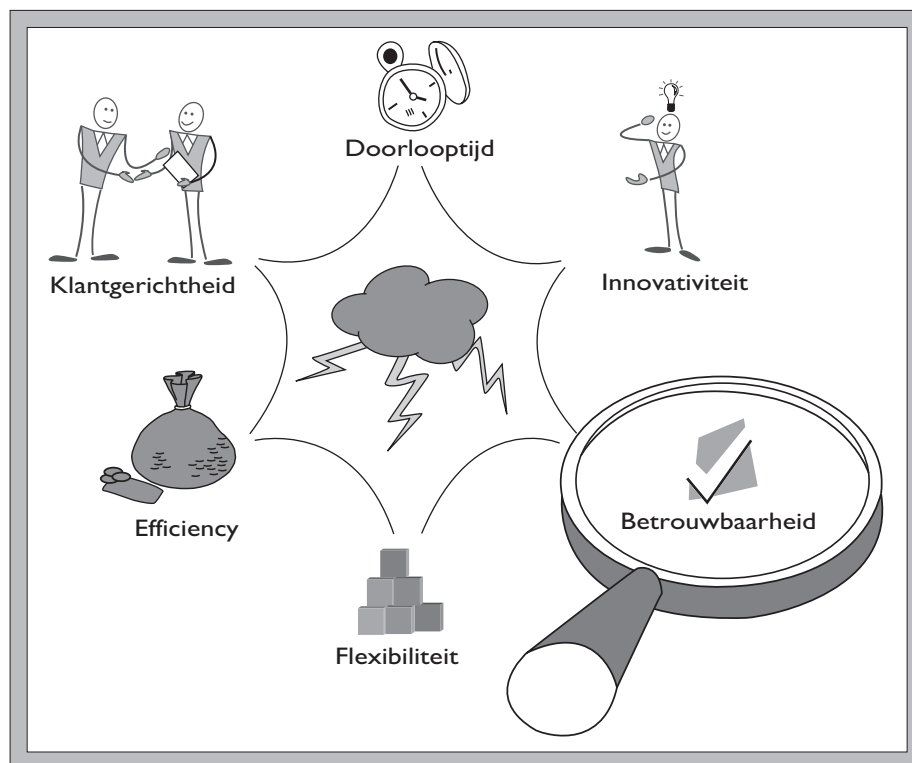
Bij het uitvoeren van bedrijfsactiviteiten treden er diverse soorten risico's op. Binnen een



Figuur 5 Scope SOx-project

SOx-project zijn we slechts geïnteresseerd in enkele risico's; dit zijn risico's die te maken hebben met de kritieke succesfactor 'betrouwbaarheid' van procedures en informatie. Bij SOx⁶-relevante risico's gaat het om risico's die externe partijen (aandeelhouders en overige belanghebbenden) lopen om gedupeerd te worden door onjuiste informatievoorziening (financiële én niet-financiële informatie) of fraude.

In het kader van SOx zijn we niet geïnteresseerd in bedrijfseconomische risico's, zoals inefficiënte bedrijfsprocessen, klantontevredenheid ten gevolge van inferieure service en producten, te hoge doorlooptijden en starheid in procesinnovatie. In figuur 6 is deze focus aangegeven.



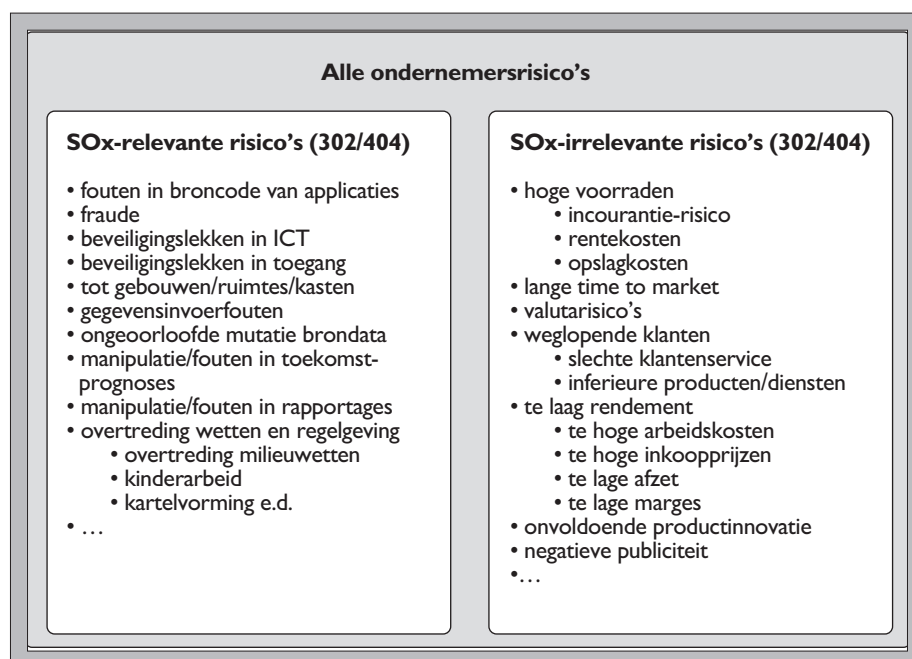
Figuur 6 SOx-focus op 'betrouwbaarheid' (Bron: KPMG)

Het feit dat er bij SOx alleen naar betrouwbaarheid wordt gekeken impliceert dat dit op gespannen voet kan komen te staan met de overige kritieke succesfactoren; als men bijvoorbeeld te veel interne controlemaatregelen instelt, kan dit ten laste gaan van de doorlooptijd van een bedrijfsproces. Binnen een SOx-project dienen derhalve ook de overige risico's en kritieke succesfactoren niet geheel uit het oog te worden verloren; men dient de minimaal noodzakelijke interne controlemaatregelen in te stellen om de betrouwbaarheid te waarborgen en daarbij zo weinig mogelijk hinder voor het behalen van de overige kritieke succesfactoren op te leveren!

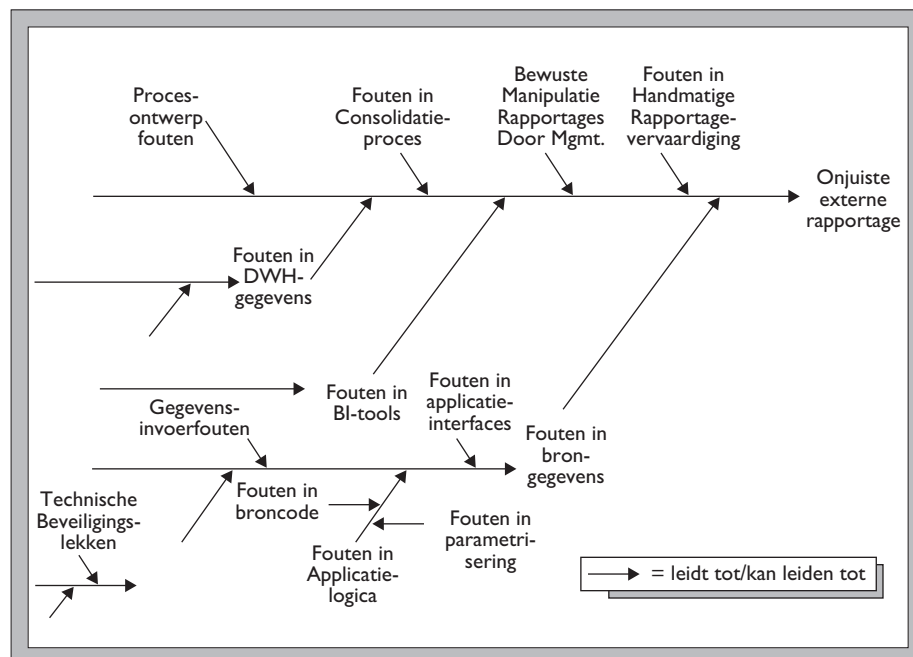
Onderstaand is ter illustratie een – niet-uitputtend – overzicht van ondernemersrisico's opgenomen, opgesplitst naar respectievelijk SOx-relevante risico's en SOx-irrelevante risico's.

In figuur 7 staan SOx-relevante risicosoorten opgesomd in de vorm van een lijst. Aangezien in de praktijk het ene risico wordt veroorzaakt door een ander risico, is er sprake van een hiërarchisch causaal verband. SOx-relevante risicosoorten kunnen worden geïdentificeerd met behulp van causale analyse. Hierbij worden oorzaak-gevolgrelaties tussen gebeurtenissen in kaart gebracht. Dit kan grafisch worden weergegeven met een boomdiagram of zoals in figuur 8 met een zogenaamd Ishikawa- of visgraatdiagram. Het diagram toont de causale relaties tussen toestanden/gebeurtenissen die uiteindelijk leiden tot externe rapportages die de bedrijfswerkelijkheid niet weerspiegelen.

Deze causale analyse kan behulpzaam zijn bij het identificeren van de SOx-relevante bedrijfsprocessen, organisatie-eenheden, applicaties, gegevens en technische componenten.



Figuur 7 SOx-relevante risicosoorten versus SOx-irrelevante risicosoorten



Figuur 8 (Partieel) Ishikawa-diagram met causale relaties SOx-relevante risicosoorten

3.1.2 Het materialiteitsbegrip

Het begrip ‘materialiteit’ is een aanduiding voor de mate waarin informatie-items⁷ van wezenlijke invloed zijn op de balans en resultatenrekening. Binnen een SOx-project kan het materialiteitsgehalte van een bedrijfsproces worden gebruikt om de scope-afbakening, projectfasering en prioriteitsvolgorde in de werkzaamheden aan te brengen.

Over de exacte definitie van het begrip ‘materialiteit’ bestaat nog geen overeenstemming. In de Richtlijnen voor de accountantscontrole 320 (RAC 320) staat de volgende definitie:

‘Informatie is materieel indien het weglaten of het onjuist weergeven daarvan de economische beslissingen die gebruikers op basis van de jaarrekening nemen, zou kunnen beïnvloeden’ (in Koopmans, 2003).

De Raad voor de Jaarverslaggeving waagt zich in tegenstelling tot veel andere accountancy experts tot een kwantitatieve uitspraak. Deze stelt in zijn richtlijnen (RJ 130 215) dat een resultaatpost materieel is als deze: ‘groter is dan 5% van de toegevoegde waarde of groter is dan 10% van het totaal van de rubriek waartoe de post behoort’ (in Koopmans, 2003). Een voorbeeld van een ander criterium wordt genoemd door Gist en Shastri (2003). Zij hebben het over ‘A percentage of some bases can be used as a rule of thumb. For example, the auditor may use 5% of income from continuing operations or 1% of revenue or assets.’

In het kader van dit artikel is een exacte, wetenschappelijk verantwoorde definitie en materialiteitsgrens niet zozeer van belang. Het gaat erom dat het begrip ‘materialiteit’ kan worden gebruikt om een besluit te nemen 1)

welke zaken al dan niet binnen de scope van het SOx-project vallen en 2) indien zaken binnen de scope vallen kan met behulp van de materialiteitsgrens een fasering of prioriteitsvolgorde worden aangebracht in de projectactiviteiten, zodat bijvoorbeeld processen met een materialiteit hoger dan x in fase 1 SOx-compliant worden gemaakt en de overige processen in fase 2.

Binnen een SOx-project is het belangrijk dat er een operationele definitie van het begrip 'materialiteit' wordt opgesteld, alsmede een operationele grenswaarde op basis waarvan kan worden bepaald of een bedrijfsproces al dan niet binnen de scope van het project valt en zo ja, welke prioriteit er binnen het project wordt gegeven aan het SOx-compliant maken van het desbetreffende bedrijfsproces. De definitie en grenswaarde dienen echter wel binnen algemeen aanvaardbare accountancynormen te vallen. De hiervoor genoemde percentages kunnen hierbij als globale leidraad worden gehanteerd. Hierbij moet opgemerkt worden dat een materialiteitsdrempel brancheafhankelijk is. Zo is onjuiste polisadministratie bij een verzekeraar van geheel andere materiële orde dan onjuiste orderregistratie in een handelsbedrijf (Hartman, 1988). Een en ander kan in de praktijk het beste in overleg met de SOx-auditor worden vastgesteld.

Voor klantordergestuurde bedrijfsprocessen is de materialiteit eenvoudiger vast te stellen dan voor niet-klantordergestuurde processen. Klantordergestuurde processen kunnen op omzetbijdrage worden geprioriteerd. Bijvoorbeeld: als de product-procescombinatie van productsoort $x >$ dan y % van de totale omzet dan is deze materieel.

Voor niet-klantordergestuurde processen is het een stuk moeilijker om de materialiteit vast te stellen. Hier zal de materialiteit bijvoorbeeld op basis van maximaal aan te richten SOx-relevante schade moeten worden vastgesteld.

Het vaststellen van de materialiteitsgrens blijft te allen tijde een arbitraire aangelegenheid. Hierdoor is het aan te bevelen om de vaststelling in samenspraak met de accountant te doen en alle overwegingen/normen die een rol hebben gespeeld bij het bepalen of iets al dan niet materieel is transparant te maken.

3.1.3 Scope-afbakening ten aanzien van bedrijfsprocessen en organisatie

Alle bedrijfsprocessen die leiden tot feiten in de externe verslaggeving zijn SOx-relevant. Bij de vaststelling van SOx-relevantie vormt logisch redeneren de basis; inkopen leiden bijvoorbeeld tot verplichtingen (schulden) die op de balans terechtkomen. Het inkoopproces is derhalve SOx-relevant. Voorts kan een overzicht van welke processen welke brongegevens raken (processen-objectenmatrix) behulpzaam zijn bij het vaststellen van SOx-relevantie. Processen die SOx-relevante gegevensobjecten raken zijn immers zelf ook SOx-relevant. Van de SOx-relevante processen zal vervolgens beoordeeld moeten worden of ze materieel zijn.

Alle rapporterende organisatie-eenheden zijn SOx-relevant. Verder vallen alleen de materiële organisatie-eenheden binnen de scope van SOx. Hiervoor kan wederom de vastgestelde materialiteitsgrens worden gehanteerd.

3.1.4 Scope-afbakening ten aanzien van applicaties

Onder applicaties valt alle software die invloed kan hebben op de kwaliteit van externe informatieverstrekking; dit zijn in beginsel:

- a gegevensverwerkende of administratieve toepassingen;
- b besturingssystemen;
- c middleware; en
- d database managementsystemen.

Al deze softwarecomponenten kunnen in geval van onvolkomen werking van negatieve invloed zijn op de kwaliteit van (bron)gegevens en daarmee direct of indirect van negatieve invloed zijn op externe rapportages.

Ad a kan worden opgemerkt dat uitsluitend gegevensverwerkende toepassingen die SOx-relevante gegevens verwerken binnen de scope vallen. Om hiervan een goed beeld te krijgen is het nodig inzicht te hebben in welke applicaties welke gegevensobjecten beheren (objecten-applicatiematrix). Voorts kan worden opgemerkt dat sommige soorten gegevensverwerkende toepassingen grotere risico's opleveren dan andere; hierbij valt bijvoorbeeld te denken aan Extraction, Transformation and Loading tools (ETL), Data Warehouses (DWH) en Business Intelligence tools (BI), aangezien deze ondersteunend zijn voor de belangrijkste SOx-processen; de rapportageprocessen.

3.1.6 Scope-afbakening ten aanzien van gegevens

Niet alle bedrijfsgegevens zijn SOx-relevant. Voorbeelden van gegevenssoorten die SOx-relevant zijn, omdat deze invloed hebben op de externe informatieverstrekking, zijn:

- transactiegegevens (inkooporders, verkooporders);

- activagegevens (onroerend goed, inventaris, configuratie-items⁸);
- verplichtingen en schulden en
- loggingbestanden van systeemtransacties (onder andere van informatiesysteemtoegang en gebouwtoegang). Hiermee kunnen pogingen tot ongeautoriseerd handelen of fraude worden opgespoord.

Voorbeelden van gegevenssoorten die niet SOx-relevant zijn, zijn:

- IT-incidenten;
- klantgegevens;
- leveranciergegevens.

Er kunnen geen algemeen geldende uitspraken worden gedaan welke gegevens al dan niet SOx-relevant zijn. Met behulp van een corporate gegevensmodel (of objectmodel) dient te worden vastgesteld welke gegevens in een specifieke situatie SOx-relevant zijn.

3.1.6 Scope-afbakening ten aanzien van technische infrastructuur

Alle technische infrastructuurcomponenten die van invloed kunnen zijn op de kwaliteit van de externe informatieverstrekking of fraude-opsporing zijn SOx-relevant. Dit zijn onder andere alle opslag- en verwerkingsmedia waarop SOx-relevante gegevens worden beheerd, evenals de transportmedia waarover deze gegevens worden verstuurd. Ook alle overige technische infrastructuurcomponenten die in netwerkcontact staan met de hiervoor genoemde componenten en van invloed kunnen zijn op de toegang tot gegevens of de gegevenskwaliteit, zijn SOx-relevant.

3.2 Randvoorwaarde nr. 2: concernbrede architectuurstandaarden

Een architectuur is een richtinggevend kader bij de ontwikkeling van onder andere bedrijfsprocessen, organisatiestructuren, informatiesystemen, gegevensverzamelingen en technische infrastructuren, met als doel een integrale ontwikkeling conform een gezamenlijke visie. Voorwaarde voor succes is dat de architectuur en de daarin opgenomen standaarden concernbreed worden gebruikt. Het is dus niet een vrijblijvend hulpmiddel, maar een verplichte ‘kapstok’.

De architectuur dient in het kader van SOx als gemeenschappelijk referentiekader, hetgeen leidt tot eenvormigheid en eenduidigheid bij het analyseren van risico’s en ontwerpen van IC-maatregelen. Twee onderdelen van de architectuur zijn van eminent belang bij de opzet van een SOx-project: de procesarchitectuur en de gegevensarchitectuur.

3.2.1 Procesarchitectuur

Een procesarchitectuur bestaat uit een gezamenlijk referentiekader voor het ontwerp van bedrijfsprocessen. Belangrijkste elementen van een procesarchitectuur die randvoorwaardelijk zijn voor een succesvol SOx-project:

- een verplichte methode voor procesontwerp, inclusief een standaardformat (sjabloon) voor procesbeschrijvingen;
- een corporate processtructuur (process map) waarin de processorten hiërarchisch zijn ondergebracht met een heldere indeling in een vast aantal aggregatieniveaus (detailniveaus waarop bedrijfsprocessen beschreven zijn) en per proces een definitie en een helder start- en eindpunt. Deze process map vormt de verplichte ‘kapstok’

waaraan alle bedrijfsprocessen moeten worden opgehangen. Dit realiseert eenheid in processen tussen de diverse organisatie-eenheden. In figuur 9 wordt ter illustratie een voorbeeld getoond van een deel van een process map;

- eenduidige nummerings- en naamgevingsconventie voor bedrijfsprocessen;
- een duidelijk beheerproces en heldere rolverdeling in het ontwikkelen en beheren van bedrijfsprocessen.

Als deze onderdelen van de procesarchitectuur ontbreken of niet goed uitgewerkt zijn voor aanvang van een SOx-project, leidt dit onherroepelijk tot een verhoogd risico op overschrijding van de factoren tijd, geld en/of kwaliteit!

Belangrijkste gevolgen van een gebrekkige of ontbrekende procesarchitectuur zijn:

- inzicht in procesverloop is niet goed/fragmentarisch, door ontbreken integraal inzicht in procesketens;
- procesrisico’s en IC-maatregelen zijn niet goed in kaart te brengen;
- de huidige processen zijn alle op verschillende wijze beschreven, waardoor interpretatieproblemen ontstaan en het ontwikkelen van IC-maatregelen bemoeilijkt wordt;
- procesbeschrijvingen zijn mogelijk (ongemerkt) niet meer actueel, waardoor de werkelijke processen afwijken van de beschreven processen. Men dient nu eerst de werkelijke processen in kaart te brengen (en dat is een project op zich) of men dreigt onzinnige IC-maatregelen te ontwikkelen op basis van de niet-actuele procesbeschrijvingen;
- men brengt IC-maatregelen op het verkeerde hiërarchisch procesniveau aan;

niveau 1 proces	niveau 2 proces	niveau 3 proces	procesdefinitie	start	eind
I. Verkoop					
	I.1 Beheren prospects				
		I.1.1 Vaststellen verkoopcampagne	besluitvorming voor uitvoering van een voorstel Voor een verkoopcampagne	voorstel verkoopcampagne	uitvoeringsbesluit
		I.1.2 Vaststellen communicatieplan			
		I.1.3 Beheren klantrelaties			
		I.1.4 Uitvoeren Verkoopcampagnes			
	I.2 Uitbrengen offerte				
		I.2.1 Vormen BID team			
		I.2.2 Reageren op RFI			
		I.2.3 Uitvoeren site survey			
		I.2.4 Uitvoeren consultancy/engineering			
		I.2.5 Opstellen offerte			
		I.2.6 Vaststellen offerte			
	I.3 Order verwerken				
		I.3.1 Ontvangen order			
		I.3.2 Kredietwaardigheidsonderzoek uitvoeren			
		I.3.3 Uitvoeren Clean Order Check			
		I.3.4 Order accepteren			

Figuur 9 Deel van een process map

- risico's tussen gelijksoortige processen van verschillende rapporterende organisatie-eenheden zijn niet te vergelijken;
- projectinterne communicatiestoornissen inzake procesgrenzen, nummering en naamgeving, met als resultaat fouten en projectoverschrijdingen op de aspecten tijd, geld en/of kwaliteit.

Kortom: een goede procesarchitectuur is cruciaal voor het welslagen van een SOx-project!

3.2.2 Gegevensarchitectuur

Een gegevensarchitectuur bestaat uit principes (regels), standaarden en globale ontwerpen (gegevensmodellen) voor de gegevenshouding. Het vormt het kader bij het ontwerp van detail-gegevensstructuren. Bij projectaanvang dient minimaal een corporate objectmodel beschikbaar te zijn, dat bestaat uit:

- een grafisch overzicht van objecten en onderlinge relaties;
- metagegevens over objecten (definities, toelichting).

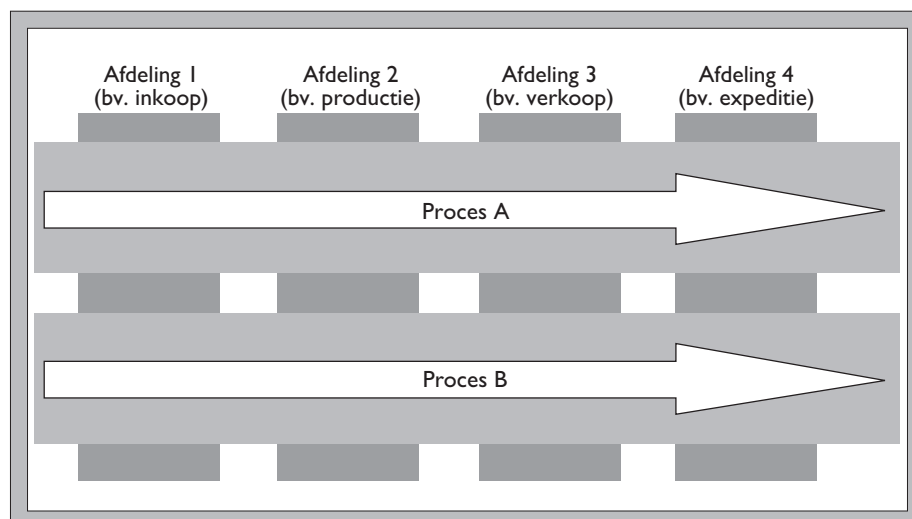
3.3 Randvoorwaarde nr. 3: goed inzicht in bestaande architectuur

Bij aanvang van het project is het cruciaal om een goed inzicht in de bestaande architectuur (bedrijfsprocessen, organisatiestructuur, applicaties, gegevensstructuur en technische infrastructuur) te hebben. Onvoldoende inzicht door bijvoorbeeld onvolledige, onjuiste en ontbrekende procesbeschrijvingen en handleidingen van informatiesystemen leiden onherroepelijk tot hogere kosten, doorlooptijd of afbreuk aan kwaliteit.

3.3.1 Integraal inzicht in de procesketen

In het kader van SOx en de AO/IC-maatregelen die nodig zijn om de SOx-risico's te reduceren, is het cruciaal om inzicht te hebben in de gehele procesketen, aangezien SOx-risico's bijna altijd proces- en afdelingsoverschrijdend zijn.

In veel organisaties bestaat een dergelijk inzicht niet. Processen zijn historisch gezien



Figuur 10 Integraal inzicht in de procesketen (Bron: KPMG)

veelal ontworpen en beschreven op afdelingsniveau. Interfaces tussen afdelingen zijn niet of niet helder beschreven. Voorzover het procesverloop tussen afdelingen wel te herleiden valt, moet vaak worden geconstateerd dat terminologie geheel verschilt, met als gevolg een grote kans op interpretatiefouten, met alle consequenties van dien.

Als de procesketen bij aanvang van het SOx-project niet helder is, dient er eerst een project te worden uitgevoerd om deze alsnog goed in beeld te brengen! Per bedrijfsproces dienen alle processtappen over de diverse afdelingen in kaart te worden gebracht om een totaalinzicht in het proces en de daaraan verbonden SOx-risico's te verkrijgen. In figuur 11 is dit integrale inzicht weergegeven in een processtappenoverzicht.

3.3.2 Correcte schatting procescomplexiteit en werkbelasting

Een SOx-project is zeer complex, alleen al vanwege de concernbrede scope en daarnaast ook vanwege de diepgang. Een goede plan-

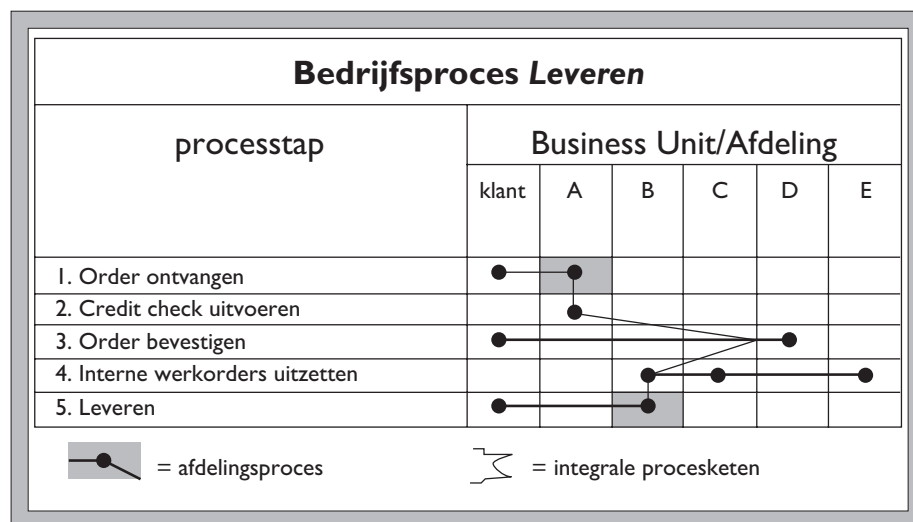
ning en werkschatting is daarom cruciaal. De belangrijkste aandachtspunten ten behoeve van een goede inschatting van de complexiteit en werkbelasting, worden in deze paragraaf behandeld.

3.3.2.1 Bepaling procescomplexiteit

Complexiteit in de zin van 'hoeveelheid processen' ontstaat zodra processen op verschillende plaatsen verschillend verlopen of als processen per product(soort) verschillen. Er is dan sprake van een 1:N-explosie. Als er bijvoorbeeld 5 business units zijn, kan men geneigd zijn te denken dat er in totaal maximaal 5 verschillende leveringsprocessen zijn. Maar omdat het leveringsproces per product-/dienstsoort kan verschillen, kan dit in de praktijk een veelvoud zijn. Per processoot zal dus gekeken moeten worden hoeveel verschillende instanties ervan voorkomen.

3.3.2.2 Werkbelasting bij besturingsprocessen

Besturingsprocessen zijn een specifiek soort bedrijfsprocessen, die in het kader van SOx



Figuur 11 Integrale procesketen met behulp van processtappenoverzicht

om extra aandacht vragen. Voor besturingsprocessen geldt namelijk dat ze pas 'SOx-compliant' kunnen zijn, als de door dit proces bestuurd processen dat ook zijn. In figuur 12 wordt het proces 'order bewaken' als voorbeeld gegeven.

Dit proces is het besturend proces voor vijf bedrijfsprocessen, die alle SOx-compliant dienen te zijn, alvorens het proces 'order bewaken' zelf als SOx-compliant kan worden aangemerkt. Bij de werkverdeling in een project dient rekening te worden gehouden met de werklust die een besturingsproces met zich meebrengt; bij de werkverdeling kan men niet eenvoudigweg aantallen processen verdelen over resources en daarbij een besturingsproces even zwaar tellen als een gewoon bedrijfsproces.

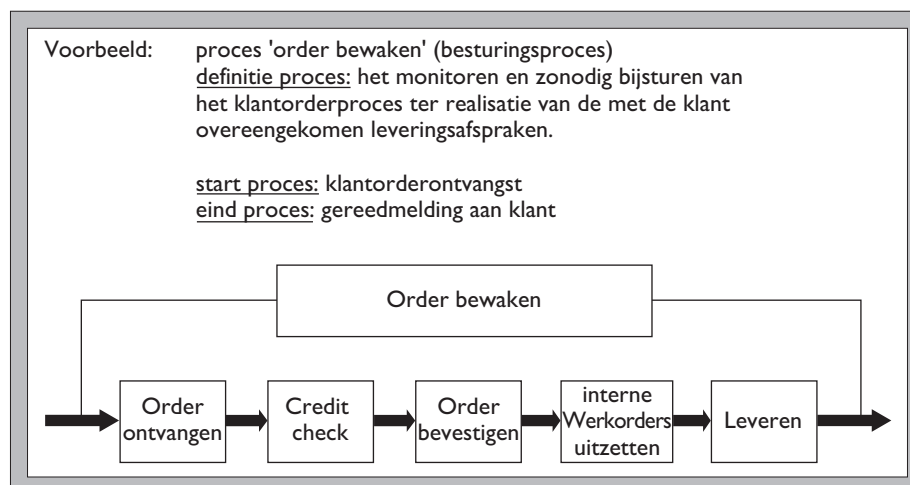
3.3.3 Inzicht in bestaande applicaties

Ten aanzien van de bestaande applicaties is het noodzakelijk om bij projectaanvang een goed inzicht te hebben in het gehele applicatielandschap: applicaties én applicatie-interfaces (grafisch applicatie-overzicht), inclusief

goede documentatie (technische en gebruikershandleidingen) van deze componenten. Belangrijk hierbij is een goede beschrijving van de geautomatiseerde invoercontroles. Ten slotte is inzicht gewenst in welke applicaties welke objecten beheren (objecten-applicatiematrix).

3.3.4 Inzicht in bestaande gegevensstructuren en gegevensverzamelingen

Bestaande gegevens dienen goed gedocumenteerd te zijn; metagegevens⁹ dienen te zijn ondergebracht in een centraal te benaderen data dictionary (gegevenswoordenboek). Bij metagegevens gaat het voornamelijk om gegevens over de betekenis (semantiek) en naamgeving (syntaxis) van entiteiten en attributen per informatiesysteem, alsmede een Entiteit Relatie Diagram. Als laatste is inzicht gewenst in welke processen welke gegevensobjecten raken (processen-objectenmatrix). Hoe minder informatie beschikbaar is, des te meer zal er een beroep op data administrators en database administrators moeten worden gedaan tijdens het project.



Figuur 12 Complexiteit bij besturingsprocessen

3.3.5 Inzicht in de bestaande technische infrastructuur

De technische infrastructuur (TI) is het fundament waarop gegevensopslag, transport en verwerking plaatsvinden. De TI kan van invloed zijn op de gegevenskwaliteit en kan dus ook van invloed zijn op externe rapportages. Het is derhalve van belang bij projectaanvang een goed inzicht te hebben in de TI. Hiervoor zijn minimaal de volgende overzichten van belang:

- overzicht netwerkachitectuur/-topologie (grafisch);
- overzicht configuratie.¹⁰

In deze paragraaf zijn de belangrijkste randvoorwaarden voor de opzet van een succesvol SOx-project behandeld. In bijlage 2 wordt naast deze drie randvoorwaarden een overzicht gegeven van alle overige aandachtspunten bij de opzet van een dergelijk project.

Bijlage I Fraudeclassificatie

Fraudecategorie	Omschrijving ¹¹
I. Management fraud a. Revenue measurement and recognition b. Provisions for uncertain future costs c. Asset valuation d. Related party transactions	Fraude door het (top)management Hieronder vallen diverse vormen van te hoge weergave van omzet Gebruik van posten 'voorzieningen' om pieken in resultaten af te vlakken Te hoge waardering van activa Transacties met derde partijen die ten onrechte buiten de boeken worden gehouden
2. Transaction fraud a. Billing schemes i. Shell company schemes ii. Pass through schemes iii. Pay-and-return schemes iv. Personal-purchase schemes b. Skimming c. Check tampering i. Forged maker	Fraude met transacties (door management/employees) Spookfacturen door employees die door het bedrijf worden betaald Oprichting fictief bedrijf door employee, dat spookfacturen stuurt aan werkgever Een door employee opgericht bedrijf levert en factureert goederen of diensten aan de werkgever Employee doet bewust dubbele betaling aan leverancier en verzoekt vervolgens om restitutie naar eigen rekening Employee bestelt goederen voor eigen gebruik Ontvreemden (deel van) van binnenkomende betalingen Fraude met betaalcheques Vervalsing van handtekening op blanco cheques

Bijlage I (zie vervolg)

<ul style="list-style-type: none"> ii. Forged endorsement iii. Altered payee iv. Altered payment amount <p>d. Payroll schemes</p> <ul style="list-style-type: none"> i. Ghost employees ii. Falsified hours/rates <p>iii. Commission schemes</p> <p>e. Non-cash misappropriations</p> <ul style="list-style-type: none"> i. Larceny ii. Asset requisition and transfer schemes iii. Purchasing and receiving schemes iv. False shipment schemes <p>f. Register disbursements</p>	<p>Onderschepping van reeds uitgevoerde betaalcheque</p> <p>Eigen naam employee</p> <p>Vervalsing door de employee van het bedrag op een voor hem bestemde cheque</p> <p>Fraude met salarisbetaling</p> <p>Salarisbetalingen aan niet-bestaande employee</p> <p>Declareren van niet-gewerkte uren of verhoging tarief</p> <p>Opvoeren van niet afgesloten verkooptransacties of verhoging verkoopcommissiepercentage</p> <p>Diefstal van activa (anders dan geld)</p> <p>Ordinaire diefstal van activa zonder enige vorm van verberging</p> <p>Employee is verantwoordelijk voor verplaatsing activum naar andere locatie en verduistert het tijdens het verplaatsingstraject</p> <p>Bij goederenontvangst worden goederen verduisterd en op ontvangstbon als 'ontbrekend' aangemerkt (goede factuur wordt aan afdeling debiteuren gestuurd, opdat leverancier volledig betaald krijgt)</p> <p>Opvoeren van niet-bestaande verkooptransactie en vervolgens de geleverde goederen ontvreemden</p> <p>Illegale kasonttrekkingen (vaak tegen vervalst betalingsbewijs)</p>
<p>3. Corruption</p> <ul style="list-style-type: none"> a. Bribery b. Kickbacks <p>c. Contract rigging</p> <p>d. Extortion</p> <p>e. Payment and receipt of illegal gratuities</p>	<p>Corruptie</p> <p>Omkoping</p> <p>Employee ontvangt van externe partij een vergoeding voor hulp van binnen bij fraude door externe partij (bijvoorbeeld bij contract rigging)</p> <p>Hulp van binnenuit door levering van inside informatie aan leverancier die contract wil afsluiten</p> <p>Afpersing/afzetterij</p> <p>Betaling en ontvangst van 'fooiën'</p>

(Bron: Viton, 2002)

Bijlage I

Bijlage 2 Checklist SOx

Deze checklist bevat een overzicht van randvoorwaarden en aandachtspunten bij de opzet van een project in het kader van de SOx-pa-

ragrafen 302/404. Het voldoen aan de punten in deze checklist maximaliseert de kans op een succesvolle projectuitvoering binnen tijd, geld en de vereiste kwaliteit.

PROJECTPLANNING
Helder beeld en definitie (SMART ¹²) wat onder 'SOx-relevant' wordt verstaan.
Operationele definitie van 'materialiteit' (SMART ¹⁰): een harde operationeel gedefinieerde grens welke processen in welke mate 'materieel' zijn.
Duidelijke auditnormen vooraf op basis waarvan later wordt vastgesteld of men SOx-compliant is.
Karakteristiek voor een SOx-project is de vaststaande deadline. Aangezien er ook aan de kwaliteit niet veel te tornen valt, blijft als enige stuurvariabele de factor geld (budget) over. Met extra geld kan worden bijgestuurd door extra mensen in te zetten. Op deze wijze kan het beoogde resultaat alsnog worden gerealiseerd in de geplande tijd tegen geplande kwaliteit. Houdt hiermee bij de aanvraag/besteding van het budget rekening; bouw een marge in.
Zorg voor een duidelijke interne goedkeuringsprocedure voor AO/IC-beschrijvingen (voordat deze door een externe accountant op SOx-compliance worden getoetst).
Beschouw het SOx-project als een ontwikkeltraject, in plaats van een routinetraject; het gaat immers in veel organisaties om grotendeels nieuwe materie. Dit betekent dat er grotere veiligheidsmarges moeten worden ingebouwd, mede omdat er weinig of geen standaarden zijn met betrekking tot schattingen van werkhoeveelheden/doorlooptijd e.d. Aan de tijdfactor valt weinig te verschuiven door de vaste deadline. Begin dus zo snel mogelijk; stel de start niet uit. Ga niet in zee met externe partijen die een dergelijk project op basis van een vaste prijs willen uitvoeren, als deze niet over een uitgebreide ervaring en referenties beschikken ten aanzien van AO/IC in het algemeen en SOx-projecten in het bijzonder.
Projectleden dienen allen kennis te hebben van: 1) ontwerp van bedrijfsprocessen, 2) AO/IC, 3) branche-/business kennis. Indien het onmogelijk blijkt om deze kennis per individu te verenigen, zorg dan op z'n minst dat deze kennis in ieder team aanwezig is. Zorg in ieder geval voor een korte introcursus voor projectbetrokkenen ter opvulling van kennishiaten op deze drie gebieden.
Voer geen proces(her)ontwerp uit tijdens ontwerp van AO/IC-maatregelen; als de kwaliteit van de procesbeschrijvingen onvoldoende is, breng dan eerst de processen helder in kaart, dan pas AO/IC-maatregelen ontwerpen/aanscherpen.

Bijlage 2 (zie vervolg)

Zet apart projecten/werkstromen op voor het in kaart brengen van de risico's en het ontwikkelen van IC-maatregelen voor: 1) bedrijfsprocessen en 2) informatievoorziening (applicaties, gegevens en technische infrastructuur).
Voor organisatie-eenheid overschrijdende processen/informatiesystemen: zet projectteams op per proces(keten) en dus niet per organisatie-eenheid. Neem het (top)management ook mee in de scope van het project; juist daar zijn de risico's het hoogste.
INVENTARISATIE
Bedrijfsprocessen
Duidelijk producten-processenoverzicht, inclusief de omzet per product ter bepaling van de hoeveelheid bedrijfsprocessen en ter vaststelling van de materialiteit ten behoeve van activiteitenprioritering (dient reeds voor aanvang project te bestaan).
Een inschatting van de complexiteit van processen (bijvoorbeeld een indeling in 3 categorieën: eenvoudig, gemiddeld en complex).
Verantwoordelijke functionarissen (proceseigenaar) per proces (dient reeds voor aanvang project bekend te zijn). Proceseigenaren worden ervoor verantwoordelijk gesteld dat hun proces uiteindelijk SOx-compliant wordt.
Verplicht het gebruik van de corporate process map en sta gedurende het project onder geen beding wijzigingen in de corporate process map toe.
Zorg voor een duidelijke beschrijving van de verschillende niveaus van procesbeschrijvingen (hiërarchisch, globaal proces, detail proces e.d.), opdat alle betrokkenen van ieder proces eenduidig het niveau kunnen vaststellen.
Compleet beeld van de hoeveelheid bedrijfsprocessen (dient reeds voor aanvang project bekend te zijn).
Een goede procesarchitectuur; die verplicht is en door alle organisatie-eenheden als uitgangspunt wordt gebruikt (dient reeds voor aanvang project te bestaan).
Zorg ervoor dat procesbeschrijvingen kwalitatief goed zijn inclusief beschrijvingen van procesinterfaces over procesgrenzen en organisatie-eenheden heen. Cruciaal zijn heldere procesdefinities in procesbeschrijvingen en process map, inclusief exacte start- en eindpunten van het proces en interfaces met andere processen (dient reeds voor aanvang project bekend te zijn).
Bestaande processen en procesbeschrijvingen dienen te zijn ontworpen conform de regels uit de procesarchitectuur.
Er dient een integraal inzicht in de procesketens te bestaan.

Bijlage 2 (zie vervolg)

Inzicht in KSF'en en KPI's per bedrijfsproces; hiermee heeft men immers rekening te houden bij het ontwerpen van IC-maatregelen. Als een proces bijvoorbeeld kritisch is t.a.v. doorlooptijd, dan kan het immers zo zijn dat relatief zware IC-maatregelen hiermee op gespannen voet komen te staan.
Huidige proces- en AO/IC-beschrijvingen dienen beschikbaar en toegankelijk te zijn (dient reeds voor aanvang van het project het geval te zijn).
Huidige proces- en AO/IC-beschrijvingen dienen van heldere metagegevens voorzien te zijn (documentnaam, auteur, versie, datum e.d.) om helderheid over de documentstatus te hebben.
Verifieer dat werkinstructies per bedrijfsproces beschreven zijn. In de praktijk komt het veelal voor dat werkinstructies per informatiesysteem beschreven zijn, omdat ze uitsluitend in gebruikershandleidingen staan. Het levert nagenoeg ondoenlijk puzzelwerk op om dergelijke werkinstructies terug te herleiden naar het proces waar ze bij horen.
Overzicht welke afdelingen welke processen/processtappen uitvoeren (processtappen-overzicht).
Organisatie
Beschikbaarheid van organogrammen.
Beschikbaarheid van procuratietabellen (wie mag wat tot welk maximumbedrag in welk proces).
Applicaties
Een grafisch applicatie-overzicht, incl. beschrijvingen van applicatie-interfaces/data flows.
Goed gedocumenteerde applicaties (technische en gebruikershandleidingen). Als applicaties niet goed gedocumenteerd zijn zullen op z'n minst extra interviews met applicatiebeheerders nodig zijn.
Applicatie-eigenaren dienen bekend te zijn (dit is vooral van belang voor applicaties die door meerdere processen en organisatie-eenheden worden gebruikt).
Beschikbaarheid van autorisatie- of CRUD ¹³ -matrices (wie mag wat doen per applicatie).
Overzicht welke applicaties worden gebruikt per proces (proces-applicatiematrix).

Bijlage 2 (zie vervolg)

Gegevens
Een goede gegevensarchitectuur (i.h.b. een corporate objectmodel, waarin alle metagegevens zijn beschreven: objecten, definities en onderlinge relaties tussen objecten); die verplicht is en concernbreed als uitgangspunt wordt gebruikt (dient reeds voor aanvang project te bestaan).
Overzicht welke objecten door welke bedrijfsprocessen worden beheerd (processen-objectenmatrix).
Overzicht welke applicaties welke gegevensgroepen bevatten/gebruiken (objecten-applicatiematrix).
Data dictionary met daarin goede documentatie van de gegevensstructuur per database (metagegevens, ERD).
Technische infrastructuur
Overzicht van de netwerkkarchitectuur/-topologie.
Overzicht van de configuratie.
PROJECTUITVOERING
Zorg voor enkelvoudige vastlegging van de AO/IC-maatregelen. Dit voorkomt fouten en bespaart onnodig werk. Dit kan bijvoorbeeld door invoermacro's te maken, waarbij interviewresultaten via gestandaardiseerde formulieren automatisch in de repository ingelezen kunnen worden.
Richt de repository zo in dat de proces- en AO/IC-beschrijvingen onder de corporate process map komen te hangen en niet onder een organisatiestructuur. Organisatiestructuren wijzigen relatief vaak, waardoor het de beheerinspanning onnodig hoog worden.
Leg de IC-maatregelen samen met de bedrijfsprocessen vast in een voor iedereen benaderbare repository/CASE tool.
IC-maatregelen moeten op het laagste niveau (werkinstructies) worden beschreven (het HOE wordt beschreven op het laagste niveau; het WAT wordt beschreven op het op één na laagste niveau.) Het werkinstructieniveau moet voor alle processen zijn beschreven, anders is het onmogelijk om de huidige IC-maatregelen te beoordelen; per processtap/IC-maatregel moet duidelijk staan beschreven WIE, WAT, WANNEER, HOE doet en hoe wordt omgegaan met afwijkingen/uitzonderingssituaties.

Bijlage 2

Literatuur

Almelo, L. van, 'De lange arm van Sarbanes Oxley', *De Accountant*, oktober 2002, p. 30 t/m 33.
Association of Certified Fraud Examiners, *Report*

to the Nation; Occupational Fraud and Abuse, 2002, <www.cfenet.com>.
Claes, P.F. en H.J.J.M. Meerman, *Risk Management; inleiding tot het risicobeheersproces*, Leiden/Antwerpen, 1991.

- Gist, W.E. en Trimbak Shastri, 'Revisiting Materiality', *The CPA Journal*, November 2003.
- Hartman, W., *Bevordering betrouwbaarheid informatiesystemen*, 2^e herz. druk, Deventer, 1988, reeks Informatiemanagement.
- Kerklaan, L. en R. Knaapen, *Kwaliteit in Kader*, Stichting Kwaliteitsdienst KDI, Rotterdam, 1981.
- Koopmans, L., 'Van materieel belang', *De Accountant*, december 2003, p. 14 t/m 18.
- Renes, R., 'COSO wat valt er te repareren?' *De Accountant*, juni 2003, p. 42 t/m 45.
- Roos Lindgreen, E., *Over informatietechnologie, accountancy en informatiebeveiliging*, Inaugurale rede aan de Universiteit van Amsterdam, 16 oktober 2002.
- Sarbanes Oxley Act 2002, One Hundred Seventh Congress of the United States of America, at the second session, *Sec. 302. Corporate responsibility for financial reports / Sec. 404. Management assessment of internal controls*, 2002.
- Viton, P.L., *Creating Fraud Awareness*, Student paper Texas A & M University, College of Business, November 2002.
- Wagner, S., *Myths and Realities of Sarbanes Oxley*, <www.fei.org>, 2004.

Noten

1. In de Verenigde Staten wordt de afkorting SOA gebruikt, maar aangezien deze afkorting in het Nederlandse taalgebied reeds in gebruik is in het kader van geheel andere problematiek, hanteren wij in Nederland de afkorting SOx. Waarom voor SOx is gekozen is de vraag; de afkorting SOx is in de chemie immers reeds in gebruik als aanduiding voor de familie der stikstofoxiden; wellicht wordt deze mogelijke verwarring als minder gênant ervaren.
 2. §302: CORPORATE RESPONSIBILITIES FOR FINANCIAL REPORTS
The signing officers (CEO and CFO) must provide certifications containing several representations:
 1. *We have reviewed this annual report;*
 2. *This annual report does not contain any untrue statement of a material fact;*
 3. *The financial statements fairly present in all material respects the financial condition and results of operations;*
 4. *We:*
 - A. *are responsible for establishing and maintaining internal controls and*
 - B. *have designed such internal controls to ensure that material information is made known to us;*
 - C. *Evaluated the effectiveness of the internal controls (within 90 days prior to the report's filing date);*
 - D. *Presented in this annual report our conclusions about the effectiveness.*
 5. *We have disclosed to the auditors and the Audit Committee:*
 - A. *All significant deficiencies in the design or operation of internal controls for financial reporting;*
 - B. *Any fraud whether or not material.*
 6. *Significant changes to internal control for financial reporting.*
- §404: MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS
The annual report should contain an internal report including:
1. *A statement of management's responsibilities for establishing and maintaining adequate internal controls and procedures for financial reporting;*
 2. *Conclusions about the effectiveness of the company's internal controls and procedures for financial reporting based on management's evaluation of those controls and procedures (...) as of the end of the company's most recent fiscal year;*
 3. *Statement that the registered public accounting firm (...) has attested to and reported on management's evaluation of the company's internal controls and procedures for financial and management reporting.*
3. Inherent risico is de kans op het optreden van een materiële fout in een informatie-item.
 4. Hieronder vallen tevens aan derden uitbestede bedrijfsprocessen. Wagner (2004) geeft aan dat het in voorkomende gevallen mogelijk is om te volstaan met een zogenoemde SAS 70 (type 2) rapportage van de service provider, waarin hij zijn interne controlemaatregelen ten behoeve van SOx documenteert.
 5. Onder applicaties vallen tevens applicatie-interfaces, middleware, besturingssystemen en database managementsystemen, inclusief aan derden uitbestede applicaties.
 6. Als er in het vervolg in dit artikel wordt gesproken over SOx of SOx-relevante risico's worden, tenzij anders aangegeven, uitsluitend risico's in de context van §302 en §404 bedoeld.
 7. Een informatie-item is een post op de balans of resultatenrekening.
 8. Configuratie-items zijn met goedkeuring van

het bevoegde management geïnstalleerde software- en hardwarecomponenten.

9. Metagegevens zijn gegevens die iets zeggen over de in de database opgeslagen bedrijfsgegevens; hierbij valt te denken aan associaties (onderlinge relaties tussen gegevens), semantiek (betekenis) en syntaxis (naamgeving) van de gegevens.
10. Configuratie-overzicht bestaat uit een beschrijving van de detailgegevens van de individuele TI-configuratie-items (servers, routers e.d.).
11. De omschrijving van de fraude in deze kolom is vrij vertaald door de auteur.
12. Het acroniem SMART staat voor de wijze waarop een begrip gedefinieerd dient te worden: Specifiek, Meetbaar, Acceptabel, Realistisch en Toetsbaar.
13. CRUD staat voor de gegevensmanipulatiefuncties/-rechten: Create, Read, Use en Delete.

Over de auteur

Drs. Edgar P. Johannsmann is organisatieadviseur op het gebied van informatievoorziening, met als specifieke aandachtsgebieden ICT Strategie en Business- en Informatie-architectuur. Hij heeft in 2003 deelgenomen aan het eerste SOx-project in Nederland.

E-mail: johannsmann.edgar@planet.nl