J. Oosterhuis - Snippe
Belastingdienst Amsterdam

Sarbanes Oxley: Doel en Middel in Onbalans?

De implementatie van sectie 404 en de rol van informatietechnologie

Sarbanes Oxley: Doel en Middel in Onbalans?

De implementatie van sectie 404 en de rol van informatietechnologie

J. Oosterhuis - Snippe
Belastingdienst Amsterdam
Amsterdam, mei 2009

Samenvatting

In dit literatuuronderzoek heb ik mij de volgende centrale vraag gesteld: '*Heeft IT bijgedragen aan een transparante financiële verslaglegging waardoor het vertrouwen van investeerders wordt hersteld*'. Na diverse schandalen als bijvoorbeeld Enron en Ahold is de Sarbanes Oxley Act verplicht gesteld, met als ultiem doel het herstellen van vertrouwen van investeerders. Vanuit mijn vakgebied ben ik geïnteresseerd in de rol van IT hierin. Deze centrale vraag heb ik proberen te beantwoorden vanuit het analyseren van in de vakliteratuur beschreven gevolgen en de impact van de implementatie van de Sarbanes Oxley Act. Dit kwalitatief ingestoken onderzoek heeft niet geleid tot directe antwoorden. Het middel, sectie 404 'management assessment of internal controls', heeft door de huidige crisis niet geleid tot het doel, maatschappelijk vertrouwen. De ongrijpbaarheid van *vertrouwen* leidt er toe dat het doel en het middel van SOX in onbalans zijn; dat SOX niet dát oplevert waaruit investeerders vertrouwen krijgen. Wel is het zo dat op basis van mijn onderzoek effecten vanuit de Sarbanes Oxley Act te identificeren zijn die al dan niet direct betrekking hebben op IT. Dit betreffen voornamelijk het verbeteren van het systeem van interne controle (waar IT gebaseerde controlemaatregelen en algemene IT beheersmaatregelen een onderdeel van vormen); het versterken van IT kennis binnen het audit committee; het budget voor IT vormt geen belemmerende factor; de CIO vervult een dubbelrol doordat hij opschuift naar de CFO en aan belang wint, maar toch niet beslissingsbevoegd is.

Inhoudsopgave

Voorwoord

In het kader van de afronding van de postdoctorale opleiding 'EDP audit' aan de Vrije Universiteit van Amsterdam dient een scriptie geschreven te worden, waarin vanuit een wetenschappelijk oogpunt een onderwerp vanuit, of wat raakt aan, het EDP audit vakgebied, nader wordt onderzocht.

Vanuit mijn werkveld binnen de EDP (verder IT) audit groep van PricewaterhouseCoopers, genaamd System en Process Assurance, kwam ik in aanraking met de Sarbanes Oxley Act. De vele commentaren, al dan niet positief, hebben mijn interesse gewekt. Nu om en nabij zes jaar na aanname van de wet in de Verenigde Staten van Amerika zijn de 'foreign registrants' verplicht om te voldoen aan de eisen gesteld in de Sarbanes Oxley Act. Een belangrijke vraag voor mij was: zijn de doelstellingen en de uitgesproken hoge verwachtingen van deze wetgeving daadwerkelijk bewaarheid? Gezien vanuit sommige commentaren uit mijn werkomgeving lijkt dit niet het geval te zijn. Als we kijken naar de huidige economische toestand lijkt er van vermeerderd investeerders vertrouwen helemaal geen sprake.

De afronding van dit stuk, hoewel niet minder interessant om mee bezig te zijn, heeft langer op zich laten wachten dan mij welgevallig is. Ik ben dan ook zeer blij met het geduld dat vanuit de opleiding en vanuit mijn werkgever is betoond. Dankbaar ben ik voor de kritische commentaren. Een speciaal dankwoord aan mijn familieleden die toch steeds geïnteresseerd waren in mijn vordering in afronding van deze opleiding. Dit heeft motiverend gewerkt. Tot slot een dankwoord aan Pim, mijn echtgenoot, voor het onvermoeid motiveren en meelezen.

Amsterdam, mei 2009

Inge Oosterhuis-Snippe

1. Inleiding

Binnen organisaties wordt de verwerking van administratieve processen veelal uitgevoerd met behulp van informatiesystemen. Door deze toegenomen automatiseringsgraad kan de accountant onvoldoende zekerheid over de getrouwheid van financiële verslaglegging verkrijgen, wanneer hij alleen gebruik maakt van de traditionele controlemethodieken. Dit wordt mede veroorzaakt doordat kennis en ervaring die accountants hebben op het gebied van bedrijfseconomie en administratieve organisatie, onvoldoende is voor het doorgronden van informatiesystemen en de impact hiervan op de administratieve organisatie. De accountant dient hiertoe experts in te schakelen, die opereren op het snijvlak van informatietechnologie (IT) en processen. Zeker sinds het laatste decennium wordt dit ook onderkend en wordt door accountantskantoren expertise op het gebied van IT -auditing binnengehaald voor controle- en beoordelingsopdrachten.

Een andere ontwikkeling is de groeiende aandacht voor financiële verslaglegging in de afgelopen jaren, voornamelijk de aandacht voor de transparantie van de totstandkoming van de financiële cijfers. Deze toegenomen aandacht voor 'transparantie' wordt niet in de laatste plaats veroorzaakt door een aantal schandalen als bijvoorbeeld Enron (2001) en Ahold. Het antwoord vanuit de Verenigde Staten van Amerika op deze schandalen is de Sarbanes Oxley Act. Deze wet heeft als ambitieuze doelstelling 'to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws and for other purposes'. Deze wet streeft kortom naar transparante financiële verslaglegging.

In veel literatuur komt de hierboven genoemde doelstelling 'het herstellen van het vertrouwen van investeerders' door transparante financiële verslaglegging terug (bijvoorbeeld Hoffman, 2005). Uit een door PricewaterhouseCoopers uitgevoerd onderzoek (McClenahen, 2003) blijkt dat een derde van de destijds ondervraagde senior managers van multinationale organisaties verwachten dat het vertrouwen van investeerders in kapitaalmarkten hersteld zou worden door de Sarbanes Oxley Act. Echter, in datzelfde onderzoek geeft de meerderheid van de 'executives' aan dat zij niet verwachten dat deze wetgeving daadwerkelijk zal ondersteunen bij de inspanningen van hun organisaties om (toegevoegde) waarde voor aandeelhouders te verhogen. Van de leidinggevenden verwacht 32% dat de wet een positieve invloed zal hebben, 6% verwacht een negatieve impact en 6% weet het niet zeker (McClenahen, 2003). Dit geeft aan dat de verwachtingen van leidinggevenden of deze wetgeving zal voldoen aan haar ambitieuze doelstellingen op dat moment sterk uiteenliepen. Op dit moment kan gesteld worden de Sarbanes Oxley Act in ieder geval geen nieuwe financiële schandalen heeft kunnen voorkomen. Een snelle conclusie is dat het maatschappelijk vertrouwen ondanks deze wet wederom geschokt is. Destijds Enron, Ahold, WorldCom, Parmalat, nu hebben we Merill Lynch, Credit Suisse, Madoff, enzovoort.

Enerzijds zien we de groeiende complexiteit door de steeds groter wordende rol van systemen (een veelheid aan systemen en veelheid aan koppelingen tussen de systemen) en anderzijds is er de groeiende vraag naar transparante verslaglegging. Ook na recente schandalen klonk opnieuw een roep om strengere regels en om meer transparantie (zie voor de relatie schandalen en regelgeving onder andere Paape 2008). Hoe verhouden zich deze twee ontwikkelingen tot elkaar? Hoe of waar ligt de relatie tussen IT en financiële verslaglegging? Dit bespreek ik aan de hand van de Sarbanes Oxley Act. Deze wetgeving is verguisd (hier kom ik later op terug) maar nog steeds actueel. Niet alleen omdat bedrijven die aan de Amerikaanse beurs zijn genoteerd hier nog steeds aan moeten voldoen, maar ook omdat met deze wet de interne controle wederom op de kaart is gezet[1]. Interne controle an

[1] De aandacht voor interne controle is niet iets wat bij implementatie van de Sarbanes Oxley wet (2002) is ontstaan. Binnen diverse Europese landen is deze aandacht er als sinds jaar en dag. In Nederland kennen we de commissie Peters (1997), Tabaksblat (2003) en de monitoring commissie Frijns eind 2003). Deze commissie Frijns is ingericht om naleving van Tabaksblat te monitoren. Zo kent het Verenigd Koningkrijk (VK) de Cadbury Code (1992) met de oprichting van de Joint Working Group (JWT) om tot eenduidige criteria te komen om de ffectiviteit te beoordelen, om vervolgens te rapporteren en voor de accountant om de rapportage te controleren. Later in 1999 is de Combined Code ontstaan. Ook binnen de Europese Unie is aandacht voor interne controle bijvoorbeeld door de Europese federatie van accountants, die in 2005 de verschillende systemen van risicomanagement en interne beheersing hebben vergeleken binnen de Europese Unie. Meestal is de reikwijdte van de verschillende codes (VK, NL, EU) en de wet (US SOX) financieel. Behalve de Combined Code deze richt zich ook op operationeel

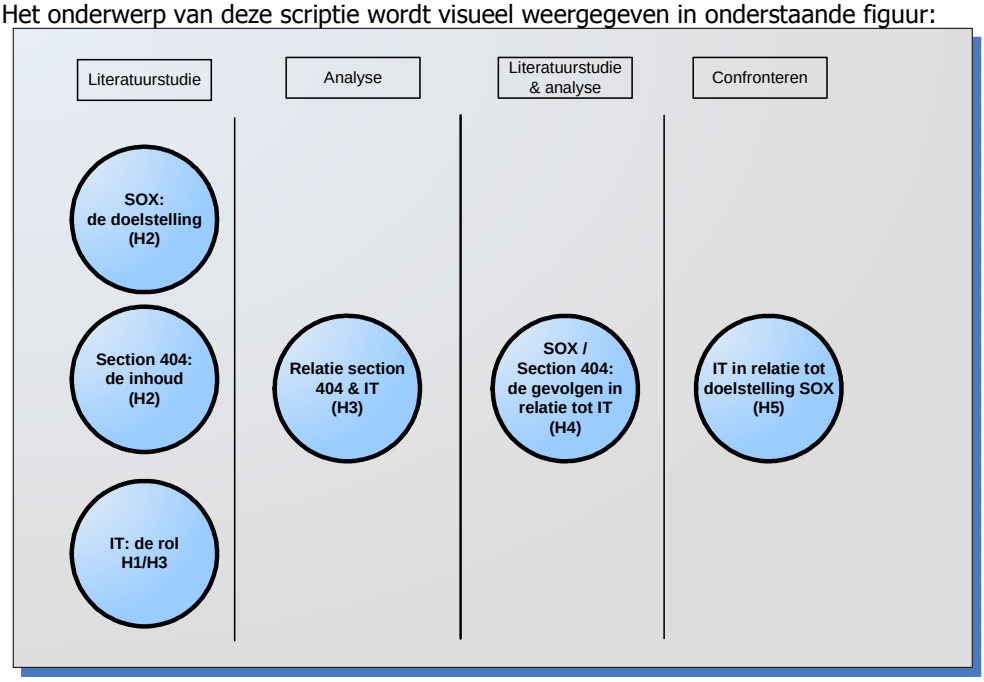
sich heeft anno 2009 niet ingeboet aan actualiteit. Denk hierbij aan het horizontaal toezicht waar de Nederlandse belastingdienst sinds een aantal jaren actief mee bezig is. De kerngedachte is dat de belastingdienst wil steunen op interne controle (ten aanzien van fiscaliteit) van een bedrijf zelf. Dit kan ook gaan over 'in control statements' die op basis van de Sarbanes Oxley Act worden afgegeven.

De vraag die ik centraal stel is hoe informatietechnologie een rol speelt in het behalen van de doelstelling van de Sarbanes Oxley Act. Ofwel: '*Heeft IT bijgedragen aan een transparante financiële verslaglegging waardoor het vertrouwen van investeerders wordt hersteld.*'

Uiteindelijk is de aanname van de wet dat transparante financiële verslaglegging het vertrouwen van investeerders herstelt. Deze aanname neem ik voor dit moment als een gegeven aan.

De relatie van informatietechnologie met de Sarbanes Oxley Act bevindt zich in de interne controle, deze laatste wordt met name zichtbaar in sectie 404 van de wet. Overigens wordt in de wet zelf niet gerept over informatietechnologie (IT) of de rol van IT.

Het onderwerp van deze scriptie wordt visueel weergegeven in onderstaande figuur:



Figuur 01: Onderzoeksmodel

In hoofdstuk 2 wordt allereerst een omschrijving gegeven van de Sarbanes Oxley Act en haar implicaties. In dit hoofdstuk wordt tevens de doelstelling weergegeven en wordt er ingegaan op de inhoud van sectie 404, als onderdeel van de Sarbanes Oxley Act.
In hoofdstuk 3 wordt beschreven wat de relatie is tussen sectie 404 en IT. Het gaat er hierbij om dat IT geen expliciete plaats inneemt in deze wet, maar dat IT weldegelijk een rol speelt bij de gehele implementatie van de Sarbanes Oxley Act. In dit hoofdstuk zal gedefinieerd worden hoe IT en de Sarbanes Oxley Act elkaar raken en beïnvloeden. Hierin wordt de relevantie van de centrale vraag beargumenteerd.
In hoofdstuk 4 worden de gevolgen van de implementatie van de Sarbanes Oxley Act en sectie 404 benoemd. Op basis van een literatuurstudie worden deze gevolgen geïdentificeerd en omschreven. Per beschreven gevolg zal de IT component belicht worden. Hierbij heb ik de aanname gedaan dat op

---

en naleving van wet- en regelgeving. SOX en Frijns kennen een verklaring van de effectiviteit. De Frijns en de Combined Code vragen om een beschrijving van de effectiviteit op financieel, operationeel en op naleving van wet- en regelgeving. Bij de diverse codes gangbaar binnen de EU is de rol van de accountant meer indirect (bijvoorbeeld jaarverslag mag niet strijdig zijn met opgedane kennis in kader van de jaarrekeningcontrole) dan bij US SOX waarbij de accountant daadwerkelijk controleert (Leeuwen e.a., 2007)

basis van de gevolgen van deze Sarbanes Oxley Act bepaald kan worden of het 'beoogde' doel van deze wet is behaald.
In hoofdstuk 5 vindt de confrontatie plaats tussen de centrale vraag van deze scriptie en de resultaten van de literatuurstudie en analyses. Hierbij geef ik een antwoord op de centrale vraag: '*Heeft IT bijgedragen aan een transparante financiële verslaglegging waardoor het vertrouwen van investeerders wordt hersteld.'* Bij mijn analyses heb ik, waar mogelijk en relevant, geput uit mijn ervaringen opgedaan als IT auditor bij PricewaterhouseCoopers en de Belastingdienst Amsterdam.

2. Doel en middel van de Sarbanes-Oxley Act of 2002

In dit hoofdstuk wordt ingegaan op de oorsprong van de Sarbanes-Oxley Act, het doel en de gebruikte middelen, met specifieke aandacht voor sectie 404.

2.1 Oorsprong en doel

De 'Sarbanes-Oxley Act of 2002[2]' en in de volksmond verworden tot 'SOX', 'SOA' of 'Sarbox' is een wet 'to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws and for other purposes'[3]. Deze wet is aangenomen op 30 juli 2002. De wet dankt zijn naamgeving aan de belangrijkste sponsors, namelijk senator Paul Sarbanes en vertegenwoordiger Michael G. Oxley.

Deze wet raakt alle aan de Amerikaanse beurs genoteerde bedrijven, zowel Amerikaanse als buitenlandse. Verplichtingen voortkomend uit deze wet raken dus óók de dochterondernemingen van aan de Amerikaanse beurs genoteerde bedrijven. Voor Amerikaanse bedrijven werd de wet al van kracht bij de eerste jaarlijkse aandeelhoudersvergadering na aanname van de wet. 'Foreign registrants' dienden aan deze wet te voldoen vanaf het boekjaar eindigend op of na 15 juli 2005.

Met de Sarbanes-Oxley Act (verder SOX) als middel wil de Amerikaanse overheid waarborgen dat het management betrouwbare financiële cijfers publiceert. Hierbij concentreert de wet zich op de interne controle over deze financiële cijfers. Dit dient te leiden tot het terugwinnen van het vertrouwen van de diverse belanghebbenden, zoals bijvoorbeeld aandeelhouders maar ook de maatschappij als geheel. Niet in de laatste plaats doordat een goede interne controle de kans op fraude zou verkleinen (PCAOB release, 2004).

SOX is een directe reactie vanuit de Amerikaanse overheid op bedrijfs- en accounting schandalen (Anonymous, 2003). Met deze wet wil men ervoor zorgen dat 'company executives, directors, and independent auditors take specific actions to achieve greater corporate accountability and transparency.' Met als doel het versterken van corporate governance en het herstellen van het vertrouwen van investeerders.

2.2 Middel

De wet is verdeeld in elf titels[4], waarvan de belangrijkste voor mijn onderwerp titel 4 'Enhanced Financial Disclosures is.

Om een antwoord te geven op de centrale vraag welke rol IT speelt bij een transparante financiële verslaglegging, dient de vraag gesteld te worden waar de relatie met IT in deze wet te vinden is. In hoofdstuk 3 zal hier uitvoeriger op ingegaan worden. De relatie met IT ligt in de veelbesproken sectie 404 'Management assessment of internal controls'.

Voor de uitvoering van SOX is de Public Company Accounting Oversight Board (PCAOB) opgericht, zij is geautoriseerd om controle ('audit') standaarden uit te geven voor de aan de Amerikaanse beurs geregistreerde bedrijven. Deze standaarden vormen de handvatten voor de auditors waarmee zij tot een opinie kunnen komen over onder andere de interne controle van de financiële verslaglegging van een bedrijf (Drexler, 2005, p16). Ofwel richtlijnen hoe om te gaan met sectie 404. Hieronder volgt een korte weergave van de inhoud van deze sectie.

---

[2] De 'Public law 107-204 enacted by the Senate and House of Representatives of the United states of America in Congress assembled'.

[3] Dit is overgenomen vanuit de tekst van de Sarbanes-Oxley Act of 2002. Zie voor de volledige verwijzing de literatuurlijst.

[4] De elf titels van de Sarbanes-Oxley Act zijn: 'Public Company Accounting Oversight Board', 'Auditor Independence, 'Corporate Responsiblitiy, 'Enhanced Financial Disclosures', 'Analyst Conflict of Interest', 'Commission resources and Authority', 'Studies and Reports', 'Corporate and Criminal Fraud Accountability', 'White Collar Crime Penalty Enhancements', 'Corporate Tax Returns' en 'Corporate Fraud and Accountability'

2.3 Sectie 404 'Management Assessment of internal controls'

Titel 4 'Enhanced Financial Disclosures' is gericht op het juist, tijdig en volledig openbaar maken van financiële rapportages. Nadrukkelijk worden ook eisen gesteld ten aanzien van het formaat: 'plain English'. Deze rapportages dienen allereerst te voldoen aan de geldende wet- en regelgeving en aanvullende richtlijnen. Aanvullend wordt geëist van het management dat verantwoordelijk is voor het publiek maken van deze gegevens, dat dit management (financieel) onafhankelijk (zie bijlage 1 sectie 402) is en zich onderwerpt aan een gedragscode en zich daadwerkelijk verantwoordelijk maakt voor deze gegevens. Er zijn verschillende organen verantwoordelijk voor review van deze financiële rapportages. Dit betreft allereerst het management zelf, vervolgens het audit committee[5] en als derde een auditor (accountant)[6]. Tot slot heeft de toezichthouder het recht om deze financiële verslaglegging te beoordelen.

De inhoud van sectie 404: 'Management assessment of internal controls':
'(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—
(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

> *(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection*
> *(a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.'*

Voor een volledig overzicht van de wettekst van titel 4 verwijs ik naar bijlage 1.

Sectie 404 Management assessment of internal controls bestaat uit twee componenten:
- Het management is verantwoordelijk voor het inrichten en onderhouden van een adequate interne controlestructuur inclusief procedures voor financiële rapportagestromen.
- Het management dient een beoordeling uit te voeren naar de werking (de effectiviteit) van haar eigen systeem van interne controle en procedures voor financiële rapportages. Deze managementbeoordeling dient te worden geëvalueerd door een auditor (externe accountant).

De CEO en CFO dienen periodiek (per jaar en per kwartaal) een rapport ten aanzien van ondermeer de interne controlemaatregelen dat door hun organisatie opgeleverd wordt, te certificeren ofwel de eerder genoemde managementbeoordeling te ondertekenen. Daarin geven ze aan dat zij verantwoordelijk zijn voor het inrichten en onderhouden van de interne controlemaatregelen, daarnaast dat deze controlemaatregelen zo zijn ingericht dat hieruit alle materiële financiële informatie kan worden gehaald, dat zij de effectiviteit van de controlemaatregelen zijn nagegaan en dat zij hierover conclusies hebben gevormd en deze in een rapport hebben neergeschreven. In het rapport dienen de CEO en CFO te indiceren welke significante wijzigingen zich hebben voorgedaan of andere factoren die deze interne controlemaatregelen kunnen beïnvloeden na de datum dat deze controlemaatregelen zijn geëvalueerd. Ook de correctieve acties welke eventueel uitgevoerd zijn om materiële zwakheden teniet te doen, dienen benoemd te worden (Busco, 2005 p. 39).

[5] Sarbanes Oxley Act, 2002: Audit committee.--The term "audit committee" means-- (A) a committee (or equivalent body) established by and amongst the board of directors of an issuer for the purpose of overseeing the accounting and financial reporting processes of the issuer and audits of the financial statements of the issuer; and (B) if no such committee exists with respect to an issuer, the entire board of directors of the issuer.

[6] De Sarbanes Oxley Act 2002, spreekt van een 'registered public accounting firm'.

Het management moet in het kader van sectie 404 niet gecorrigeerde deficiënties of materiële zwakheden rapporteren zowel aan het audit committee als aan de auditor en uiteindelijk aan de SEC[7]. Het is het management van de organisatie niet toegestaan te concluderen dat interne controlemaatregelen met betrekking tot financiële verslaglegging effectief zijn indien er een of meerdere materiële zwakheden zijn geconstateerd gedurende de managementevaluatie (Gupta et al, 2006, p31).

De wet wil hiermee het management als het ware dwingen haar verantwoordelijkheid te nemen. Niet alleen cijfers evalueren in de rapportages en deze vervolgens ondertekenen maar kennis nemen van het proces wat leidt tot die financiële cijfers. Sterker nog het management wordt 'gedwongen' controlemaatregelen in het proces te evalueren. In de praktijk is het binnen grote organisaties, waar het hoger management niet direct betrokken is bij de primaire processen een complexe klus om dit soort beoordelingen uit te voeren. De verschillende managementlagen, waar de financiële verslagleggingprocessen als het waren doorsnijdingen van vormen en het trapsgewijs, per managementlaag, vertalen van de impact van deficiënties op het niveau van controlemaatregel naar de financiële verslaglegging van een heel bedrijf, blijkt lastig.

[7] Paragraaf 404 bepaalt dat elke beursgenoteerde onderneming verplicht is om in haar bij de SEC gedeponeerde jaarverslag een aparte rapportage op te nemen over de interne procedures die betrekking hebben op de financiële verslaggeving, onder meer de effectiviteit van de procedures moet worden geëvalueerd. De verklaring moet worden ondertekend door de bestuursvoorzitter en de chief financial officer van de onderneming. Paragraaf 404 bepaalt voorts dat de accountant deze evaluatie moet controleren en onderschrijven (http://www.commissiecorporategovernance.nl/news/item/SEC_publiceert_guidance_bij_opstellen_internal_control_statement/105?mid=100040).

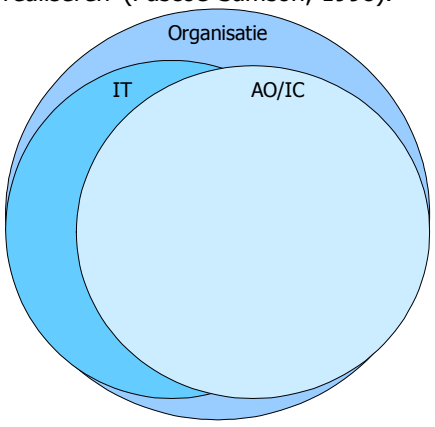
3. Sarbanes Oxley Act en IT

In de inleiding is al benoemd dat in de wet zelf geen expliciete plaats wordt ingenomen door IT. Gezien het belang van IT voor veel organisaties is het evident dat SOX, wat zich sterk richt op interne controle, en IT raakvlakken heeft. In dit hoofdstuk wordt ingegaan op dit speelveld. Overigens is het zo dat de PCAOB wel expliciet aandacht besteedt aan de rol van IT.

3.1 Sectie 404 geplaatst in de organisatie

Om een goed begrip te krijgen van de rol van IT binnen SOX, is in figuur 2 sectie 404 geplaatst in haar context, namelijk de organisatie welke moet voldoen aan de 'Sarbanes Oxley Act'.

Vanuit diverse disciplines kunnen verschillende definities van een organisatie worden gegeven. Een socioloog zal immers een andere visie hebben op een organisatie dan een bedrijfseconoom, de eerste zal zich bijvoorbeeld meer toespitsen op de gedragspatronen van mensen. Voor het hier beoogde doel wordt uitgegaan van een meer algemene bedrijfseconomische definitie van een organisatie: '*Een organisatie is een herkenbare eenheid, waarin mensen op een gecoördineerde wijze en met behulp van technische en financiële middelen activiteiten uitvoeren, ten einde gemeenschappelijke doelen te realiseren'* (Pascoe-Samson, 1998).



Figuur 02-1: Sectie 404 en de organisatie

De buitenste cirkel in figuur 02-1 wordt gevormd door de organisatie. Een deel van deze organisatie bestaat uit IT systemen of entiteiten die gebruik maken van IT systemen. Deze entiteiten kunnen breed worden ingevuld. Dit kan een specifieke afdeling zijn, bijvoorbeeld de afdeling Facturatie, die als geheel gebruikmaakt van een set aan systemen. Dit kan ook één persoon zijn bijvoorbeeld de medewerker Facturatie, die facturen boekt in het ERP[8] pakket. Tot slot kan dit het systeem zelf zijn, dat middels interfaces volledig geautomatiseerd gebruik maakt van andere systemen.

Administratieve organisatie en interne controle (AO/IC) vormen een cirkel binnen de organisatie. AO[9] heeft betrekking op alle activiteiten die betrekking hebben op het verzamelen, vastleggen en verwerken van gegevens, het verstrekken van gerichte informatie ten behoeve van het besturen, het doen functioneren en beheersen van een organisatie evenals het afleggen van verantwoording. AO is bedoeld voor het organiseren van de informatiehuishouding van een organisatie en het waarborgen van de betrouwbaarheid daarvan. Een definitie van IC[10] is het proces dat gericht is op het verkrijgen van een redelijke mate van zekerheid over het bereiken van doelstellingen op gebied van:

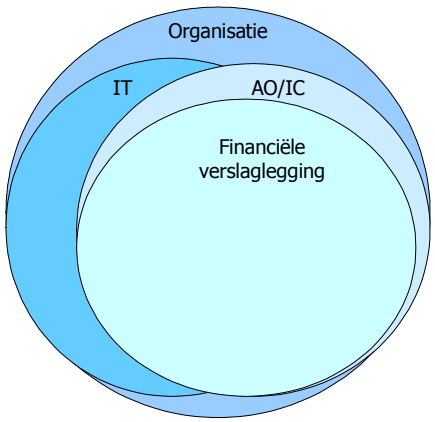
- De effectiviteit en efficiency van de bedrijfsprocessen;
- De betrouwbaarheid van de financiële informatieverzorging;
- De naleving van relevante wet- en regelgeving, beleidsrichtlijnen en procedures;
- Het bewaken van activa of waarden.

[8] ERP Enterprise resource planning: geïntegreerde geautomatiseerde afhandeling van de logistieke, administratieve en financiele bedrijfsprocessen (naar: Gijs Houtzagers, Holland Casino, Eramus gastcollege).
[9] Bron: http://www.agf.nl/nieuwsbericht_detail.asp?id=17599
[10] Bron: wikipedia

De definitie van interne controle zoals door COSO[11] gehanteerd, is beperkter en zegt niets over 'het bewaken van activa of waarden' (Leeuwen, 2007).

Interne controle wordt namens of door de leiding uitgevoerd. AO/IC maakt daarmee in theorie een gecontroleerde bedrijfsvoering mogelijk. In figuur 02-1 is door de overlappende cirkels van IT en AO/IC aangegeven, dat AO/IC gebruik maakt van IT. Zie ook het eerder gegeven voorbeeld ten aanzien van facturatie. Een deel van de IT valt buiten de AO/IC, dit kunnen spreadsheet applicaties (Excel etc.) zijn die medewerkers gebruiken, maar die geen onderdeel vormen van de AO/IC. Een voorbeeld is een medewerker facturatie die naast de registratie van facturen in het ERP pakket ook in Excel een lijst bijhoud ter eigen controle. De registratie in het ERP pakket is voor de AO/IC primair van belang terwijl de lijst van de medewerker dat niet is.

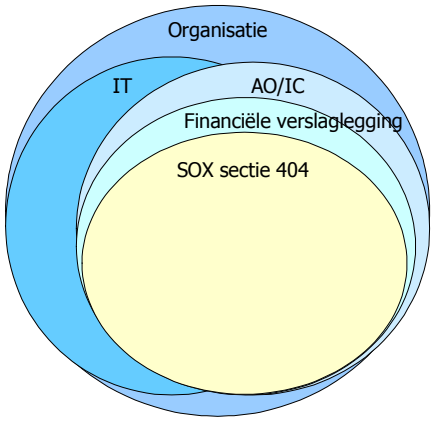
Een opmerking ten aanzien van de gehanteerde cirkels, het is een visualisatie, de grootte geeft niet een werkelijke situatie of een wetenschappelijk onderbouwde situatie weer.



Figuur 02-2: Sectie 404 en de organisatie

Financiële verslagleggingprocessen (zie figuur 02-2) waarover SOX eisen stelt, vormen als het ware een product van de cirkels IT Systemen en AO/IC. Immers financiële rapportages, als resultante van de financiële verslagleggingprocessen, kunnen in diverse mogelijke combinaties gebruik maken van IT en AO/IC. Hiermee wordt inzichtelijk dat SOX gebruik maakt van IT, en dat IT dus een onderdeel vormt van de scope van SOX.

[11] Committee of Sponsoring Organizations of the Treadway Commission (COSO), is a U.S. private-sector initiative, formed in 1985. Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence. COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems. COSO is sponsored and funded by 5 main professional accounting associations and institutes; American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives Institute (FEI), The Institute of Internal Auditors (IIA) and The Institute of Management Accountants (IMA) (Beschrijving overgenomen van nl.wikipedia.org).



Figuur 02-3: Sectie 404 en de organisatie

In figuur 02-3 wordt sectie 404 weergegeven als de kleinste kern binnen de organisatie en bijna overlappend met de cirkel financiële verslagleggingprocessen. Deze cirkel visualiseert die controlemaatregelen (al dan niet gebruikmakend van IT) die opgenomen zijn in een interne controlestructuur (AO/IC). Deze controlemaatregelen zijn relevant voor die financiële verslagleggingprocessen welke resulteren tot financiële rapportages, bijvoorbeeld de jaarrekening.

Zoals in hoofdstuk 2 toegelicht bestaat 404 uit twee delen. In het eerste deel komen impliciet de IT-systemen voor de controle aan de orde: '*Het management is verantwoordelijk voor het inrichten en onderhouden van een adequate interne controlestructuur inclusief procedures voor financiële rapportagestromen'.* In figuur 02-3 dient ten behoeve van SOX sectie 404 het management zich een oordeel te vormen over de kleinste kern. Verantwoordelijkheden binnen deze interne controlestructuur kunnen over diverse managementlagen worden verdeeld. De IT manager zal een rol spelen ten aanzien van bijvoorbeeld algemene IT controlemaatregelen en de manager van de afdeling Facturatie zal verantwoordelijkheden hebben voor controlemaatregelen binnen het facturatieproces. Uiteindelijk zijn de CEO en de CFO verantwoordelijk voor het geheel.

Deze interne controlestructuur bestaat uit een veelheid en diversiteit aan controlemaatregelen. Hieronder wordt dit onderscheid gedefinieerd, om een beeld te geven van de mate waarin de verschillende soorten controlemaatregelen gebruik maken van IT.

3.2 Onderverdeling controlemaatregelen

Ten aanzien van interne controlemaatregelen kan onderscheid gemaakt worden naar diverse soorten controlemaatregelen. Dit geeft een verder inzicht in de rol van IT. Er kan onderscheid gemaakt worden naar vier soorten, namelijk handmatige ('manual'), applicatieve, geautomatiseerde en algemene IT beheersmaatregelen. Dit zijn alle 'harde' controlemaatregelen, ik ga hiermee impliciet voorbij aan een minstens zo belangrijke groep controlemaatregelen, de zogenaamde 'soft controls' of zachte controlemaatregelen. Dit betreft bijvoorbeeld de 'tone at the top' van een onderneming. COSO benoemt dit als belangrijk element. In mijn scriptie ga ik hier omwille van de scope niet verder op in.

Hieronder geef ik een korte invulling van de controlemaatregelen zoals ik deze hanteer voor deze scriptie:

- handmatige controlemaatregelen betreffen die categorie controlemaatregelen waarvoor geen gebruik wordt gemaakt van IT (applicaties, besturingssystemen, enzovoort). Een voorbeeld van zo'n handmatige controlemaatregel betreft het handmatig vergelijken van een bestelformulier met het overzicht van ontvangen goederen en de van de leverancier verkregen factuur;
- applicatieve controlemaatregelen betreffen controlemaatregelen waarbij gebruik gemaakt wordt van applicaties (IT), maar waarbij handmatige opvolging (vaak door de 'business') is vereist. Hierbij kan gedacht worden aan het uitvoeren van een trendanalyse op basis van een systeem gegenereerd rapport of het handmatig opvolgen van uitvallijsten welke ontstaan op basis van systeeminstellingen. Een voorbeeld voor de laatste is een uitvallijst bij het automatisch, vaak batchgewijs, genereren van facturen. Dit betreft bijvoorbeeld uitval op basis van minimale

afwijkingen ten opzichte van voorgaande facturen bij de betreffende klant. Deze uitval moet handmatig door medewerkers facturatie worden opgevolgd. Omwille van de scheiding tussen geautomatiseerde en gedeeltelijk geautomatiseerde controlemaatregelen zal ik de laatste 'applicatief' noemen.

- geautomatiseerde controlemaatregelen betreffen die controlemaatregelen waarbij geen menselijk ingrijpen plaatsvindt. Dit betreffen vaak door applicaties uitgevoerde calculaties. Bijvoorbeeld het automatisch berekenen van een factuurbedrag waarbij ingevoerde prijzen en kwantiteiten worden vermenigvuldigd.
- algemene IT beheersmaatregelen (ITGC's[12]), dit betreffen controlemaatregelen welke ingericht worden binnen een organisatie om het systeemlandschap te onderhouden en de continuïteit hiervan te waarborgen. ITGC's kunnen bestaan uit handmatige, applicatieve en geautomatiseerde controlemaatregelen in wisselende combinaties. Uiteraard afhankelijk van de organisatie. Een aantal belangrijke deelgebieden binnen de ITGC's zijn:
    a. Wijzigingenbeheer;
    b. Incident- en probleembeheer;
    c. Continuïteitsmanagement onder andere back-upmanagement en uitwijkfaciliteiten;
    d. Beveiligingsmanagement.

De handmatige ITGC's hebben ondermeer betrekking op het volgen van procedures. Bijvoorbeeld het afwerken van een checklist voor het in productie nemen van een wijziging als onderdeel van wijzigingenbeheer.

Zonder werkende ITGC's kan niet worden gesteund op de applicatieve en geautomatiseerde controlemaatregelen. De ITGC's vormen de basis voor de effectieve werking van deze controlemaatregelen. Een voorbeeld wordt gevormd door controlemaatregelen welke ingericht zijn op het gebied van wijzigingenbeheer. Indien er geen centrale registratie is en er geen onvoldoende impactanalyse wordt uitgevoerd op voorkomende wijzigingen, kan de organisatie niet zeker zijn dat haar applicatieve en geautomatiseerde controlemaatregelen nog steeds voldoen aan het beoogde doel. Immers deze controlemaatregel kan in dat geval onopgemerkt voor de business zijn gewijzigd en incorrect werken. Voor volledige invulling van de ITGC's wordt verwezen naar COBIT [7], deze systemen geven een mogelijke basis voor de invulling van controlemaatregelen op het gebied van ITGC.

Als het gaat om de betrouwbaarheid van deze maatregelen, betreffende correcte uitvoering en de kans op fouten, kan gesteld worden dat handmatige controlemaatregelen het meest foutgevoelig zijn en volledig geautomatiseerde het minst. Applicatieve controlemaatregelen vallen qua foutgevoeligheid hier tussenin. Deze verdeling is gebaseerd op de mate van menselijke ingrijpen dat nodig is om de controlemaatregel uit te voeren; meer menselijke handelingen geeft meer kans op fouten.

3.3 Impliciete eisen vanuit de wet

SOX stelt impliciet eisen aan de IT door middel van sectie 404. Impliciet omdat in deze wet het woord 'IT' of gerelateerde bewoordingen niet voorkomen. Niettemin leiden eisen op het gebied van transparantie en verklaarbaarheid, tot eisen ten aanzien van IT (Hoffman, 2005, p36).

De PCAOB[13] heeft in aanvulling op de wet en in ondersteuning ten aanzien van de uitvoering van SOX diverse richtlijnen uitgegeven waarin IT expliciet aan bod komt. Deze richtlijnen betreffen de zogenaamde audit standards, afgekort tot AS. Dat er binnen deze standaarden aandacht besteedt wordt aan IT volgt niet alleen logisch uit de in paragrafen 3.1 en 3.2 uitgelegde relatie tussen SOX en IT, maar volgt ook eenvoudigweg uit de ontwikkeling die al enkele decennia aan de gang is waarbij organisaties in steeds verdergaande mate worden ondersteund door informatietechnologie.

[12] ITGC staat voor IT General Controls, zie de definitielijst.

[13] Evalueren van interne controle, sectie 404. The Public Company Accounting Oversight Board (or PCAOB) (sometimes called "Peekaboo") is a private-sector, non-profit corporation created by the Sarbanes-Oxley Act, a 2002 United States federal law, to oversee the auditors of public companies. Its stated purpose is to 'protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports'. Although a private entity, the PCAOB has many government-like regulatory functions, making it in some ways similar to the private Self Regulatory Organizations (SROs) that regulate stock markets and other aspects of the financial markets in the United States. Noot; Taken van de PCAOB staan beschreven in sectie 101 van de Sarbanes Oxley Act.

Audit standards ten aanzien van sectie 404 geven aan dat een internal control framework dient te worden gehanteerd voor beoordeling van de effectiviteit; veelal wordt COSO door organisaties gebruikt als standaard. Belangrijk om te weten is dat dit governance framework niet verplicht is. Organisaties zijn vrij in het hanteren van willekeurig welk framework, echter de onderwerpen vanuit COSO dienen te worden geadresseerd, binnen het door de organisatie ingerichte interne controle systeem. In de praktijk blijkt vaak dat bovengenoemde framework (COSO) door de organisaties als standaard wordt overgenomen en geïmplementeerd.

3.4 IT kennis noodzakelijk bij SOX

De PCAOB geeft in haar 'audit standards' aan dat ITGC's meestal geen directe relatie hebben met financiële verslagleggingprocessen. De relatie tussen een proces als wijzigingenbeheer kan bijvoorbeeld niet één op één worden gerelateerd aan bepaalde financiële verslagen.

De PCAOB stelt in haar auditing standaarden dat alleen die ITGC's beoordeeld hoeven te worden waarbij deze relatie evident is. Dit betekent in de praktijk dat alleen ITGC's worden beoordeeld van applicaties welke van belang zijn voor financiële verslaglegging. Dit zou een beperking van de scope en werkzaamheden betekenen en daarmee een kostenbesparing (In hoofdstuk vier zal verder gesproken worden over het kosteneffect). Bij deze redenering van de PCAOB wordt naar mijn mening geen rekening gehouden met de algemene toepasbaarheid van ITGC's. ITGC's zijn namelijk processen welke meerdere applicaties en systemen omvatten. Om zo efficiënt en effectief mogelijk te zijn, zal er binnen organisaties naar gestreefd worden om centrale IT beheerprocessen in te richten, met bij voorkeur een overkoepelende procedure voor wijzigingen en incidenten. Dit is ook iets wat vanuit het IT audit vak wordt ondersteund, en deze aanbeveling zie ik in mijn praktijk regelmatig terugkeren. Het is dus maar de vraag in hoeverre deze uitspraak van de PCAOB daadwerkelijk tot een beperking van de scope leidt.

Bovenstaande geeft aan dat SOX niet alleen om actieve betrokkenheid van Finance vraagt maar ook om actieve betrokkenheid van IT en daarmee van de Chief Information Officers (CIO's). Daarnaast is betrokkenheid nodig van professionals die kunnen inschatten in hoeverre welke ITGC processen voor SOX in scope dienen te zijn. Deze professionals dienen het auditvak te kennen en dienen de impact van voorkomende bevindingen te kunnen schatten in relatie tot SOX. Voorgaande maakt het inschakelen van IT auditors relevant, zo niet noodzakelijk. Deze IT auditors kunnen vanuit de interne auditdienst worden ingeschakeld of vanuit een accountantskantoor. Deze professionals werken namelijk op het snijvlak van (bedrijfs) processen en IT, daarnaast zijn zij gewend om met de accountantscollega's de impact van bevindingen vanuit IT op de financiële verslaglegging te beoordelen.

Het zal, dat is ten minste mijn ervaring, niet vaak voorkomen dat bevindingen op het gebied van IT leiden tot uitzonderingen in de accountantsverklaring of tot een afkeurende verklaring. Dit is een gevolg van de controleaanpak die wordt gehanteerd. In het kader van een systeemgerichte controle wordt (zo veel mogelijk) gesteund op de interne controle van een organisatie. Indien dit niet of beperkt kan omdat bepaalde controlemaatregelen niet werken dan betekent dit dat een accountant aanvullende gegevensgerichte werkzaamheden dient uit te voeren. Dit mechanisme werkt ook door bij IT; wanneer niet gesteund kan worden op de ITGC's dan dient een andere controleaanpak te worden ontwikkeld.

4. Gevolgen van de Sarbanes Oxley Act

In dit hoofdstuk worden verschillende vanuit de vakliteratuur geïdentificeerde gevolgen van de SOX benoemd. Steeds zullen deze gevolgen gerelateerd worden aan de centrale vraagstelling van deze scriptie: '*Heeft IT bijgedragen aan een transparante financiële verslaglegging waardoor het vertrouwen van investeerders wordt hersteld.'* Ofwel geven de gevolgen van implementatie van SOX inzicht in de bijdrage van IT.

Deze geïdentificeerde gevolgen laten zich onderverdelen in interne, externe en kosten. Intern geeft aan of het binnen een organisatie speelt en extern of het van buitenaf effect heeft op de organisatie. Tot slot is bestaat er wisselwerking tussen de verschillende gevolgen. Bijvoorbeeld toegenomen activiteiten door het audit committee (paragraaf 4.4) houdt in dat hier budget voor dient te zijn en daarmee is het een kostenverhogend element (paragraaf 4.10). Vanzelfsprekend zullen niet alle geïdentificeerde gevolgen zich voordoen of hebben gedaan bij elke organisatie die met SOX bezig is.

Tot slot rest mij de opmerking dat ik deze gevolgen geïdentificeerd heb op basis van literatuuronderzoek. In de literatuur wordt bijna geen onderscheid gemaakt naar welk onderdeel van de wet nu welke gevolgen heeft. Hierover wordt vaak in algemene termen gesproken als gevolgen van SOX. Echter, in de praktijk zijn het vaak gevolgen van sectie 404 (302).

Externe gevolgen:

4.1 Onafhankelijkheidseisen vanuit SOX

Eisen ten aanzien van onafhankelijkheid worden door de Sarbanes Oxley Act op scherp gesteld. Hierbij worden een tweetal voorbeelden benoemd. Als eerste kan een accountant niet helpen bij het opstellen van interne controlemaatregelen en deze vervolgens zelf gaan reviewen (in het kader van sectie 404). Als tweede mag een accountant geen managementfuncties uitvoeren of managementbesluiten nemen (Drexler, 2005, p.17).
Indien een accountant non-audit[14] diensten verleend aan een organisatie welke dient te voldoen aan de Sarbanes Oxley Act zou hij bij contract akkoord moeten gaan om geen controlewerkzaamheden uit te voeren bij hetzelfde bedrijf. Dit betekent dat er een strengere scheiding komt tussen enerzijds advieswerkzaamheden en anderzijds controlewerkzaamheden. Drexler (2005, p.17) voorspelt hierin dat dit zal leiden tot accountantskantoren welke zich richten op één van beide diensten, advies óf controle.

In mijn dagelijkse praktijk neem ik inderdaad een scheiding waar tussen advieswerkzaamheden en controlewerkzaamheden. Afzonderlijke bedrijfsentiteiten van een (accountants)kantoor die zich bezig houden met danwel 'advies' danwel 'audit'. Maar in mijn praktijk zie ik niet de ontwikkeling dat een kantoor zich specifiek richt op 'advies' of 'audit'. De laatste tijd is naar mijn mening meer een tendens zichtbaar waarbij de grijze gebieden ten aanzien van onafhankelijkheid worden opgezocht. Binnen het accountantskantoor waar ik tot voor kort werkzaam ben geweest (er is geen reden aan te nemen dat overige accountantskantoren niet gelijksoortige programma's hebben) zijn risicomanagementprogramma's ingericht om na te gaan welke opdrachten aangenomen kunnen worden tegen welke risico's, ondermeer of de opdracht überhaupt uitgevoerd kan worden bij de betreffende organisatie. Dit kan dan bijvoorbeeld gaan om adviesopdrachten bij een auditklant. Dit geldt voor opdrachten op allerlei gebied en daarmee ook voor opdrachten die de IT of IT gerelateerde controlemaatregelen raken of betreffen. Inhoudelijk hebben de onafhankelijkheidseisen vanuit SOX geen directe relatie met IT en als zodanig kan er niet gesproken worden van een bijdrage van IT aan transparante financiële verslaglegging. Het is naar mijn mening wel zo dat deze eisen op een lager niveau een positieve invloed hebben op transparantie financiële verslaglegging. Immers wanneer eenzelfde persoon of entiteit zowel verantwoordelijk is voor het ontwerp van interne

[14] NON-AUDIT SERVICES or non-attest, term "non-audit services" means any professional services provided to an issuer by a registered public accounting firm, other than those provided to an issuer in connection with an audit or a review of the financial statements of an issuer. Uit de Sarbanes Oxley Act

controlemaatregelen als voor de beoordeling van de werking, dan creëer je 'blinde vlekken' met het risico dat deficiënties onopgemerkt blijven. Dit geldt overigens ook intern bij organisaties.

4.2 Negatieve invloed op fusies, overnames en beursnotatie

In een overzichtartikel uit 2004 geeft Koehn aan dat SOX een negatieve invloed heeft op fusies en overnames (van SOX plichtigen). Dit zou een gevolg zijn van de bezorgdheid van de managers bij de overname partij of zij verantwoordelijk gehouden kunnen worden voor de historie van de over te nemen partij. Dit betekent dat due diligence[15] onderzoeken langer duren en dat het tijdpad ten aanzien van te sluiten overeenkomsten langer wordt.

Daarnaast leiden de te maken kosten (zie ook paragraaf 4.10) om SOX compliant te zijn en te blijven tot het zich terugtrekken van (buitenlandse) bedrijven van de Amerikaanse beurs. Denk hierbij aan bedrijven als KPN. Organisaties analyseren of de te maken kosten voor SOX opwegen tegen de te genereren voordelen, wanneer de kosten te hoog worden en het perspectief van deze organisatie op de Amerikaanse markt niet rooskleurig is, kan dit leiden tot terugtrekking van de beurs (Leeuwen, 2007).

Deze geïdentificeerde gevolgen leiden niet direct tot inzichten op het gebied van interne controle, IT en het bereiken van transparante financiële verslaglegging.

Interne gevolgen:

4.3 Verbetering van het systeem van interne controle

Het begrip en kennis van interne controlesystemen binnen organisaties en bij medewerkers is verbeterd door de Sarbanes Oxley Act. Ho (2007, p5) geeft aan dat binnen organisaties de kennis is toegenomen als het gaat om hoe controlemaatregelen impact kunnen hebben op financiële risico's. Bijkomend effect ten aanzien van interne controlesystemen is de kwalitatief verbeterde documentatie van sleutel controlemaatregelen (en processen), toegenomen begrip van controlemaatregelen en aanwezige risico's, eenduidiger relatie van controlemaatregelen met de financiële verantwoording. Tevens kan door het voldoen aan SOX operationele efficiëntie bereikt worden in het aantal controlemaatregelen door je als organisatie te richten op de belangrijkste controlemaatregelen en door een goed begrip van de relatie tussen bedrijfsproces en financieel proces.

Ook verbeteringen van het systeem van interne controle kunnen tijdelijk leiden tot hogere kosten. Bijvoorbeeld wanneer een organisatie haar interne controle systeem had verwaarloosd of wanneer een organisatie een steile groeicurve heeft doorgemaakt en haar AO/IC nog niet aangepast had aan de nieuwe situatie. Graag verwijs ik voor dit onderwerp naar paragraaf 4.10 hieronder, voor meer details.

Mede door SOX wordt een trend zichtbaar van hernieuwde aandacht voor het interne controlesysteem: dus niet alleen aan de Amerikaanse beurs[16] genoteerde bedrijven verbeteren hun interne controlesysteem, maar denk ook aan ontwikkelingen gebaseerd op de code Tabaksblad[17]. Daarnaast zie ik in mijn praktijk diverse bedrijven bezig met het inrichten van een 'business control framework'. Deze worden door het hoger management geïnitieerd.

De ontwikkelingen ten aanzien van interne controle en het verbeteren daarvan, bijvoorbeeld door het bepalen van de sleutelcontrolemaatregelen, de documentatie daarvan, het periodiek vaststellen van de werking verloopt langzamer wanneer deze niet wordt gesteund door een set van maatregelen (inclusief 'boeteclausules'). Vanuit SOX wordt ook een beoordeling door een externe accountant

[15] www. wikipedia.org: `Due diligence` is het onderzoek dat meestal plaatsvindt bij bedrijfsovernames en outsourcing. De overnemende partij zal zich ervan willen overtuigen dat er geen kat in de zak wordt gekocht en daartoe een (uitgebreid) boekenonderzoek laten verrichten. Ook zal onderzocht worden of er geen juridische, fiscale of andere problemen zijn. Door een due diligence onderzoek kan ook de waarde van het over te nemen bedrijf beter worden bepaald.
[16] De SEC registrants
[17] Voor meer informatie www.commissiecorporategovernance.nl

gevraagd. Dit maakt dat er directe controle is door accountants en/of IT auditors die vaker met dit bijltje hebben gehakt. Zij hebben ervaring met interne controle systemen bij andere organisaties en kennen de eisen waaraan 'effectieve' controlemaatregelen dienen te voldoen. Verwacht mag worden dat zij tevens beschikken over inhoudelijke kennis van de industrie en markt waarin de betreffende organisatie opereert.
Dat beursgenoteerde bedrijven auditing standaarden voor accountancy firms gebruiken voor implementatie en onderhouden van SOX helpt ook bij het sneller op niveau brengen van controlemaatregelen en documentatie daarvan. Verbeteringen in het systeem van interne controle zullen theoretisch ook leiden tot verbeteringen ten aanzien van applicatieve en geautomatiseerde controlemaatregelen.

4.4 Verandering van de rol van het 'audit committee'

De Sarbanes Oxley Act stelt expliciet eisen ten aanzien van audit committees[18], het is geen verwonderlijke ontwikkeling dat deze committees te maken krijgen met toegenomen activiteiten (zie ook paragraaf 4.10). Fletcher schrijft in 2003 (p59) al dat de rol van het audit committee zoals deze voor implementatie van de wet was ingericht, is veranderd. Dit geldt ook voor de relatie van het audit committee met de CFO, aangezien de laatste het audit committee tijdig dient te voorzien van juiste en volledige informatie.

Naast dat een audit committee meer activiteiten uit te voeren krijgt bij implementatie van SOX en het blijvend voldoen aan SOX, vereisen deze activiteiten ook dat een audit committee voldoende kennis en ervaring bezit. Paape (2008) onderschrijft het belang om binnen het audit committee voldoende financiële kennis in huis te hebben. Mijns inziens dient het audit committee ook voldoende IT kennis te hebben. Vanuit haar formele (SOX) taak heeft het audit committee een soort 'monitoring' functie over 'accounting and financial reporting processes' en over 'audits of the financial statements'. In het geval er bevindingen zijn ten aanzien van IT gebaseerde controlemaatregelen en ITGC's zal het audit committee voldoende kennis van zaken moeten hebben om deze op impact in te schatten. Dit kan betekenen dat IT hoger op de organisatieagenda komt te staan.

4.5 Certificering

Een gevolg van Sarbanes Oxley Act welke door Fletcher (2003, p. 59) wordt beschreven, is het 'doordruppeleffect' van certificering. Hierbij worden controllers door CFO's verplicht om certificaten te ondertekenen dat door hen opgestelde rapportages compleet en accuraat zijn en voldoen aan de financiële verslagleggingregels. Hiermee vertoont het management risicomijdend gedrag (Leeuwen, 2007).

Dit vormt overigens een potentieel kostenverhogend element (paragraaf 4.10). Daarnaast gaat dit effect niet uit van vertrouwen in de expertise van de controllers. Fletcher trekt hierover echter geen verdere conclusies.

Het is de vraag in hoeverre dit binnen Nederlandse bedrijven speelt in het kader van het voldoen aan de Sarbanes Oxley Act. In mijn werkomgeving heb ik dit doordruppeleffect niet waargenomen. Daarnaast lijkt het een typische overreactie, niet uitgaand van vertrouwen maar van het oneigenlijk zoeken naar zekerheid. Een zekerheid die naar mijn mening niet door het tekenen van een certificaat kan worden geleverd. Deze certificering zoals door Fletcher weergegeven heeft geen relatie met IT[19].

Tot slot lijkt dit een tegengestelde beweging ten aanzien van 'professionalisering van de financiële functie' als beschreven in de volgende paragraaf. Certificering lijkt meer tot een ontwikkeling van 'indekken' te leiden dan tot een ontwikkeling naar 'het nemen van verantwoordelijkheid' waar die professionalisering op duidt.

[18] Audit committee is a committee (or equivalent body) established by and amongst the board of directors of an issuer for the purpose of overseeing the accounting and financial reporting processes of the issuer and audits of the financial statements of the issuer. Bron: Sarbanes Oxley Act.
[19] Leen Paape (2008) gaat hier verder op in, zie de verwijzing in de literatuurlijst.

4.6 Professionalisering van de financiële functie

Busco (2005) signaleert dat als gevolg van de implementatie van de Sarbanes Oxley Act de financiële functie verder professionaliseert. De wet vraagt namelijk van de financiële specialisten dat zij meer en meer betrokken zijn bij het opstellen van de strategie, het meten van prestaties en continue verbeteren van processen. Busco (2005) beschrijft als reden dat de financiële functie verplicht is om de verantwoording achterliggend aan de cijfers te verzamelen en vervolgens te verspreiden aan een brede groep van belanghebbenden. Een belangrijke uitdaging welke Busco ziet is dan ook de interne organisatie zo op te lijnen dat het voorgaande mogelijk wordt.

Professionalisering van de financiële functie heeft niet direct een impact op de IT, of het moet al zijn dat door deze professionaliseringsslag meer aandacht is voor in eerste instantie onderbelichte elementen als applicaties waar de financiële cijfers uit voortkomen. Ik kan me in dat licht voorstellen dat eisen gesteld worden aan de IT afdeling en aan de inrichting van IT systemen. In die zin dat voldoende waarborgen genomen worden dat kritische applicaties qua continuïteit zijn geborgd of voldoende afgeschermd voor misbruik door een ongeautoriseerde gebruiker (applicatieve en/of geautomatiseerde controlemaatregelen). Wanneer echter de financiële functie eisten stelt aan IT, moet deze functie daartoe vanzelfsprekend voldoende kennis hebben: kennis over de applicaties maar ook over de beheersomgeving van deze applicaties (ITGC's). Ontwikkelingen die hiermee te maken hebben zijn 'hogere budgetten IT'(paragraaf 4.7) en verandering van de rol van de Chief Information Officer (paragraaf 4.8).

4.7 Meer budget voor IT

Hoffman (2005) geeft aan dat vanuit de Sarbanes Oxley Act een toegenomen vraag zichtbaar is geworden naar data toegankelijkheid. Als gevolg hiervan signaleert Hoffman dat Chief Information Officers (CIO's) budget krijgen voor projecten waar voorheen geen prioriteit aan werd gegeven. Door meer budget kan CIO de rol van IT en de toegevoegde waarde ervan (door goede inrichting) aantonen, waardoor de IT afdeling een verdere professionalisering door kan maken.

Meer geld is noodzakelijk en daarom misschien een logisch gevolg van SOX; indien meer eisen gesteld worden aan IT (zie ook voorgaande paragraaf) en meer gesteund gaat worden op applicatieve en geautomatiseerde controlemaatregelen, dan dient IT hierbij aangehaakt te zijn. Ook heeft dit effect op de ITGC's deze dienen immers effectief te zijn. Kortom, het IT deel van de interne controle zou beter ingericht kunnen worden, wanneer hier afdoende budget voor is. Of beter gezegd dan is geld in ieder geval geen belemmerende factor. In mijn werk bij een van de 'Big 4' zag ik dit in de verschillende SOX trajecten (sectie 404) terugkomen, een wezenlijk deel van het budget van de bedrijven werd besteed aan IT (ITGC's en AC's). Ook het besteedbare budget van de IT audit groep op deze bedrijven weerspiegelt het belang van IT.

4.8 Dubbele rol van de Chief Information Officer

Hoffman (2005, p. 36) omschrijft de dubbele positie van de Chief Information Officers (CIO) als gevolg van de invoering van de Sarbanes Oxley Act. Deze complexiteit ontstaat omdat de functie van de CIO aan belang wint. In navolging van de wet leren mensen inzien dat IT omgevingen complex zijn en dat hun organisatie sterk afhankelijk is van IT, waaruit de conclusie getrokken wordt dat IT problematiek, in welke vorm dan ook, directe impact heeft op de bedrijfsvoering. Hoewel Hoffman aan geeft dat die dubbele rol van de CIO naarvoren komt in geval van problemen, geeft hij ook aan dat IT problematiek niet leidt tot het aan de kaak stellen van de rol van de CIO maar die van de Chief Executive Officer (CEO) of Chief Finance Officer (CFO), omdat '*accountability resides with those directly responsible for the business*'. Enerzijds wint de CIO functie dus aan belang en invloed, maar anderzijds worden zij bij misstanden of problemen hier niet op aangesproken, maar eerder de CFO en CEO. Historisch zie je dit terug in het bedrijfsleven omdat IT vaak onder de Financiële functie hangt en niet een zelfstandige entiteit of unit vormt binnen een bedrijf.

Hoffman (2, 2005, p. 36) beschrijft tevens een andere mogelijke groeirichting die aansluit bij laatstgenoemde. Dit betreft het groeien van de CIO rol naar die van de CFO, als gevolg van de eis van de CFO om bewijs te krijgen dat IT in overeenstemming met de gestelde eisen en wensen opereert. Dit betekent dat ook de CIO voldoende kennis van de primaire bedrijfsprocessen dient te hebben,

waarbij de aandacht van de CIO gericht dient te zijn op data-integriteit, beveiliging en de interactie tussen controlemaatregelen en systemen. De vraag is volgens Hoffman of na het voldoen aan de Sarbanes Oxley Act de CIO weer in haar oude positie terugvalt.

Concluderend, bovenstaande houdt in dat de functie van CIO aan belang wint en zichtbaarder wordt door de aan IT gestelde eisen, waarbij de CIO opschuift naar de CFO. Echter, ook wordt hier duidelijk dat van de CIO wordt verwacht de primaire processen en door redenerend bijbehorende AO/IC te kennen. Aan het produceren van een product zit nu eenmaal een administratieve stroom verbonden. Voor het assembleren van een auto zijn manuren, machinecapaciteit en onderdelen nodig, elk met hun eigen administratieve stroom en controlemaatregelen om te waarborgen dat er geen capaciteit en kapitaal verloren gaat. De CFO en CEO zijn ook het uiteindelijke management dat dient af te tekenen over de interne controle; gezien de hoge mate van automatisering en daarmee het groeiende aantal geautomatiseerde controlemaatregelen is het niet verwonderlijk dat CFO aangehaakt wil zijn bij de CIO. Hierin zit naar mijn mening wel een tegenstrijdigheid, namelijk dat de CIO die schijnbaar aan belang wint ('opschuift naar de CFO'), echter niet de eindverantwoordelijkheid draagt. In hoeverre is het dan zo dat IT daadwerkelijk aan belang wint? Of anders, kan de CIO ten aanzien van de IT gebaseerde controlemaatregelen en beheeromgeving een voldoende tegengewicht bieden bij problemen? Zolang de laatste zich niet voordoen lijkt het een goede ontwikkeling dat de CIO direct aangehaakt is bij de CFO en dicht op de primaire processen zit, om zo efficiënt en effectief mogelijk de 'business' te ondersteunen. Dezelfde spanning vindt je ook terug in paragraaf 4.7, 'Groeiend budget voor IT', daaruit zou namelijk geconcludeerd kunnen worden dat de IT (binnen SOX, sectie 404) aan belang wint.

4.9 Zero risk strategie

CIO's zagen als gevolg van de implementatie van SOX (Hoffman_2, 2005, p. 36), de door hen gehanteerde besluitvorming op basis van risicomanagement, uit handen genomen worden. Dit doordat auditors eisen stelden ten aanzien van IT waarbij geen of bijna geen risico tolerantie werd gehanteerd**.** Het is bij zo'n aanpak moeilijk om als IT, kostenbesparend en performance verhogend, te werken.

Overigens zal de CFO deze risicomijdende strategie in eerste instantie navolgen. Dit volgt onder andere uit paragraaf 4.8; de CFO is immers eindverantwoordelijke en zal de beoordeling van de inrichting van de interne controle mede ondertekenen. Wanneer bij het niet voldoen aan eisen van de auditors dit zal leiden tot problemen bij de evaluatie van de auditors, zullen de eisen worden ingewilligd en zal de CFO dit bij de CIO afdwingen. De laatste is meestal niet eindverantwoordelijk.

De relatie van 'zero risk strategy' en haar implicaties naar de bijdrage van IT in transparante financiële verslaglegging is niet direct. Wat helder mag zijn is dat 'alles' doen niet per definitie de beste oplossing is. In de praktijk is deze 'zero risk strategie' voor SOX losgelaten, niet in de laatste plaats vanwege de klachten vanuit het bedrijfsleven over hoge kosten (zie paragraaf 4.10). Audit standaarden (PCAOB) zijn hierop aangepast in 2007.

Op zich biedt IT ook veel mogelijkheden om kostenbesparingen door te voeren. Indien meer gesteund kan worden op geautomatiseerde controlemaatregelen (dus inclusief effectieve ITGC's), betekent dit een vermindering van de uit te voeren testwerkzaamheden. Geautomatiseerde controlemaatregelen hoeven maar een keer getest te worden. Daarnaast kan bij geautomatiseerde controlemaatregelen en het geautomatiseerde deel van applicatieve controlemaatregelen, onder bepaalde voorwaarden, roulatie gehanteerd worden[20].

Kosten:

[20] Wanneer de ITGC's werken en betreffende controlemaatregelen niet zijn gewijzigd volstaat het om geautomatiseerde controlemaatregelen eens per drie jaar te testen.

4.10 Kosten verhogende factoren

Een veel gehoorde klacht over SOX betreft de kosten die gepaard gaan met implementatie van deze wet. Vooral het midden en kleinbedrijf zouden onevenredig hoge kosten hebben. Dit gaat om 'operations' kosten, 'compliance' kosten en extra fees ten aanzien van aanvullende controles op de 'financial statements' (Anonymous, 2003, p.4).

De hieronder opgenomen opsomming van kostenverhogende factoren zijn onder te verdelen in twee categorieën. De eerste betreft kosten verhogende factoren die door de organisaties zelf worden veroorzaakt (intern) en niet specifiek aan SOX toe te wijzen zijn. Bijvoorbeeld dat de documentatie van interne controlesystemen niet in orde was. De tweede categorie betreft de kostenverhogende factoren die direct aan invoering van de wet zijn te wijten (extern). Een voorbeeld hiervan is onvoldoende richtlijnen ter ondersteuning van implementatie van de wet. Ik concentreer me op de laatste categorie, externe factoren.

Onduidelijkheid van wetgeving
Een kostenverhogende factor werd gevormd doordat bij implementatie van SOX de wet en uitvoering niet juist is geïnterpreteerd. In eerste instantie hebben veel organisaties ook naar operationele processen gekeken (vanuit een bottom up aanpak) en werd niet vanuit de key financial areas gewerkt. Ik verwijs hierbij naar paragraaf 3.1, Sectie 404 geplaatst in de organisatie. Dit resulteerde in te veel (te monitoren en te testen) controlemaatregelen (Ho, 2007, p5). Dit resulteerde in meer werkzaamheden, maar ook meer discussies over wat nu de voornaamste controlemaatregelen zijn (Ho, 2007, p5).

Bewijs van onafhankelijkheid
Fletcher (p.58) identificeerde in 2003 al dat het bespreken van bevindingen met accountants meer tijd in beslag nam dan vóór SOX. Fletcher geeft als oorzaak dat accountantskantoren hun onafhankelijkheid willen aantonen en omdat ze erop staan dat bepaalde bevindingen (eerder afgedaan als niet materieel) worden gecorrigeerd. Meer discussie, meer inzet van accountants, meer correcties betekent meer geld kwijt aan accountantsondersteuning. Accountants lopen zelf meer risico's onder SOX, voeren om dit risico te mitigeren meer werkzaamheden uit en hebben dit teruglaten komen in hun fees. Dit is volgens Basilo (2007) versterkt doordat auditors onvoldoende gebruik gemaakt hebben van werkzaamheden van '*competent internal auditors and SOX consulting firms*'.

Gericht op audit en controlemaatregelen
De focus van de SEC en PCAOB ten aanzien van interpretatie en uitvoering van de wet is sterk gericht op audit en controlemaatregelen (Sharman, 2007). Dit wordt versterkt door accountantskantoren die sterk bottom up en control gericht aan de slag zijn gegaan (Gupta et al, 2006, p.28). Tevens zie ik in mijn praktijk dat bij aanvang van de SOX implementatie er minder aandacht was voor het steunen op werk van derden, bijvoorbeeld internal audit of een advieskantoor anders dan de eigen externe auditor. Risicomijdend gedrag?

Verkeerd gebruik van richtlijnen
Auditing standards (met name AS2) werden veelal door management als de standaard gebruikt voor het evalueren van hun interne controlemaatregelen. Dit terwijl het een beoordelingsinstrument voor de externe auditor is om vast te stellen of de interne controlemaatregelen effectief zijn (Gupta et al 2006, p. 30-33). De oorzaak moet ook gezocht worden in het algemene karakter van COSO. Met COSO is het lastig bepalen of een controlemaatregel nu al dan niet effectief is. Aanvullend geldt dat er geen specifieke implementatie richtlijnen waren opgezet voor het management. Kortom, de auditing standaard is gehanteerd voor implementatie van SOX, welke niet voor dit doel bedoeld was omdat een heldere handleiding ontbrak. Hierdoor hebben bedrijven te veel maatregelen genomen.

Training
Het trainen van personeel bij invoering van nieuwe standaarden levert in het algemeen organisaties extra kosten op, dit gold ook voor implementatie van SOX (Ho, 2007, p5, Fletcher 2003, p.61). Aanvullend geldt dat de leercurve bij dit soort implementaties meer tijd in beslag neemt in de eerste ronde. Wanneer er meer kennis is van de standaard bij de SOX consulting firms / accountants

kantoren en ondersteunende tooling beschikbaar is, zullen de kosten dalen (Ho, 2007, p2; Basilo 2007, p.8).

Achterstanden
Organisaties hadden hun interne controledocumentatie op basis van jarenlang risk based auditen verwaarloosd. Dit actueel maken van deze documentatie is tijdrovend gebleken (Basilo 2007). Aanvullend bestond er zeker in situaties waarin controledocumentatie achterstallig onderhoud kende, het risico dat de operatie binnen organisaties wijzigde als gevolg van SOX (Fletcher, 2003). Ook dit resulteerde in extra kosten, bijvoorbeeld door verlies van productiviteit bij de start van de implementatie, wijzigingen in het proces om te voldoen aan interne controledoelstellingen, implementatie van nieuwe technologie en toegenomen controlekosten.

Met opzet wordt in bovenstaande opsomming niet gerept over algemeen projectmatige elementen zoals management commitment, goede coördinatie, duidelijke mijlpalen enzovoort. Echter dit zijn wel degelijk zaken die mee kunnen spelen en kunnen leiden tot onevenredig hoge kosten. Onevenredig is naar mijn mening dat de uiteindelijke doelstelling en/of het bewezen nut niet meer opweegt tegen de kosten.

PCAOB en SEC probeerden naar aanleiding van klachten uit het bedrijfsleven op deze laatste categorie in te spelen. Deze klachten komen ook terug in uitspraken van de The US Chamber of Commerce om AS2 te versoepelen, dit zou namelijk een verlichting van de SOX 404 kosten betekenen (Chamber Hopes Cox Forces Revision in Auditing Standard No. 2, 2005, p61). De SEC heeft naar aanleiding van de klachten twee ronde tafels gehouden, waarbij naast de SEC, PCAOB, externe auditors en investeerders aanwezig waren. Met als doel om de focus externe auditors van 'bottom-up control centric' om te zetten naar een meer 'top-down, risk-based' benadering[21] te verschuiven. De PCAOB heeft in 2007 een nieuwe controle standaard uitgebracht (Leeuwen, 2007).
De kosten van SOX zullen de komende jaren waarschijnlijk verder dalen. De administratie van SOX is minder complex, er is meer ervaring bij organisaties, bedrijven en toezichthouders en de aanpak

[21] De roep om een meer risicogebaseerde aanpak in plaats van een controlegebaseerde aanpak kent voor- en tegenstanders. Enerzijds zou de risico gebaseerde aanpak efficiënter en daarmee minder kostbaar zijn voor organisaties. De verschillende rationalisatieprojecten binnen organisaties richten zich ook op het minimaliseren van controlemaatregelen, een opschoning vindt voorbeeld plaats op elkaar overlappende controlemaatregelen. Daarnaast kan verdere automatisering ook efficiëntie opleveren.

Tegenstanders geven aan dat er ook risico's kleven aan een meer risicogebaseerde aanpak. Allereerst is er subjectiviteit in het spel (Basilo, 2007, p8) en daarnaast dient een voldoende analyse plaats te vinden of alle mogelijke zwakheden in het systeem van interne controle zijn afgedekt en of voldoende controlemaatregelen zijn ingericht om eventuele risico's en zwakheden in het systeem van interne controle af te dekken (Sharman, 2007, p15 en Basilo 2007, p8). Sharman waarschuwt ook voor het te sterk de nadruk leggen op controlemaatregelen (Sharman, 2007, p15) ofwel het creëren van een cultuur waarin controlemaatregelen worden afgedraaid als een lesje of een stappenplan, checklist, dit leidt niet tot het halen van de doelstelling van sectie 404. Dit risico is aanwezig als een organisatie zich alleen richt op het voldoen aan de wetgeving, maar deze wetgeving niet voldoende 'internaliseert'. SOX is gericht op het nemen van verantwoordelijkheid met name van het top management. SOX wil dus 'governance' verbeteren.

Met betrekking tot het laatste onderschrijf ik uitspraken van Christiano Busco et al (2005, p. 35- 43). Zij stellen dat een 'primary focus on compliance isn't enough for good governance. Vervolgens beargumenteren zij het belang van performance en kennismanagement, naast compliance (Christiano Busco et al, 2005, p. 35-43). Compliance houdt in dat het creëren van toegevoegde waarde als organisatie in overeenstemming dient te zijn met interne en externe regelgeving. Het niet voldoen aan deze regelgeving kan immers je imago en reputatie beschadigen. Dit gaat ook uit van de eerder gegeven definitie van een organisatie (hoofdstuk 2). Vervolgens is performance een belangrijk element ofwel verantwoording aan de aandeelhouders. Om als een organisatie voldoende waarde te creëren is het van belang dat je risicomanagement hebt ingebed. Zowel op financieel, operationeel, imago, omgeving, etc. Dit gaat verder dan alleen formeel risicomanagement tevens dient cultural awareness gecreëerd te worden ten aanzien van risico's in de dagelijkse activiteiten. Tot slot is er het element kennismanagement, hiermee kan het 'commitment' van een medewerker ten aanzien van regelgeving, normen & waarden, doelen en 'organization performance' worden vergroot.
Deze drie elementen zijn van belang voor het bereiken van 'good governance'. Ik denk dat deze drie elementen ook van toepassing zijn bij implementatie en onderhoud van SOX, en daarmee ook voor inrichting van het systeem van interne controle. Hiermee bereik je het eerder genoemde 'internalisatie'. Niet het afdraaien van checklisten om voor de vorm te voldoen aan regelgeving. Eigenlijk komt het erop neer om als topmanagement te bewaken dat je personeel gemotiveerd is om eigen verantwoordelijkheid te nemen. In feite om hun werk gewoon 'goed' te doen. Deze eigen verantwoordelijkheid nemen geldt voor alle lagen van de organisatie en voor alle soorten werk of het nu uitvoering, monitoring of controle betreft. De middelen kunnen nog zo fantastisch zijn als ze niet met verantwoordelijkheid worden gehanteerd zal het doel er niet mee worden bereikt.

wordt meer risk-based (Ho, 2007, p6; Paape, 2008). Tevens zie ik vanuit mijn praktijk dat diverse organisaties zijn begonnen met rationalisatieslagen. Dit laatste houdt in dat door de meer risk-based, top down approach de te ruime scoping bij aanvang van de implementatie van SOX wordt rechtgezet. Dit heeft een direct effect op de kosten, aangezien minder controlemaatregelen als key worden opgenomen en er dus minder getest en geëvalueerd dient te worden. Daarnaast zal een verder gaande automatisering de weg openen voor meer geautomatiseerde controlemaatregelen, dat betekent dat minder uitgebreide deelwaarnemingen genomen hoeven te worden. Tot slot kan het handig inzetten van geautomatiseerde tools ter ondersteuning van SOX het proces van evalueren efficiënter maken.

5. Doel en Middel in onbalans?

In dit hoofdstuk keer ik terug naar de centrale vraag '*Heeft IT bijgedragen aan een transparante financiële verslaglegging waardoor het vertrouwen van investeerders wordt hersteld*.' Hierbij ga ik eerst op metaniveau in op deze vraag, vervolgens ga ik specifiek in op de vraagstelling op basis van de in hoofdstuk 4 geïdentificeerde gevolgen alvorens te komen tot een slotconclusie.

In de tijdspanne dat ik aan deze scriptie heb gewerkt, heb ik SOX geïmplementeerd zien worden bij Nederlandse SOX-plichtigen. Vanuit mijn werkzaamheden bij PricewaterhouseCoopers heb ik in diverse SOX trajecten geassisteerd, ook heb ik de eerste rationalisatieslagen bij deze *foreign registrants* meegemaakt. Deze rationalisatie zette in, na het eerste jaar dat deze *registrants* SOX plichtig waren. Ofwel de implementatie van een meer risicogebaseerde en *top down* aanpak. Bij deze nieuwe aanpak werden de werkzaamheden in het kader van de jaarrekening en de werkzaamheden voor SOX op een efficiëntere manier samengevoegd. Logisch, zeg je achteraf, immers hoe zou SOX en dan metname sectie 404: interne controle over financiële verslagleggingprocessen, losgekoppeld kunnen zijn van de processen die leiden tot de jaarrekening? Ook betekende de rationalisatie dat binnen de audits meer gericht werd op *key controls* (financiële) en minder op operationele controls[22]. Niet alleen uit kosten perspectief, immers minder *key controls* is minder testwerk, maar ook omdat interne controle effectiever wordt. Als organisatie kun je je richten op die risico's, op die zaken die de kern van je *business* vormen.

5.1 Op metaniveau

In dezelfde tijdspanne dat SOX geïmplementeerd werd, deden zich diverse schandalen voor. In de inleiding heb ik hier reeds aan gerefereerd. De schandalen in de financiële sector hebben geleid tot een kredietcrisis (2008) en uiteindelijk zijn we op dit moment (2009) in een wereldwijde recessie weggezakt. Hoe diep deze recessie is en hoe lang die gaat duren daarover wordt veelvuldig gepubliceerd in de media.

Wanneer ik op een hoger niveau naar de centrale vraag van deze scriptie kijk, dan lijkt het mij dat het **middel**, sectie 404 'management assessment of internal controls', niet geleid heeft tot het **doel**, maatschappelijk vertrouwen. Dit raakt dus vooral het laatste gedeelte van de centrale vraag, te weten: *'waardoor het vertrouwen van investeerders wordt hersteld'*.

SOX heeft blijkbaar niet kunnen voorkomen dat schandalen zich voordeden. Specifieker uitgedrukt betekent dit dat interne controle en daardoor ontstane transparante(re) financiële verslaglegging, deze schandalen niet hebben kunnen voorkomen. Het vertrouwen van investeerders is door de huidige crisis gedaald.

Dit doet mij nu de vraag stellen of de onderliggende aanname van SOX misschien onjuist is? Is het zo dat goede interne controle leidt tot transparante verslaglegging en dat daardoor het vertrouwen van investeerders stijgt? Interne controle en transparante verslaglegging zijn de primaire levensbehoeften van een organisatie, maar zorgen die automatisch voor meer vertrouwen van investeerders?

Gaandeweg dit onderzoek is mijn twijfel komen te liggen bij het vertrouwensaspect binnen de centrale vraag, het vertrouwen van investeerders. Vertrouwen is ´zacht´ en ´ongrijpbaar´, Waarom vertrouw je iemand, op persoonlijk niveau? Vaak kan ik dat niet goed uitleggen, en is het een gevoel of noem het instinct. Welke factoren geven investeerders vertrouwen? Ik denk dat dit niet alleen ´harde´ factoren zijn, en hierin sta ik niet alleen. Ook past hier voor mij oplettendheid, omdat mijn onderzoek zich hier niet op richt. Mijn centrale vraag was gericht op het verband tussen SOX en transparante financiële verslaglegging: zorgt SOX dat de IT-processen bijdragen aan een transparante verslaglegging, en hoe zit dat dan. Maar uiteindelijk geeft voor mij de ongrijpbaarheid van het begrip

[22] Anders dan diverse codes binnen de EU vraagt SOX alleen een oordeel op financieel gebied niet op operationeel gebied. Dit laatste is voor een organisatie uiteraard ook van belang maar verdient een andere aanpak. Hoeft niet per se als key control te boek te staan.

vertrouwen voldoende aan dat het **doel** en het **middel** van SOX in **onbalans** zijn. Dat het niet dát oplevert waaruit investeerders vertrouwen krijgen.

Die nadruk op vertrouwen zie ik veel terug in de media, maar ook bij mijn huidige werkgever, de Belastingdienst. Het fenomeen horizontaal toezicht gaat uit van een basis van vertrouwen tussen de twee partijen, de organisatie en de Belastingdienst. Dit uitgangspunt wordt onderstreept door een convenant. In de praktijk betekent dit een totaal andere proactieve manier van werken, waarbij de Belastingdienst niet meer achteraf, soms jaren later, een controle op bijvoorbeeld de omzetbelasting uitvoert, maar waarbij ze in het hier en nu met de organisatie bespreekt: 'hoe ben je in control over je organisatie?'; 'Hoe richt je jouw interne beheersing in en hoe dekt dit jouw fiscale risico's af?' Een belangrijk element in gesprekken met deze organisaties en in analyses die de Belastingdienst uitvoert is de *tone at the top*. Ook bij SOX vormt dit een aandachtspunt. Wat is de houding van de leiding van een organisatie. Wat is hun *risk appetite*?

5.2 Terug naar de geïdentificeerde gevolgen

Transparante verslaglegging
Wat valt er nu aan de hand van de geïdentificeerde gevolgen van SOX (zie hoofdstuk 4) te zeggen over de centrale vraag. Dit snijdt zich toe op het eerste gedeelte van de centrale vraag *´Heeft IT bijgedragen aan een transparante financiële verslaglegging... ´*. Het lastige is dat in de literatuur beschreven gevolgen van sectie 404 of SOX op een ander, meer algemeen, niveau zijn dan nodig is voor een goede beantwoording van deze vraag. Ik heb voorafgaand aan deze scriptie op basis van beperkt literatuur onderzoek tot deze aanpak besloten en nu achteraf moet ik concluderen dat het interessante inzichten geeft in deze wetgeving maar dat het geen expliciete *harde* inzichten geeft in de bijdrage van IT aan transparante financiële verslaglegging.

Nu ik heb aangegeven waar ik geen voldoende antwoord op heb kunnen geven, rest de vraag wat ik wel zie op basis van de geïdentificeerde gevolgen van SOX. Ik beperk me hierin conform de vraagstelling tot de IT gerelateerde ontwikkelingen. Een aantal van deze ontwikkelingen geven inzicht in de wisselwerking tussen sectie 404 en IT. Doordat sectie 404 zich richt op interne controle geeft dit ook mogelijke inzichten voor de relatie van IT en interne controle.

Algemeen kan gesteld worden dat ook uit de geïdentificeerde gevolgen van SOX blijkt dat IT belangrijk is danwel belangrijker is geworden voor organisaties. Zowel de financiële functie (paragraaf 4.6) als de (externe) auditor stelt eisen aan IT, ook het groter beschikbare budget voor IT (paragraaf 4.7) geeft aan dat IT binnen organisaties, in het kader van SOX, belangrijk wordt gevonden. Er is blijkbaar inzicht dat zonder aandacht voor IT SOX implementatie en onderhoud om compliant te blijven onvoldoende mogelijk is. Achterliggende gedachte bij het stellen van eisen aan IT is, dat de financiële functie voldoende kennis heeft over IT of in ieder geval dat zij een discussie aangaat met de IT functie over wat IT al dan niet kan leveren. Waar zij ten aanzien van interne controle wel comfort kan leveren en waarvoor niet. Ten aanzien van dit laatste is het dan belangrijk om na te gaan wat hiervan de gevolgen zijn. Betekent dit aanvullend gegevensgericht werk? een andere controleaanpak?

Als er gekeken wordt naar de veranderende rol van het audit committee (paragraaf 4.4), met name als het gaat om de beoordeling van de interne controle, zal er ook binnen het audit committee (naar analogie van de financiële functie) inzicht moeten zijn in wat het belang van IT is. Hoe IT inwerkt op de primaire processen en belangrijker nog andersom, welke eisen stellen de primaire processen aan IT. Deze expertise moet in het audit committee zijn vertegenwoordigd.

Bijkomend is dat de IT functie zich zo op een andere manier op een hoger niveau zichtbaar kan maken in de organisatie en het belang van IT kan duiden. Ik zie hierbij een analogie vanuit mijn werkzaamheden bij jaarrekeningcontroles. Het bleek vaak lastig om bevindingen vanuit de IT audit, die in het kader van de jaarrekening tijdens een interim-controle was uitgevoerd voldoende onder het voetlicht te krijgen bij het management van een organisatie. Het kwam met regelmaat voor dat IT bevindingen op het gebied van ITGC's en AC's niet op tafel kwamen bij het management. Vanuit de IT audit groep is daar destijds veel aandacht voor geweest om de IT bevindingen en de impact hiervan

goed te duiden en vervolgens ervoor te zorgen dat de verantwoordelijke partner van de IT audit groep met de accountants aan tafel kwam bij het management[23].

Een spanningsveld wordt gevormd door de dubbelrol van de CIO (paragraaf 4.8), deze functie wint aan belang door het belang dat IT vormt voor een organisatie. De rol van de CIO groeit meer en meer naar de eindverantwoordelijke CFO toe. In dit laatste zit de spanning, de CIO heeft namelijk vaak niet de eindverantwoordelijkheid over IT (te weten over systemen, (deels) geautomatiseerde controlemaatregelen en ITGC's). Vanuit de historie ligt deze verantwoordelijkheid echter vaak bij de CFO.

Tot slot wordt de interne controle 'an sich' verbeterd door SOX (paragraaf 4.3). De eisen die door SOX gesteld worden met sectie 404 leiden tot een verbeterd systeem van interne controle. Dit betekent mijn inziens ook een verbetering voor de IT gebaseerde controlemaatregelen en de ITGC's. Deze verbetering en aanscherping van het systeem van interne controle krijgt een extra *boost* door de rationalisatieslagen die gestart zijn bij veel SOX plichtigen. Ook verwacht ik door een versterkte aandacht voor het verminderen van kosten een zoektocht naar het slimmer inrichten van het systeem van interne controle een focus op *key controls*, uitbuiten van (deels) geautomatiseerde controlemaatregelen en een goede beoordeling van welke manier van controle het meest efficiënt is.

Het is te hopen dat deze huidige crisis niet leidt tot het verminderen van de aandacht voor interne controle (onderhoud, monitoring, etc.) dat zou veel bedrijven terugbrengen naar een pre SOX situatie. De bedrijven die SOX compliant moeten zijn dienen hier ook in de toekomst aan te voldoen, maar de nadruk die SOX geeft aan interne controle is doorgesijpeld naar andere bedrijven die niet SOX compliant hoeven te zijn. In mijn praktijkervaring bij PricewaterhouseCoopers maar ook nu wanneer ik vanuit mijn functie bij de Belastingdienst bedrijfsbezoeken afleg zie ik bij niet SOX plichtigen aandacht voor *business control frameworks*, al dan niet veroorzaakt door de aandacht van hun externe accountants voor interne controle.

5.3 Vervolgonderzoek

Ik zou mij op basis van deze scriptie in een vervolgonderzoek graag bezighouden met het ontleden van het vertrouwen van investeerders. Welke elementen vormen dit vertrouwen, welke vermeerderen het vertrouwen of verminderen het vertrouwen juist. Vanuit deze insteek zou ik dan willen achterhalen hoe en welke rol interne controle hierbij speelt. Daarbij zou ik graag de in deze scriptie gehanteerde onderverdeling hanteren van interne controlemaatregelen (zie paragraaf 3.2): handmatige, applicatieve, geautomatiseerde controlemaatregelen en algemene IT beheersmaatregelen. Dit onderzoek dient kwantitatief van aard te worden waarbij door middel van een vragenlijst bovengenoemde relaties door middel van hypothesen getoetst worden. De doelgroep van dit onderzoek zou gevormd moeten worden door managers en investeerders. Waarbij de managers afkomstig zijn van bedrijven die te categoriseren zijn naar groot zakelijk (inclusief financiële dienstverlening) en de hogere laag van het midden bedrijf. Daarnaast dient een verdeling gehanteerd te worden naar al dan niet geregistreerd aan de beurs (Amerikaans en niet Amerikaans) en niet aan de beurs geregistreerde bedrijven.

[23] Het voert te ver de hele audit aanpak zoals deze gehanteerd wordt te beschrijven. Hierbij wil ik nog aangeven dat voorafgaand aan de werkzaamheden verantwoordelijken voor uitvoering van de werkzaamheden in het kader van de jaarrekening en/of SOX audit met het bedrijf om tafel dienen te gaan. Met verantwoordelijken doel ik dan op vertegenwoordiging vanuit de benodigde expertises (accountanc y en IT audit).

Definities

Algemene IT controlemaatregelen (ITGC)
Information Technology General Controls: Controls used to manage and control the IT activities and computer environment, covering the following areas: IT Control Environment, Program Development, Program Changes, Access to Programs and Data, and Computer Operations"(bron: audit guide used by audits executed by PricewaterhouseCoopers).

Applicatieve controlemaatregelen
Automated control procedures (e.g., calculations, posting to accounts, generation of reports, edits, control routines, etc.) or manual controls that are dependent on IT (e.g., the review by an inventory manager of an exception report when the exception report is generated by IT). When IT is used to initiate, authorize, record, process, or report transactions or other financial data for inclusion in financial statements, the systems and programs may include controls related to the corresponding assertions for significant accounts or disclosures or may be critical to the effective functioning of manual controls that depend on IT (bron: audit guide used by audits executed by PricewaterhouseCoopers).

Audit committee
Audit committee is a committee (or equivalent body) established by and amongst the board of directors of an issuer for the purpose of overseeing the accounting and financial reporting processes of the issuer and audits of the financial statements of the issuer (bron: Sarbanes Oxley Act).

Controle activiteit (= controlemaatregel)
The policies and procedures that help ensure that management's directives are carried out. They include business performance reviews, application controls, including safeguarding of assets, and general computer controls (bron: audit guide used by audits executed by PricewaterhouseCoopers).

Controle doelstelling
The objective(s) related to internal control over financial reporting to achieve the assertions that underlie a company's financial statements. Information processing objectives are a type of control objective (bron: audit guide used by audits executed by PricewaterhouseCoopers).

Geautomatiseerde controlemaatregelen
Controls performed by computer systems or enforced by system security parameters (bron: audit guide used by audits executed by PricewaterhouseCoopers).

Figuren

Literatuurlijst

Anonymous 'Chamber Hopes Cox Forces Revision in Auditing Standard No.2', *Strategic Finance*, 2005, (87), p.61.

Anonymous 'Sarbanes-Oxley loses popularity with execs', *Quality progress*, 2003 (36), p. 19. www.pw.com/gx/eng/about/press-rm/index.html.

Anonymous, 'Chemical executive take the oath', *Chemical Market Reporter*, 2002 (262), p.4.

Anonymous, 'Sarbanes-Oxley doubles the cost of compliance', *AFP Exchange*, 2003 (23), p.5)

Basilo, T.A., 'Reducing Sarbanes-Oxley Compliance Costs', *The CPA Journal*, 2007 (77), p. 6, 8-9.

Bloch, G.D, 'Sarbanes-Oxley's effects on interanl controls for revenue, *The CPA Journal*, 2003 (73), p. 68-70.

Busco, C., M.L. Frigo, E. Giovannie et al, 'Beyond Compliance: Why integrated governance matters today', *Strategic Finance,* 2005, p. 35 – 43.

Drexler, P.M. 'Can Proposed Audit Adjustments Challenge Auditor Independence?', *The CPA Journal*, 2005 (75), p.16 – 17.

Fletcher, G, 'Sarbanes-Oxley leaves heavy footprints on corporate America', *AFP Exchange*, 2003 (23), p. 56-61.

Gupta, P.P., en J.C. Thomson, 'Management reporting on Internal Control', *Strategic Finance*, 2006, p. 27-33.

Ho, S K and A.R. Oddo, 'Lessons Learned form Secton 404 of the Sarbanes-Oxley Act' *The CPA Journal*, 2007, p.1-8.

Hoffman, T., 'Transparency Trumps', *Computerworld*, 2005 (39), p. 36.

Hoffman_2, T, 'The Sarb-Ox SHIFT', *Computerworld*, 2005 (39), p. 36.

Koehn, J. L. en S.C. Del Vecchio, 'Ripple effects of the Sarbanes-Oxley Act', *The CPA Journal'*, 2004 (74), p.36-40.

Leeuwen, O. en P. Wallage, 'De zoektocht naar meer transparantie', *Bestuurlijke informatieverzorging*, 2007 (10), p.469 – 479.

Mahan, B., 'What Nonaccelerated Filers Can learn About Sarbanes-Oxley Compliance', *The CPA Journal*, 2005, p. 9.

McClennahen, J.S., T. Purdum, 'Sarbane's Oxley's limited Impact', *Industry Week*, 2003 (252), p.54.

Oliverio, M.E, 'Sarbanes-Oxley: Is reconsideration warranted?', *The CPA Journal,* 2003 (73), p.6,8.

Paape, L. 'In Control verklaringen: gebakken lucht of een te koesteren fenomeen', 2008, p. 103.

Pascoe-Samson, E, 'Organisatie, besturing en informatie', *Kluwer bedrijfsinformatie, ISBN 90-267-2801-8,* 1998, p.20.

PCAOB, 'An Audit of internal control over financial reporting performed in conjunction with an audit of financial statements, *PCAOB Release No. 2004-001,* 2004.

Sharman, P.A., 'Balancing Risk and Control Approaches for Sarbanes-Oxley Compliance', *The CPA Journal*, 2007 (77), P15.

Sarbanes-Oxley Act of 2002, To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.
Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled. PUBLIC LAW 107–204—JULY 30, 2002 116 STAT. 745

Bijlage 1: Wettekst title 4 'Enhanced Financial Disclosures'

Voor een volledig overzicht wordt verwezen naar de Sarbanes-Oxley Act, zie de literatuurlijst.

Sectie	Onderwerp	Korte weergave van de inhoud
401	Disclosures in Periodic Reports	DISCLOSURES REQUIRED.—Section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m) is amended by adding at the end the following (i and j): – (i) ACCURACY OF FINANCIAL REPORTS.—Each financial report that contains financial statements, and that is required to be prepared in accordance with (or reconciled to) generally accepted accounting principles under this title and filed with the Commission shall reflect all material correcting adjustments that have been identified by a registered public accounting firm in accordance with generally accepted accounting principles and the rules and regulations of the Commission. (…)
402	Enhanced conflict of interest provisions	(a) PROHIBITION ON PERSONAL LOANS TO EXECUTIVES.—Section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m), as amended by this Act, is amended by adding at the end the following: "(k) PROHIBITION ON PERSONAL LOANS TO EXECUTIVES.— "(1) IN GENERAL.—It shall be unlawful for any issuer (as defined in section 2 of the Sarbanes-Oxley Act of 2002), directly or indirectly, including through any subsidiary, to extend or maintain credit, to arrange for the extension of credit, or to renew an extension of credit, in the form of a personal loan to or for any director or executive officer (or equivalent thereof) of that issuer. An extension of credit maintained by the issuer on the date of enactment of this subsection shall not be subject to the provisions of this subsection, provided that there is no material modification to any term of any such extension of credit or any renewal of any such extension of credit on or after that date of enactment. "(2) LIMITATION.—Paragraph (1) does not preclude any home improvement and manufactured home loans (…) "(3) RULE OF CONSTRUCTION FOR CERTAIN LOANS.—Paragraph (1) does not apply to any loan made or maintained by an insured depository institution (…).
403	Disclosures of transactions involving management and principal stockholders	AMENDMENT.—Section 16 of the Securities Exchange Act of 1934 (15 U.S.C. 78p) is amended by striking the heading of such section and subsection (a) and inserting the following: **"SEC. 16. DIRECTORS, OFFICERS, AND PRINCIPAL STOCKHOLDERS.** "(a) DISCLOSURES REQUIRED.— "(1) DIRECTORS, OFFICERS, AND PRINCIPAL STOCKHOLDERS REQUIRED TO FILE.—Every person who is directly or indirectly the beneficial owner of more than 10 percent of any class of any equity security (other than an exempted security) which is registered pursuant to section 12, or who is a director or an officer of the issuer of such security, shall file the statements required by this subsection with the Commission (and, if such security is registered on a national securities exchange, also with the exchange). "(2) TIME OF FILING.—The statements required by this subsection shall be filed— "(A) at the time of the registration of such security on a national securities exchange or by the effective date of a registration statement filed pursuant to section 12(g); "(B) within 10 days after he or she becomes such beneficial owner, director, or officer; "(C) if there has been a change in such ownership, or if such person shall have purchased or sold a security based swap agreement (as defined in section 206(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 78c note)) involving such equity security, before the end of the second business day following the day on which the subject transaction has been executed, or at such other time as the Commission shall establish, by rule, in any case in which the Commission determines that such 2-day period is not feasible. (…)
404	Management assessment of internal	(a) RULES REQUIRED.—The Commission shall prescribe rules

	controls	requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall— (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting. (b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.
405	Exemption	Nothing in section 401, 402, or 404, the amendments made by those sections, or the rules of the Commission under those sections shall apply to any investment company registered under section 8 of the Investment Company Act of 1940 (15 U.S.C. 80a–8).
406	Code of Ethics for senior Financial officers	(a) CODE OF ETHICS DISCLOSURE.—The Commission shall issue rules to require each issuer, together with periodic reports requiredpursuant to section 13(a) or 15(d) of the Securities Exchange Act of 1934, to disclose whether or not, and if not, the reason therefor, such issuer has adopted a code of ethics for senior financial officers, applicable to its principal financial officer and comptroller or principal accounting officer, or persons performing similar functions. (b) CHANGES IN CODES OF ETHICS.—The Commission shall revise its regulations concerning matters requiring prompt disclosure on Form 8–K (or any successor thereto) to require the immediate disclosure, by means of the filing of such form, dissemination by the Internet or by other electronic means, by any issuer of any change in or waiver of the code of ethics for senior financial officers. (…)
407	Disclosures of audit committee Financial expert	(a) RULES DEFINING "FINANCIAL EXPERT".—The Commission shall issue rules, as necessary or appropriate in the public interest and consistent with the protection of investors, to require each issuer, together with periodic reports required pursuant to sections 13(a) and 15(d) of the Securities Exchange Act of 1934, to disclose whether or not, and if not, the reasons therefor, the audit committee of that issuer is comprised of at least 1 member who is a financial expert, as such term is defined by the Commission. (b) CONSIDERATIONS.—In defining the term "financial expert" for purposes of subsection (a), the Commission shall consider whether a person has, through education and experience as a public accountant or auditor or a principal financial officer, comptroller, or principal accounting officer of an issuer, or from a position involving the performance of similar functions— (1) an understanding of generally accepted accounting principles and financial statements; (2) experience in— (A) the preparation or auditing of financial statements of generally comparable issuers; and (B) the application of such principles in connection with the accounting for estimates, accruals, and reserves; (3) experience with internal accounting controls; and (4) an understanding of audit committee functions.
408	Enhanced revies of periodic disclosures by issuers	(a) REGULAR AND SYSTEMATIC REVIEW.—The Commission shall review disclosures made by issuers reporting under section 13(a) of the Securities Exchange Act of 1934 (including reports filed on Form 10–K), and which have a class of securities listed on a national securities exchange or traded on an automated quotation facility of a national securities association, on a regular and systematic

		basis for the protection of investors. Such review shall include a review of an issuer's financial statement. (b) REVIEW CRITERIA.—For purposes of scheduling the reviews required by subsection (a), the Commission shall consider, among other factors— (1) issuers that have issued material restatements of financial results; (2) issuers that experience significant volatility in their stock price as compared to other issuers; (3) issuers with the largest market capitalization; (…) (4) emerging companies with disparities in price to earning ratios; (5) issuers whose operations significantly affect any material sector of the economy; and (6) any other factors that the Commission may consider relevant.
409	Real time issuer disclosures	Section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m), as amended by this Act, is amended by adding at the end the following: "(l) REAL TIME ISSUER DISCLOSURES.—Each issuer reporting under section 13(a) or 15(d) shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer, in plain English, which may include trend and qualitative information and graphic presentations, as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest.'