

# Nederlandse en Amerikaanse SOXA 404-ervaringen

*Drs. R. Smidt-van der Veer CMA/CFM*

*Drs. A. E. van der Slik RC<sup>1</sup>*

1	Inleiding	A1510- 3
2	Betekenis van SOXA en de SOXA 404-verklaring	A1510- 3
2.1	SOXA 302-verklaring	A1510- 4
2.2	SOXA 404-verklaring	A1510- 5
3	SOXA office Regio NL binnen ABN AMRO	A1510- 6
4	Documentatie van de controles	A1510-11
4.1	Control Environment Questionnaires	A1510-12
4.2	Control templates	A1510-13
5	Ervaring binnen een business unit	A1510-14
5.1	Ervaringen met een SOXA- vastleggingstool	A1510-15
5.2	Overgang van project naar staande organisatie	A1510-15
5.3	Integratie van frameworks	A1510-16
5.4	Proceseigenaren verantwoordelijk voor SOXA deliverables	A1510-17

1 Drs. R. Smidt CMA/CFM is senior SOXA consultant bij het SOXA office Regio NL van ABN AMRO.  
Drs. A. E. van der Slik RC is Manager Central Services bij ABN AMRO Mellon Global Securities Services.

6	Amerikaanse SOXA 404-ervaringen	A1510-17
6.1	Materieel gebrek in de IC	A1510-18
6.2	Extra compliancekosten en de gevolgen voor de controllers	A1510-19
6.3	Gevolgen voor de toezichhouders	A1510-19
6.4	Lessen uit de Amerikaanse ervaringen	A1510-19
6.5	Voordelen van de SOXA 404- verklaring	A1510-20
7	Samenvatting en conclusies	A1510-21
8	Literatuurlijst	A1510-22

## 1 Inleiding

Als reactie op diverse boekhoudschandalen, zoals Worldcom, Enron en Parmalat, zijn er internationaal verschillende 'corporate governance codes' opgesteld. In de Verenigde Staten is de Sarbanes Oxley Act (SOXA) in werking getreden in juli 2002.

In dit artikel lichten we de betekenis toe van de SOXA en de SOXA 404-verklaring. De Sarbanes Oxley Act bestaat uit 11 titels, waarbij we met name op de artikelen 3 en 4 zullen ingaan. Vervolgens bespreken we de corporate governance praktijkervaringen van het SOXA office Regio NL van ABN AMRO. Buitenlandse ondernemingen die in de Verenigde Staten beursgenoteerd zijn, moeten per 2006 voor het eerst een SOXA 404-verklaring afgeven. Voor deze verklaring moeten beursgenoteerde ondernemingen verantwoordelijkheid nemen voor een werkend en effectief systeem van interne beheersingsmaatregelen. De wijze, waarop de interne beheersingsmaatregelen worden vastgelegd, wordt toegelicht. Vervolgens worden ervaringen van ABN AMRO Mellon besproken, een joint venture van ABN AMRO en Mellon Financial Corporation. Hierbij worden de vastleggingstool, de overgang van een project naar een staande organisatie, de integratie van frameworks en de verantwoordelijkheid van de proceseigenaren toegelicht.

In de Verenigde Staten moesten ondernemingen per 2004 SOXA 404 compliant zijn. In het Controllers Leadership Research zijn de eerste resultaten hiervan bekendgemaakt. Op basis van de ervaringen in Amerika zullen we bepaalde conclusies trekken voor mogelijke ontwikkelingen in de Nederlandse praktijk. Het artikel eindigt met een samenvatting en conclusies.

## 2 Betekenis van SOXA en de SOXA 404-verklaring

Naar aanleiding van de grote beursfraudes in Amerika (Worldcom, Enron) hebben twee senatoren, Michael Oxley en Paul Sarbanes, een nieuwe wet opgesteld: de Sarbanes Oxley Act van 2002. Deze nieuwe wet- en regelgeving is gericht op het verbeteren van de kwaliteit en de transparantie van de financiële rapportage plus de disclosures ter bescherming van de beleggers.

Wat zijn de doelstellingen van de SOXA-wetgeving? De doelstellingen zijn:

- Het waarborgen van de kwaliteit en de transparantie van de

financiële rapportage plus disclosures, onafhankelijke audits en de service van externe accountantskantoren voor publieke bedrijven.

- Het verbeteren van goed ondernemingsbestuur en het verbeteren van de betrouwbaarheid van de externe verslaggeving.
- Het opzetten van Public Company Accounting Oversight Board (PCAOB).
- Het zich onafhankelijk opstellen van de accountantskantoren.
- Het verbeteren van het toezicht op de financiële rapportage en audits door de Securities and Exchange Commission.

De act bestaat uit 11 titels, waarvan vooral titel IV Enhanced Financial Disclosures grote impact heeft. Titel IV gaat in op het belang van interne beheersingsmaatregelen: het management van beursgenoteerde ondernemingen dient jaarlijks een rapportage op te stellen met daarin expliciet een verklaring omtrent:

- hun verantwoordelijkheid voor het inrichten en onderhouden van een adequaat interne beheersingssysteem (structuur en procedures) en voor de financiële rapportage en;
- de resultaten van de beoordeling van de effectiviteit van het systeem van interne controle met betrekking tot de financiële verslaggeving door de onderneming.

De externe accountant van de onderneming dient deze rapportage te controleren en van een verklaring te voorzien. Deze controle en het afgeven van de verklaring maken onderdeel uit van de jaarrekeningcontrole.

Ook titel III Corporate responsibility gaat in op het belang van interne beheersingsmaatregelen. Titel III bepaalt dat er sprake is van een onafhankelijke Audit Commissie. Daarnaast dienen de CEO en CFO kwartaal- en jaarverslagen te certificeren, inclusief een verklaring over de effectiviteit van het in de onderneming aanwezige systeem van interne beheersingsmaatregelen.

## 2.1 SOXA 302-verklaring

De CEO en CFO zijn verplicht door middel van een 302-verklaring, die bij jaar- en kwartaalverslagen wordt toegevoegd, te verklaren dat zij het verslag hebben beoordeeld. Daarin verklaren zij naar hun beste eer en geweten dat er geen sprake is van materiële onjuistheden of omissies en dat de financiële informatie een getrouw beeld geeft van resultaat en vermogen van de onderneming. Materiële onjuistheden en omissies in de interne beheersing moeten bij de externe accountant, Audit Commissie en in het jaar- en kwartaalverslag worden gemeld. De 302-verklaring wordt al afgegeven door Europese ondernemingen.

## 2.2 SOXA 404-verklaring

Per 2006 dienen ondernemingen, gevestigd buiten de VS die aan de Amerikaanse beurs genoteerd zijn, ook de SOXA 404-verklaring af te geven. Wat houdt de SOXA 404-verklaring in? Sectie 404 van de Sarbanes-Oxley Act bepaalt dat het management van beursgenoteerde bedrijven verantwoordelijkheid moeten nemen voor een werkend en effectief intern beheersingssysteem en dat zij over de effectiviteit van dat systeem moeten rapporteren.

Sectie 404 bepaalt dat het jaarverslag een rapport van het management over de interne controle moet bevatten. Dit rapport heeft de volgende inhoud:

- het management geeft aan dat het verantwoordelijk is voor het opzetten en onderhouden van een adequate interne beheersingsstructuur en procedures voor financiële rapportage;
- identificatie van het framework dat het management gebruikt om de effectiviteit van interne controle met betrekking tot financiële rapportage te evalueren;
- een beoordeling (assessment) van het management met betrekking tot de effectiviteit van de interne beheersingsstructuur en de procedures voor financiële rapportage per het einde van het fiscale jaar.

In tabel 1 zijn de verschillen tussen de SOXA 302 en SOXA 404-verklaring weergegeven.

Tabel 1. *Verschillen tussen SOXA 302 en 404*

SOXA 302	SOXA 404
Gericht op tijdige en volledige informatievoorziening naar beleggers (zowel financieel als niet-financieel)	Gericht op de interne beheersing van de financiële rapportage
Geen bemoeienis externe accountant	Vereist een jaarlijkse verklaring van de externe accountant, enerzijds over de kwaliteit van de uitgevoerde beoordeling door het management en anderzijds een eigen conclusie ten aanzien van de effectiviteit van de interne beheersing van de financiële rapportage

SOXA 302	SOXA 404
Geen documentatievereisten	Documentatie ten aanzien van de effectiviteit van de interne beheersing van de externe rapportage vereist
Betrekking op kwartaalver- slaggeving	Betrekking op jaarlijkse ver- slaggeving
Is reeds van kracht	Vanaf juli 2006 van kracht (voor bedrijven gevestigd buiten de VS)

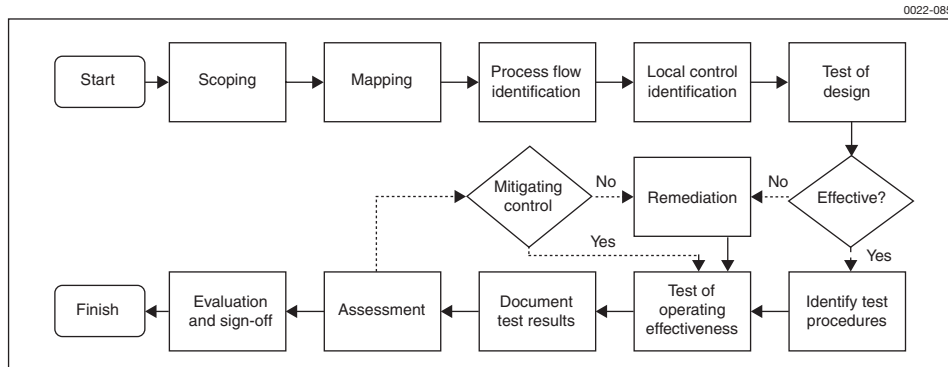
De 302-verklaring gaat uit van het principe 'tell me', terwijl bij 404 het principe 'prove me' van kracht is. Documentatie is van essentieel belang bij de 404-verklaring.

### 3 SOXA office Regio NL binnen ABN AMRO

De Amerikaanse SOXA-wetgeving is van toepassing op bedrijven die in de Verenigde Staten beursgenoteerd zijn. Omdat ABN AMRO een beursnotering in de Verenigde Staten heeft, moet zij aan de SOXA-vereisten voldoen. Bedrijven met het hoofdkantoor buiten de Verenigde Staten, echter met een beursnotering in de Verenigde Staten, hebben uitstel gekregen. Zij dienen per 2006 aan SOXA 404 te voldoen. Dit uitstel is echter pas halverwege 2005 bekendgemaakt, toen ABN AMRO al gevorderd was met SOXA compliance voor 2005. ABN AMRO heeft toen besloten al per 2005 een interne SOXA 404-verklaring af te geven.

ABN AMRO heeft een centraal SOXA office, dat de richtlijnen en de vereiste documenten opstelt voor het SOXA-proces. Daarnaast hebben de verschillende business units binnen ABN AMRO een eigen SOXA office dat rapporteert aan het centrale SOXA office. De verschillende SOXA offices hangen organisatorisch onder de afdeling Finance. Het SOXA-proces binnen ABN AMRO is weergegeven in figuur 1.

De verschillende business units (reporting entities) rapporteren aan het hoofdkantoor. Om de benodigde materialiteit voor SOXA te behalen, is per entiteit de scope bepaald. De materialiteit wordt bepaald op basis van Form 20F. Form 20F is de jaarrekening van bedrijven gevestigd buiten de Verenigde Staten voor de Securities and Exchange Commission gebaseerd op de Amerikaanse accounting regels (US GAAP). Voor de zo-



Figuur 1. SOXA-proces binnen ABN AMRO

genaamde Foreign Filers (zoals ABN AMRO) is de Form 20F gebaseerd op de IFRS jaarrekening. Materialiteit wordt berekend op basis van zowel kwantitatieve factoren (bijvoorbeeld 5% van pre-tax income) alsook op basis van kwalitatieve factoren (bijvoorbeeld inherente risico's).

Het groep SOXA office hanteert bij de vaststelling van de scope voor het SOXA-proces de volgende indeling:

- List 1: Grootste reporting entities. Hiervoor geldt dat de beschreven processen 80% van de reporting value (is de som van alle Form 20F-rekeningen in de balans en W&V-rekening in absolute termen) moeten dekken;
- List 2: Entities met een of meer 20F-rekeningen met een minimaal saldo van € 1 miljard;
- List 3: Entities met een verhoogd inherent risico. Dit zijn companies met een groot potentieel risico;
- List 4: Entities niet behorende tot list 1 en 2 met een totale reporting value groter dan € 1 miljard;
- List 5: Entities met een reporting value < € 1 miljard > € 100 miljoen;
- List 6: Entities met een reporting value < € 100 miljoen.

De grotere entiteiten bijvoorbeeld list 1 reporting entities zullen aan meer processen van SOXA voldoen dan de kleinere entiteiten.

De list 1 reporting entities koppelen vervolgens de verschillende balansen en verlies- en winstrekeningen aan verschillende processen (mapping). De processen moeten 80% van de reporting value dekken. Groep SOXA office heeft een aantal processen geïdentificeerd waarvoor een aantal templates<sup>1</sup> is ontwikkeld. Voor al deze verschillende processen zijn proceseige-

<sup>1</sup> Een template is een voorgeschreven formaat.

naren benoemd die verantwoordelijk zijn voor het hele proces. Voorbeelden van processen zijn Hypotheken, FX Money Market, Derivaten en Asset Liability Management. Daarnaast zijn er ook ondersteunende processen, zoals Human Resources en Accounts payable.

De templates van de verschillende processen hebben een centrale controlcatalogus waarin globale beheersingsmaatregelen worden omschreven met daaraan gekoppeld de risico's. Op grond van deze controlcatalogus worden de lokale beheersingsmaatregelen (local control) op detailniveau beschreven. Bij deze lokale beheersingsmaatregelen wordt er uitgegaan van de 4W en 1H namelijk:

- *Welke* controle wordt uitgevoerd (bijvoorbeeld een cijferbeoordeling)?
- *Wie* voert de controle uit (bijvoorbeeld financiële analist, manager van de afdeling, CFO)?
- *Wanneer* wordt de controle uitgevoerd (bijvoorbeeld dagelijks, wekelijks, eenmaal per kwartaal)?
- *Waar* blijkt de controle uit (bijvoorbeeld aansluitingsoverzicht, notulen, e-mail)?
- *Hoe* wordt de controle uitgevoerd (bijvoorbeeld door middel van een review of een goedkeuring)?

Indien er geen lokale beheersingsmaatregel is die aansluit bij de centrale controlcatalogus, is er sprake van een design gap. Een design gap is een hiaat in de interne beheersing doordat een interne beheersingsmaatregel niet adequaat is ontworpen waardoor een financieel risico niet of niet in voldoende mate wordt afgedekt. De proceseigenaar zal dan een verbeterplan opstellen, waarin wordt aangegeven wanneer door wie en op welke wijze de gap zal worden opgelost.

Binnen ABN AMRO is ervoor gekozen om de Test of Operating Effectiveness door de Interne Auditafdeling te laten uitvoeren. Deze ontwikkelt testplannen en bespreekt deze met de proceseigenaren. Operating effectiveness is de mate waarin ter afdekking van mogelijke financiële risico's ontworpen interne beheersingsmaatregelen daadwerkelijk bestaan en werken. De Interne Auditafdeling interviewt hiervoor personen en kijkt de documentatie na om het proces te evalueren. Verder wordt het proces getest en worden steekproeven genomen om te bepalen of interne beheersingsmaatregelen effectief werken. De frequentie waarmee de interne beheersingsmaatregel wordt uitgevoerd, bepaalt de grootte van de steekproef. Tabel 2 geeft een overzicht van de verschillende frequenties en daarbij gerelateerde steekproefgrootte.

Tabel 2. Frequentie uitvoering interne beheersingsmaatregel en steekproefgrootte

Frequentie van de beheersingsmaatregel	Steekproefgrootte
Dagelijks	25
Wekelijks	5
Maandelijks	3
Kwartaalbasis	2
Halfjaar basis	1

Als er een hiaat is in de interne beheersing doordat een goed ontworpen interne beheersingsmaatregel niet werkt zoals beoogd, waardoor een financieel risico niet of niet in voldoende mate wordt afgedekt, is er sprake van een operating gap.

De Interne Auditmanager maakt het volgende onderscheid in operating gaps gerelateerd aan de 4 W en 1 H, namelijk:

Wie?	A1: interne beheersingsmaatregel wordt uitgevoerd door een persoon met onvoldoende autoriteit; A2: interne beheersingsmaatregel wordt uitgevoerd door een persoon zonder de benodigde competenties;
Welke?	B1: interne beheersingsmaatregel zoals ontworpen wordt niet uitgevoerd en het type beheersingsmaatregel mitigeert niet het risico of raakt de rekening zekerheid (assertion). De verschillende zekerheden komen in de volgende alinea bij de tweede bullet aan de orde;
Waar?	C1: het gedocumenteerde bewijsmateriaal is niet in compliance met het ABN AMRO bewijsmateriaal beheersingsmaatregel beleid;
Wanneer?	D1: de frequentie van de uitvoering van de beheersingsmaatregel wordt niet uitgevoerd zoals ontworpen;
Hoe?	E1: de beheersingsmaatregelprocedure zoals uitgevoerd is significanter dan gedocumenteerd en mitigeert niet het risico of bereikt de rekening zekerheden;
	F1: het bewijsmateriaal van de beheersingsmaatregel bestaat en het voldoet aan de rekening zekerheid, maar is anders dan beschreven. De beheersingsmaatregel dient te worden herschreven.

Als de gaps zijn geïdentificeerd, vindt er een *assessment* plaats. Deze assessment vindt plaats tussen de Interne Auditafdeling, het SOXA office en de proceseigenaar. De testrapportage van de Interne Auditafdeling wordt besproken in een vergadering met de proceseigenaar, SOXA Office Regio NL en Interne Audit accountmanager. De volgende aspecten worden besproken.

- Classificatie van ineffectieve controls in risicograden (SOXA high/medium/low). De risicograden zijn afhankelijk van de materialiteit in de jaarrekening. Hiervoor worden bepaalde ranges gehanteerd.
- Nadere inschatting van compensating controls, dus beheersingsmaatregelen die het ontbreken van bepaalde beheersingsmaatregelen met daaraan gekoppelde zelfde risico's compenseren. Een criterium hiervoor is dat dezelfde kenmerken (assertion) in de jaarrekening wordt geraakt. Binnen de jaarrekening worden de volgende kenmerken (assertions) onderkend:
  - completeness (volledigheid);
  - existence (bestaan van een post);
  - valuation (waardering);
  - presentation and disclosure (presentatie en bekendmaking);
  - rights and obligations (rechten en verplichtingen).

Voorbeeld: een transactie wordt ingebracht door een medewerker. Een andere medewerker controleert en tekent af. Indien deze controle door de tweede medewerker niet wordt afgetekend, kan deze worden gecompenseerd door het vierogen principe via de toegangsrechten van een bepaald transactiesysteem. Dit betekent dat voor beheersingsmaatregelen die in de testfase niet blijken te bestaan of niet goed blijken te functioneren, wordt geanalyseerd of er andere beheersingsmaatregelen bestaan die betrekking hebben op dezelfde risico's met dezelfde zekerheid (assertion).

- Bepalen van de waarschijnlijkheid van een fout in de jaarrekening. Bij het bepalen van de waarschijnlijkheid van fout in jaarrekening wordt de volgende indeling gehanteerd volgens Financial Accounting Standards Board Statement no 5, namelijk:
  - remote: de kans op een toekomstige fout is gering;
  - reasonably possible: de kans op een toekomstige fout is meer dan gering maar minder dan waarschijnlijk;
  - probable: de kans op een fout is waarschijnlijk.

Vooral deze stap is een lastige, omdat de waarschijnlijkheid en de grootte van het bedrag moeilijk te bepalen zijn. Veel gaps zijn F1 gaps, deze kunnen snel worden opgelost omdat de interne beheersingsmaatregel wel effectief is, maar de omschrijving van de beheersingsmaatregel moet worden aangepast.

De Raad van Bestuur van ABN AMRO draagt de eindverantwoordelijkheid voor SOXA 404. De CEO en CFO ondertekenen het 'external management report on internal controls' (externe sign off).

Intern op BU niveau ondertekenen verschillende functionarissen het 'SOXA 404 Statement'. Deze 'statement' heeft slechts werking binnen ABN AMRO (interne sign off). Binnen Regio NL (incl. dochters) verrichten de volgende functionarissen de interne sign off:

- Management Team Regio NL;
- Proceseigenaren Regio NL;
- Managementteams van de dochters.

#### 4 Documentatie van de controles

Hoe worden alle controles gedocumenteerd? SOXA 404 vereist zoals reeds eerder aangegeven dat ondernemingen de effectiviteit van de interne controle beoordelen en hierover rapporteren. De onderneming moet ook aangeven welk raamwerk en normenkader zij heeft gehanteerd bij de evaluatie van het interne beheersingssysteem. Een algemeen geaccepteerd raamwerk wat hiervoor volgens de Securities and Exchange Commission (SEC), Public Company Accounting Oversight Board (PCAOB) en het Koninklijk Instituut voor Registeraccountants (NIVRA) kan worden gebruikt is het COSO-framework. De PCAOB geeft in Auditing Standard no 2 (AS2) aan dat het management zijn beoordeling over de effectiviteit moet baseren op een geschikt, erkend control framework. De PCAOB geeft verder aan wat onder een geschikt raamwerk wordt verstaan en geeft aan dat het COSO-framework een geschikt raamwerk<sup>1</sup> is. De PCAOB geeft daarbij wel aan dat ook andere geschikte raamwerken gebruikt mogen worden.

ABN AMRO maakt gebruik van het COSO-Internal Control Integrated Framework uit 1992, omdat deze wordt aanbevolen door de PCAOB en het COSO-framework zijn waarde heeft bewezen. Het COSO-framework uit 1992 bestaat uit de volgende componenten:

- 1 control environment,
- 2 risk assessment,
- 3 control activities,
- 4 information & communication en
- 5 monitoring.

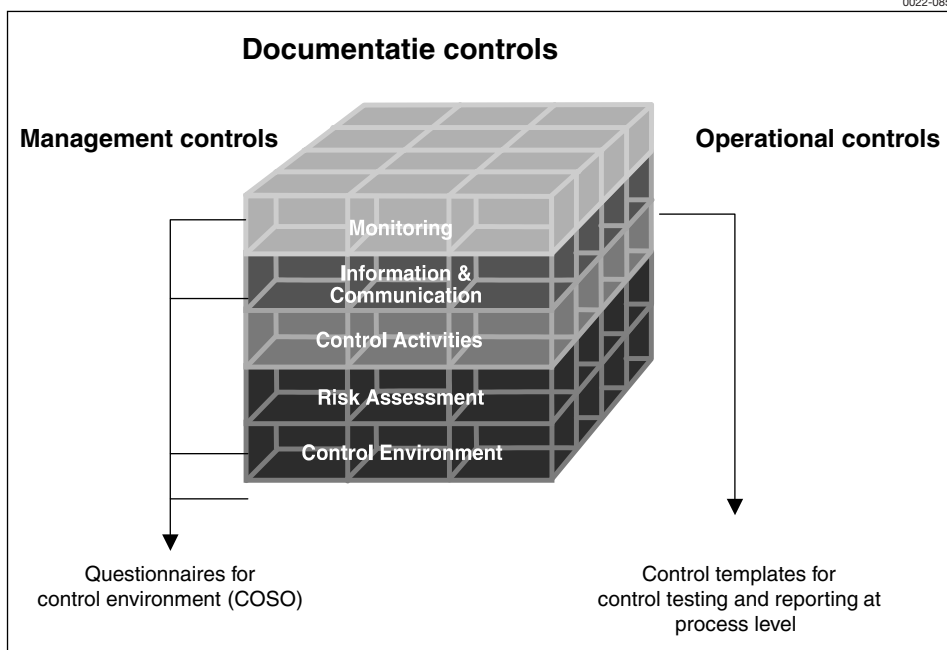
In 2004, is het COSO-model II, Enterprise Risk Management Framework, ontwikkeld. Aan de drie COSO-doelstellingen:

- 1 Andere raamwerken zijn: Turnbull, CoCo en COBIT.

operations, reporting en compliance is de strategische doelstelling toegevoegd. Verder zijn de vijf COSO-componenten uitgebreid met:

- 1 objective setting,
- 2 event identification.
- 3 risk response.

Aangezien het COSO-model II pas in 2004 is ontwikkeld, terwijl in 2004 al het project SOXA was opgestart, heeft ABN AMRO gekozen voor het COSO-framework uit 1992. Wellicht zullen in de toekomst nieuwere releases van COSO in overweging worden genomen.



*Figuur 2. COSO-framework*

#### 4.1 Control Environment Questionnaires

Naast het voldoen aan specifieke interne controledoelstellingen, betekent SOXA 404 ook dat de controleomgeving adequaat dient te functioneren. Immers Enron en Worldcom hadden een ineffektieve controleomgeving. De controleomgeving bestaat uit een aantal procesoverstijgende zaken, zoals organisatiecultuur, tone at the top, integriteit, beloningsstructuur van de top en HR-beleid. Integriteit en ethische waarden zijn belangrijke onderdelen van de controleomgeving. Kaptein, Rozekrans en De Groot (2005) geven aan dat 'Een stelsel van beheersingsmaatregelen zonder imbedding in de waarden en normen van managers en medewerkers is als een huis zonder

fundament.’ Om de procesoverstijgende zaken in kaart te brengen en te beoordelen is een vragenlijst met betrekking tot de corporate policies opgesteld, de Control Environment Questionnaire (CEQ).

De CEQ sluit aan bij de hiervoor genoemde COSO-componenten, te weten 1. controleomgeving, 2. risicobeoordeling, 4. informatie en communicatie en 5. bewaking. (Het hiervoor besproken proces van ontwerp, documentatie en testen van beheersingsmaatregelen heeft betrekking op component 3. controleactiviteiten.) In deze questionnaires zijn per COSO-component corporate policies geformuleerd. Met betrekking tot de controleomgeving wordt bijvoorbeeld gevraagd een oordeel te vormen over op welke wijze het management omgaat met integriteit, ethische normen en waarden en op welke wijze wordt omgegaan met fraude. Identificatie van risico, anticiperen van het management op wijzigingen zijn voorbeelden van corporate policies die onderdeel zijn van de COSO-component risicobeoordeling. Hetzelfde geldt voor COSO-componenten Informatie en Communicatie en Bewaking waar wordt gevraagd een oordeel te vormen over de wijze waarop wordt omgegaan met de informatie van iemand die de klok luidt over ontoelaatbare praktijken, klachtenafhandeling, internal audit enzovoort.

Deze vragenlijsten worden door het MT BU NL en het MT van de dochters ingevuld. Vooral deze management beheersingsmaatregelen zullen de kwaliteit en het functioneren van de operationele beheersingsmaatregelen bepalen. Ook hier geldt dat evidence zeer belangrijk is. De Interne Auditafdeling test ook de antwoorden van de Management Control Environment Questionnaire.

Het is moeilijk om de effectiviteit van de controleomgeving te meten. De controleomgeving is niet transactie georiënteerd, hierdoor is het onmogelijk een ‘walkthrough’ of een ‘sample test’ uit te voeren. Een survey, interview of notulen kunnen hierbij uitkomst bieden. Echter een onderneming kan beweren een ‘code of conduct’ te hebben, maar het enkel bestaan van dit document wil nog niet zeggen dat het ook effectief werkt.

#### **4.2 Control templates**

Voor het vastleggen van de control activiteiten zijn templates ontwikkeld waarbij per proces de interne beheersingsmaatregelen zijn beschreven. Deze templates bevatten een overzicht van de rekeningen waarop het proces betrekking heeft, een centrale controlcatalogus, lokale beheersingsmaatregelen, testprocedures binnen Interne Auditafdeling enzovoort. Per template is een proceseigenaar verantwoordelijk voor het hele proces. Zo zijn er templates voor de processen hypotheek, consumer lending enzovoort.

Vanuit SOXA is het van belang dat de processen en daarin begrepen controls zijn vastgelegd in procesdocumentatie. Veel organisaties kiezen ervoor om in het kader van SOXA de processen (opnieuw) te beschrijven in procedures. ABN AMRO heeft echter reeds een uitgebreide set procedures en heeft ervoor gekozen de bestaande procedures te gebruiken voor de SOXA-documentatie. Het is wel aan de proceseigenaren om ervoor te zorgen dat de bestaande procedures volledig en up-to-date zijn.

Over het jaar 2005 is de SOXA 404-verklaring ondertekend door het Management Team BU NL, hoewel er extern nog geen verklaring hoeft te worden gegeven. In het jaar 2006 zullen de uitdagingen met name liggen op het beperken van het aantal beheersingsmaatregelen. Voor het beperken van het aantal beheersingsmaatregelen is de risk-based approach van de PCAOB Release van mei 2005 als uitgangspunt genomen. Per proces zijn de risico's geïdentificeerd. Vervolgens worden de beheersingsmaatregelen gekoppeld aan de risico's. Tot slot wordt beoordeeld of de beheersingsmaatregelen de kenmerken van de desbetreffende jaarrekening dekken.

## 5 Ervaring binnen een business unit

Bovenstaande ervaringen zijn vanuit het SOXA office regio NL beschreven. Hier volgt een ervaring vanuit een van de rapporterende business units, zijnde ABN AMRO Mellon, een joint venture van ABN AMRO en Mellon Financial Corporation.

Vanuit de scoping door ABN AMRO is ABN AMRO Mellon een list 4 entiteit. Dit betekent dat in 2005 met name het Financial Statement Closing Process binnen de scope valt. De volgende activiteiten hebben voor dit proces plaatsgevonden.

ABN AMRO heeft een standaard template voor het Financial Statement Close proces gecreëerd: dit betekent dat het SOXA office een aantal beheersingsmaatregelen heeft samengesteld die standaard in een dergelijk proces voorkomt (key controls). Iedere business unit geeft per key control aan op welke wijze deze beheersingsmaatregelen lokaal zijn ingericht (local controls). Deze 'local controls' zijn beschreven en later gedurende 2005 getest. Voor ABN AMRO Mellon betekent dit niet dat het proces is veranderd, maar meer dat een grotere bewustwording is ontstaan omtrent de controles die in dit proces worden uitgevoerd.

Na het testen heeft een assessment plaatsgevonden, zowel door de proceseigenaren als door de managing board. De CEO en CFO hebben afgetekend voor de SOX 404-verklaring per jaareinde 2005.

### **5.1 Ervaringen met een SOXA-vastleggingstool**

Een SOXA-project bestaat uit een aantal stappen die worden vastgelegd. Voor deze vastlegging maakt ABN AMRO gebruik van de tool SAP Management Information Control. In deze tool worden de volgende aspecten per business unit vastgelegd:

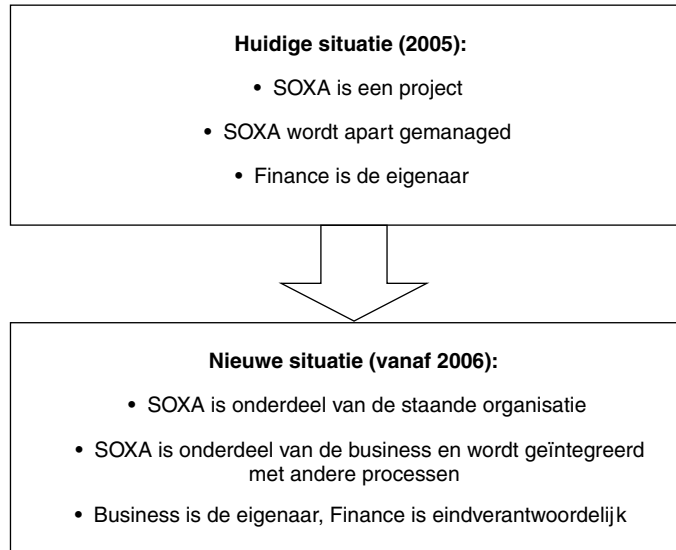
- scope van de business unit;
- beschrijvingen van de local controls;
- de 'uitslagen' van de 3 fasen van SOXA: effectiveness of documentation, effectiveness of design en effectiveness of operations. Deze worden beoordeeld als 'adequate' of 'deficient';
- in het geval van deficiencies worden verbeterplannen in de tool vastgelegd.

In deze tool is de voortgang van de SOXA-werkzaamheden in de business units te monitoren; zo is te zien welke activiteiten (design, testen) al hebben plaatsgevonden of nog gepland staan. De SAP MIC tool die wordt gebruikt binnen ABN AMRO is in ontwikkeling.

### **5.2 Overgang van project naar staande organisatie**

2005 was het eerste jaar voor ABN AMRO om aan SOXA te voldoen. Nu is het zaak om een overgang van SOXA als project naar SOXA als staande organisatie te bewerkstelligen. Dit betekent dat SOXA geïntegreerd moet worden in de staande processen en niet meer kan worden gezien als een eenmalig project. Bij SOXA office regio NL wordt niet meer gesproken over een project. Het is een afdeling binnen Finance. In figuur 3 is weergegeven hoe de overgang van een project naar de bestaande organisatie eruitziet.

0022-0852



*Figuur 3.*  
Overgang van project naar  
staande organisatie

### 5.3 Integratie van frameworks

Naast SOXA voldoet ABN AMRO Mellon aan een aantal andere frameworks: SAS 70<sup>1</sup>, interne procedures en, in de toekomst, Basel II<sup>2</sup>.

Deze raamwerken zijn gedeeltelijk overlappend en gedeeltelijk verschillend. De SAS 70 heeft bijvoorbeeld betrekking op de operationele betrouwbaarheid vanuit het oogpunt van de klant, waarbij betrouwbaarheid van de financiële rapportage niet van belang is. Het SOXA-raamwerk heeft juist wel betrekking op de financiële rapportage en niet op operationele doelstellingen.

1 De Statement on Auditing Standards Number 70, Service Organizations (SAS 70) is een internationaal erkende auditing standaard. Deze standaard is ontwikkeld door het American Institute of Certified Public Accountants (AICPA). Volgens deze standaard onderzoekt en beoordeelt een onafhankelijke auditor de beheersmaatregelen van een dienstverlenende organisatie. De auditor(s) sluit een SAS 70 audit af met een formeel rapport (Service Auditor's Report).

2 BASEL II is een update op een ouder akkoord van het internationale bankwezen BASEL I uit 1988. Doel is het verbeteren van de internationale consistentie van de regulering van kapitaal en het promoten van een gedegen risicomanagement binnen grote en internationaal actieve banken. Dit Basel II Capital akkoord gaat in op 1 januari 2007.

BASEL II is een akkoord tussen banken, centrale banken (ook de Nederlandsche bank) en toezichhouders en heeft specifiek betrekking op de 3 pijlers:

- kredietrisico's,
- marktrisico's,
- operationele risico's.

BASEL II verplicht financiële instellingen een goed risicobeheer te voeren.

Deze raamwerken hebben echter de volgende aspecten gemeenschappelijk:

- documentatie waarin de procesgang wordt vastgelegd;
- het procesontwerp wordt beoordeeld;
- de uitvoering van het proces wordt getest.

Om deze elementen te optimaliseren kan een aantal aspecten worden gecombineerd: procesdocumentatie voor het ene raamwerk kan ook voor een ander raamwerk worden gebruikt, zolang de benodigde elementen aanwezig zijn. (Dit verhoogt de kans op intensiever gebruik en onderhoud van de procesdocumentatie.)

#### **5.4 Proceseigenaren verantwoordelijk voor SOXA deliverables**

Een van de belangrijkste elementen van SOXA is dat de proceseigenaren verantwoordelijk zijn voor de processen en de controls, en niet de Finance functie. In de praktijk blijkt echter dat de verantwoordelijkheid voor het SOXA-project binnen de Finance functie ligt. De SOXA-projectorganisatie en de Finance functie verdiepen zich in alle SOXA-materie, dat een heel eigen jargon en begrippenkader kent. De Finance functie klopt dan bij de proceseigenaren aan om verantwoordelijkheid te nemen voor het procesontwerp en de uitvoering. Helaas blijkt het lastig om de proceseigenaren, meestal drukke managers, zich in deze specifieke materie intensief genoeg te laten verdiepen. Aansturing vanuit het SOXA office blijkt vitaal om de juiste producten te verkrijgen. Het SOXA office doet ook de quality assurance van de op te leveren controls. Binnen Regio NL zijn de proceseigenaren en de SOXA-procesmanagers formeel benoemd via een benoemingsbrief van de CFO. Daarnaast heeft de CFO ook een proceseigenarenbijeenkomst gehouden waarbij SOXA en de vereisten en de verantwoordelijkheden van de proceseigenaren zijn toegelicht. Hierdoor zal het SOXA-raamwerk ook bij de operationele managers meer bekendheid krijgen.

Nu een aantal praktijkervaringen binnen ABN AMRO en ABN AMRO Mellon is toegelicht, worden Amerikaanse ervaringen gebaseerd op het Controllers Leadership Research beschreven.

## **6 Amerikaanse SOXA 404-ervaringen**

Waar de Europese ondernemingen een jaar uitstel hebben gekregen om SOXA 404 compliant te zijn, geldt dat niet voor de Amerikaanse ondernemingen. Zij dienen al over 2004 SOXA 404 compliant te zijn. De Amerikaanse ondernemingen dienen dus naast het Amerikaanse jaarverslag (Form 10K) ook een internal control statement af te geven. In deze internal control

statement worden de interne beheersingsmaatregelen van de organisatie en eventuele gebreken in de interne controle vastgelegd *en* gecertificeerd door de externe accountant. Gebaseerd op het Controllers Leadership Research willen we de lezers laten delen in de eerste SOXA 404-ervaringen uit Amerika. Allereerst wordt aangegeven hoeveel ondernemingen een materieel gebrek in de interne controle rapporteerden en wat de gevolgen hiervan waren op de beurskoers. Verder worden de soorten materiële gebreken in de IC (Interne Controle) aangegeven. Vervolgens wordt ingegaan op de gestegen kosten van compliance als gevolg van SOXA 404 en de gevolgen in de tijdsbesteding van de controller. Ook de veranderingen bij de verschillende toezichthouders wordt kort toegelicht.

Tot slot gaan we in op de toekomst. Wat zullen de belangrijkste SOXA initiatieven voor Finance zijn en wat zullen de twee belangrijkste uitdagingen om voor het tweede jaar SOXA 404 compliant te zijn? Verder geven we een aantal adviezen.

### 6.1 Materieel gebrek in de IC

Van de 2636 ondernemingen die in de periode januari tot 16 maart 2005 een Form 10K (kwartaalverslag volgens US Gaap) hebben aangeleverd, rapporteerde 11% van de (289) ondernemingen een materieel gebrek in de IC. Het effect op de beurskoers was nog beperkt, omdat dit het eerste jaar is dat de Amerikaanse ondernemingen SOXA 404 compliant dienen te zijn en de ondernemingen nog de gelegenheid krijgen om herstelplannen te laten zien. Verder is de reactie op de beurskoers het grootst bij het rapporteren van meerdere materiële gebreken. Ook is de reactie groter als het materieel gebrek in de IC leidt tot een restatement van de cijfers.

Binnen de organisaties zijn de reacties op een materieel gebrek in de IC heftig. Bij 60% van de ondernemingen die een materieel gebrek in de IC vertoonden, werd de CFO binnen 3 maanden vervangen.

Geconstateerde materiële gebreken hebben betrekking op:

- 43% financiële processen en procedures;
- 14% personeel en training: sinds 1992 zijn de gemiddelde kosten van de Finance afdeling als % van de opbrengsten gedaald van 1,9% naar 1,1% in 2002. Deze kostenbesparende maatregelen hebben geleid tot talrijke personeel gerelateerde weaknesses. Door het grote personeelsverloop en personeelstekort hebben bepaalde onderwerpen te weinig/onvoldoende aandacht gekregen, waardoor een verzwaking in de interne beheersingsmaatregelen optrad;
- 10% tax accounting;
- 6% opbrengstenverantwoording;
- 5% internationale activiteiten;
- 4% documentation;

– 18% overige.

## 6.2 Extra compliancekosten en de gevolgen voor de controllers

De inspanningen om SOXA 404 compliant te zijn, zijn aanzienlijk. In tabel 3 zijn de bedrijfsopbrengsten versus de gemiddelde extra audits vergeleken.

Tabel 3. *Vergelijking bedrijfsopbrengst en gemiddelde extra audits*

Bedrijfsopbrengsten	<\$ 5 mrd	\$ 5 mrd-\$10 mrd	\$10-\$50 mrd	>\$50 mrd
Gemiddeld extra audits	6,285	20,756	11,540	19,000
Gemiddelde totale compliancekosten per mrd \$ in opbrengsten	\$1.9 mio	\$1.1 mio	\$0.6 mio	\$0.3 mio

Ook de controllers zullen veel meer tijd besteden aan controls, compliance en externe rapportages. Een vergelijking in de tijdsbesteding aan kernactiviteiten van de controllers in 2004 versus 2003 laat een verschuiving zien. De tijdsbesteding aan controls, compliance en externe rapportages stijgt met 41%, terwijl de tijdsbesteding aan intern advies, budgettering en planning en managementrapportage met 22% daalt. Dit komt enerzijds doordat de controllers nieuwe taken erbij hebben gekregen, zoals SOXA-teamvergaderingen, SOXA-trainingen en het testen van interne controlemaatregelen, terwijl anderzijds de frequentie van audit commissie presentaties, de presentatie van het bestuur en het overleg met de externe accountant enzovoort toeneemt.

## 6.3 Gevolgen voor de toezichthouders

Ook bij de organisaties die toezicht houden op de regelgeving zijn er veranderingen. De Securities and Exchange Commission stelt zich actiever op ten opzichte van de grote ondernemingen. Het personeel binnen de PCAOB (Public Company Accounting Oversight Board: toezichthouder op de externe accountant ontstaan met de Sarbanes Oxley Act) is met 50% gestegen. De PCAOB voelt druk om te tonen dat SOXA 'tanden' heeft. Uiteindelijk leidt de veranderende rol van de toezichthouders naar aanleiding van SOXA tot een toenemende invloed van de externe accountants en toenemende zorgen van de controllers. De SEC heeft een werkgroep in het leven geroepen die voor het eind van 2006 aanbevelingen moet doen om tot een eenvoudiger en minder ingrijpend en bureaucratisch proces te komen.

## 6.4 Lessen uit de Amerikaanse ervaringen

De belangrijkste SOXA-initiatieven voor ondernemingen zullen zijn:

1. standaardiseren van documentatie en testprocedures;
2. trainen van het finance personeel op SOXA issues;
3. verminderen van het aantal kerncontroles;

4. trainen van personeel bij de bedrijfsonderdelen op SOXA issues;
5. herdefiniëren van taken en verantwoordelijkheden voor 302 en 404.

Om in het tweede jaar SOXA 404 compliant te zijn, zullen de twee belangrijkste uitdagingen zijn:

1. het creëren van een goede testcultuur. Als er in het eerste jaar geen significante gebreken in de interne controle zijn gevonden, moet er toch een cultuur blijven bestaan voor het constant testen van controls;
2. *het* herstellen van de flexibiliteit van een onderneming. Om in 2004 SOXA compliant te zijn, heeft 63% van de Amerikaanse ondernemingen belangrijke wijzigingen in het vierde kwartaal van 2004 vermeden.

#### 6.5 Voordelen van de SOXA 404-verklaring

Naast de nadelen van de grote tijdsinspanning en de hoge kosten worden er in het artikel van Tackett, Wolf en Claypool ook een aantal voordelen van SOXA 404 genoemd. Dat zijn de volgende voordelen:

1. de breedte en diepte van de interne beheersingsmaatregelen over de financiële rapportage zijn significant toegenomen. Bedrijven moeten de significantie van de beheersingsmaatregelen individueel en tezamen beoordelen en deze beheersingsmaatregelen ook documenteren;
2. een duidelijke controleomgeving die de morele toon van de organisatie aangeeft, door bijvoorbeeld ethische codes binnen de organisatie, het screenen van sollicitanten en heldere toewijzing van verantwoordelijkheden;
3. er is een uniforme controleomgeving en interne controlemaatregelen over de financiële rapportage. Dit zal de vergelijkbaarheid van de financiële rapportage ondersteunen;
4. een korte termijn psychologisch effect voor de financiële markten, omdat de regering de accountantfirma's onder druk zet teneinde grote auditgebreken te voorkomen;
5. het zal moeilijker zijn om de financiële cijfers verkeerd weer te geven door middel van fraudemethoden, aangezien samentenspanning tussen senior management, de audit commissie en de Raad van Commissarissen nodig is.

Binnen de niet-Amerikaanse ondernemingen zal vooral de nadruk liggen op het voldoen aan de SOXA 404-verklaring. In de komende jaren zal er meer ruimte moeten zijn om de echte resultaten van interne beheersingsmaatregelen te zien, namelijk door het afnemen van onregelmatigheden, het verminderen van operationele slordigheden en een betere kwaliteit van diensten. Dit zal met name optreden bij ondernemingen waar gemotiveerd wordt gewerkt aan aantoonbare procesverbeteringen.

Dit zijn de lessen die uit het Controllers Leadership Research zijn getrokken:

- open de portemonnee: accepteer de kosten van duurzame compliance;
- let op de communicatie: communiceer niet dat u geen gebreken verwacht, dit kan leiden tot vrees en het onderdrukken van falende interne beheersingsmaatregelen;
- moedig het vroegtijdig identificeren van interne beheersingsproblemen aan;
- investeer in compliance gerelateerde managementprogramma's;
- ontwikkel de capaciteiten om veranderingen in de organisatieprocessen te ondersteunen;
- stuur op controledoelen: richt u op het duidelijk communiceren met en instrueren van proceseigenaren, zodat de proceseigenaren in staat zijn en de verantwoordelijkheid nemen om de SOXA-producten tijdig op te leveren en het herstel van gebreken in de interne beheersing.

## 7 Samenvatting en conclusies

In dit artikel zijn de eerste praktijkervaringen met SOXA beschreven. Enerzijds vanuit een lokaal SOXA office binnen ABN AMRO. Hier zijn de verschillende fasen en de wijze waarop de controlemaatregelen worden gedocumenteerd beschreven. Naast de control templates waarin de controlemaatregelen per proces worden vastgelegd, zijn de vragenlijsten met betrekking tot de controleomgeving van belang. Zowel voor de control templates als voor de vragenlijsten is het bewijsmateriaal van belang. Corporate values zijn bijvoorbeeld gedefinieerd, maar of er ook volgens de corporate values wordt gehandeld is heel moeilijk vast te stellen. Daarnaast zijn de SOXA-ervaringen binnen een dochter ABN AMRO Mellon beschreven. De grote uitdagingen liggen met name in de overgang van een projectorganisatie naar de bestaande organisatie, de integratie van SOXA in andere compliance frameworks en de betrokkenheid van de proceseigenaren.

Vervolgens is een aantal Amerikaanse SOXA 404 ervaringen beschreven. Allereerst is aangegeven hoeveel ondernemingen een materieel gebrek in de interne controle rapporteerden en wat de gevolgen hiervan waren op de beurskoers. Verder zijn de soorten materiële gebreken in de IC (Interne Controle) aangegeven. De materiële gebreken werden met name veroorzaakt door financiële processen en procedures (43%). Het Financial Statement Closing proces is dan ook de belangrijkste template.

De kosten van compliance als gevolg van SOXA 404 zijn enorm

gestegen. Over de hele linie is er sprake van een forse toename, waarbij de piek in de stijging van audituren voor ondernemingen met 5 tot 10 miljard dollar omzet extra opvalt.

Ook de controllers zullen meer tijd besteden aan controls, compliance enzovoort. Een vergelijking in de tijdsbesteding aan kernactiviteiten van de controllers in 2004 versus 2003 laat een verschuiving zien. De tijdsbesteding aan beheersingsmaatregelen, compliance en externe rapportages stijgt met 41%, terwijl de tijdsbesteding aan intern advies, budgettering en planning en managementrapportage met 22% daalt. De rol van de toezichthouder is ook veranderd: de Securities Exchange Commission en de PCAOB zullen meer tanden tonen.

Tot slot werd op de toekomst ingegaan. De belangrijkste initiatieven zullen zijn:

1. standaardiseren van documentatie en test procedures;
2. trainen van het finance personeel op SOXA issues;
3. het verminderen van het aantal kerncontroles;
4. trainen van personeel bij de bedrijfsonderdelen op SOXA issues;
5. het herdefiniëren van taken en verantwoordelijkheden voor 302 en 404.

Een volledige evaluatie van de SOXA initiatieven is nog niet mogelijk omdat 2006 het eerste jaar is dat niet-Amerikaanse ondernemingen aan de SOXA 404-verklaring moeten voldoen.

Prioriteit bij de niet-Amerikaanse ondernemingen ligt dit jaar vooral bij het voldoen aan SOXA om de vereiste SOXA 404-verklaring te kunnen ondertekenen. In de komende jaren zal de aandacht meer moeten liggen bij het verminderen van operationele slordigheden, betere kwaliteit van diensten enzovoort.

## 8 Literatuurlijst

Kaptein, M., R. Rozekrans en R. de Groot, 'Integriteit als auditobject', *Maandblad voor Accountants en Bedrijfseconomen*, oktober 2005.

Nimwegen, H. van en F. H. 'Spits, Corporate Governance en business controls', *Handboek Management Accounting*, december 2003.

Tackett, J. A., F. Wolf en G. Claypool, 'Practice Forum: Internal control under Sarbanes Oxley: a critical examination', *Managerial Auditing Journal*, Vol. 21, No. 3, 2006-06-02.

Controllers Leadership Research.

Voor de richtlijnen van de SEC wordt verwezen naar:

[www.sec.org](http://www.sec.org).

Voor de Form 20F en het jaarverslag van ABN AMRO wordt verwezen naar: [www.abnamro.com](http://www.abnamro.com).

Committee of Sponsoring Organizations of the Treadway Commission, Internal Control - Integrated Framework - Executive summary, AICPA, 1994.

Committee of Sponsoring Organizations of the Treadway Commission, Internal Control - Integrated Framework - Evaluation tools, AICPA, 1994.

SEC, Sarbanes-Oxley Act of 2002, 2002.

